2015-01-01

When Can The Primitive Element Be Written As A Sum Of Two Algebraic Elements Adjoined To The Field Of The Rational Numbers

Mohamad Moussa
University of Texas at El Paso, mmmoussa@miners.utep.edu

WHEN CAN THE PRIMITIVE ELEMENT BE WRITTEN AS A SUM OF TWO ALGEBRAIC ELEMENTS ADJOINED TO THE FIELD OF THE RATIONAL NUMBERS

MOHAMAD MEDHAT MOUSSA

Department of Mathematical Sciences

APPROVED:

Piotr J. Wojciechowski, Chair, Ph.D.

Art Duval, Ph.D.

Luc Longpré, Ph.D.

Charles H. Ambler, Ph.D.
Dean of the Graduate School

WHEN CAN THE PRIMITIVE ELEMENT BE WRITTEN AS A SUM OF TWO ALGEBRAIC ELEMENTS ADJOINED TO THE FIELD OF THE RATIONAL NUMBERS

by

MOHAMAD MEDHAT MOUSSA

THESIS

Presented to the Faculty of the Graduate School of

The University of Texas at El Paso

in Partial Fulfillment

of the Requirements

for the Degree of

MASTER OF SCIENCE

Department of Mathematical Sciences

THE UNIVERSITY OF TEXAS AT EL PASO

August 2015

Acknowledgements

I would like to acknowledge my advisor, Prof. Piotr Wojciechowski, for his support and guidance throughout my graduate work. Moreover, special thanks for the Mathematics Department, Prof. Mariani, for the financial support they provided me during my graduate study at UTEP. A special appreciation for the professors who taught me, for their hard work in teaching us. Finally, I must express my special gratitude to my wife and family members for all their motivation.

Abstract

Given a field $\mathbb{F}$ and elements α and β not in $\mathbb{F}$, then $\mathbb{F}(\alpha, \beta)$ is the smallest field containing α, β and $\mathbb{F}$. A *simple extension* is a field extension which is generated by the adjunction of a single element. The Primitive Element Theorem says that if $\mathbb{F}$ is a field of characteristic 0, and α and β are algebraic over $\mathbb{F}$, then there is an element γ in $\mathbb{F}(\alpha, \beta)$ such that $\mathbb{F}(\alpha, \beta) = \mathbb{F}(\gamma)$. When can we say that $\gamma = \alpha + \beta$? We will introduce some situations where $\gamma = \alpha + \beta$ is true and some when this is not true, where $\mathbb{F}$ is the field of rational numbers $\mathbb{Q}$.

Table of Contents

Chapter 1

Motivation

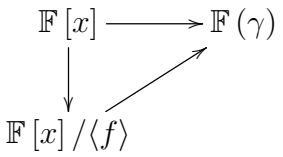
Our work in this thesis, is to investigate the situations where we can replace the field extension $\mathbb{F}(\alpha, \beta)$ by a simple extension $\mathbb{F}(\gamma)$. The importance of simple extensions is that they are completely classified.

Take $\phi : \mathbb{F}[x] \longrightarrow \mathbb{F}(\gamma)$ be a ring homomorphism defined by $\phi(g(x)) = g(\gamma)$, where $g(x) \in \mathbb{F}[x]$. Let f be the minimal polynomial of γ over $\mathbb{F}$, and then

$$\ker \phi = \{g(x) \in \mathbb{F}[x] : g(x) = 0\} = \langle f \rangle.$$

Since f is an irreducible polynomial, then $\langle f \rangle$ is a maximal ideal of $\mathbb{F}[x]$, and thus $\mathbb{F}[x] \diagup \langle f \rangle$ is a field.

By the First Isomorphism Theorem for rings, $\mathbb{F}[x] / \langle f \rangle = \mathbb{F}(\gamma)$.



Any simple algebraic extension of $\mathbb{F}$ is of the form $\mathbb{F}[x]/\langle f \rangle$ for some irreducible $f \in \mathbb{F}[x]$. Therefore, we can say that classifying $\mathbb{F}(\gamma)$ (up to isomorphism) is equivalent to classifying the irreducibility of f in $\mathbb{F}[x]$.

In field theory, the Primitive Element Theorem (Artin's theorem on primitive elements) says that a finite extension is simple if and only if there are only finitely intermediate fields. In particular, any finite separable extension is simple. The Primitive Element Theorem is formulated as: Let $\mathbb{F}$ be a subfield of $\mathbb{C}$, and α, β are two algebraic elements over $\mathbb{F}$, then

there exist $\gamma \in \mathbb{F}(\alpha, \beta)$ such that $\mathbb{F}(\alpha, \beta) = \mathbb{F}(\gamma)$.

The Primitive Element Theorem guarantees the existence of such an element γ. The difficulty in this theorem is to find what is this element γ. Can we say that $\gamma = \alpha + \beta$? We will introduce some situations where $\gamma = \alpha + \beta$, and other situations where γ can not be written as $\alpha + \beta$.

In our research, we are going to study under what conditions each of the following is true:

- $\mathbb{Q}\left(\alpha\sqrt{\delta}, \beta\sqrt{\eta}\right) = \mathbb{Q}\left(\alpha\sqrt{\delta} + \beta\sqrt{\eta}\right)$ for $\alpha, \beta, \delta, \eta$ rational numbers and $\sqrt{\delta}, \sqrt{\eta} \notin \mathbb{Q}$.
- $\mathbb{Q}\left(\sqrt{a + b\sqrt{p}}, \sqrt{q}\right) = \mathbb{Q}\left(\sqrt{a + b\sqrt{p}} + \sqrt{q}\right)$ for any a, b rational numbers and p, q prime numbers.
- $\mathbb{Q}\left(\sqrt{a + b\sqrt{p}}, \sqrt{c + d\sqrt{p}}\right) = \mathbb{Q}\left(\sqrt{a + b\sqrt{p}} + \sqrt{c + d\sqrt{p}}\right)$, where a, b, c, d are rational numbers and p is any prime number.

Chapter 2

Basic definitions and theorems

Some basic definitions and theorems will be presented that will help in the development of the main results.

Definition 2.1. A *field* is a set $\mathbb{F}$ together with two operations, usually called addition and multiplication, and denoted by $+$ and $\cdot$, respectively, such that the following axioms hold; subtraction and division are defined in terms of the inverse operations of addition and multiplication.

- *Closure of F under addition and multiplication* For all a, b in $\mathbb{F}$, both $a + b$ and $a \cdot b$ are in $\mathbb{F}$ (or more formally, $+$ and $\cdot$ are binary operations on $\mathbb{F}$).
- *Associativity of addition and multiplication* For all a, b, and c in $\mathbb{F}$, the following equalities hold:

$$a + (b + c) = (a + b) + c \quad \textit{and} \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

- *Commutativity of addition and multiplication* For all a and b in $\mathbb{F}$, the following equalities hold:

$$a + b = b + a \quad \textit{and} \quad a \cdot b = b \cdot a$$

- *Existence of additive and multiplicative identity elements* There exists an element of $\mathbb{F}$, called the additive identity element and denoted by 0, such that for all a in $\mathbb{F}$, $a + 0 = a$.

Likewise, there is an element, called the multiplicative identity element and denoted by 1, such that $1 \neq 0$ and for all a in $\mathbb{F}$, $a \cdot 1 = a$.

- *Existence of additive inverses and multiplicative inverses* For every a in $\mathbb{F}$, there exists an element $-a$ in $\mathbb{F}$, such that $a + (-a) = 0$.

  Similarly, for any $a \neq 0$ in $\mathbb{F}$, there exists an element a^{-1} in $\mathbb{F}$, such that $a \cdot a^{-1} = 1$.

- *Distributivity of multiplication over addition* For all a, b and c in $\mathbb{F}$, the following equality holds:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

Definition 2.2. The *characteristic* of a ring R is the least positive integer n such that $nx = 0$ for all x in R. If no such integer exists, we say that R has characteristic 0. The characteristic of R is denoted by *char* R.

Definition 2.3. Let $\mathbb{F}$ be a field. Any expression of the form $a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$ where $a_i \in \mathbb{F}$, $0 \leq i \leq n$, $n \in \mathbb{N} \cup \{0\}$, $a_n \neq 0$ is called a *polynomial* in x of degree n, with coefficients from $\mathbb{F}$.

We say that x is an *indeterminate* of a *variable*. The a_n is called the *leading coefficient* and a_0 is called a *constant term*.

The set of all polynomials over $\mathbb{F}$ is denoted by $\mathbb{F}[x]$. Two polynomials f and g from $\mathbb{F}[x]$ are said to be equal, if their degrees are equal and the respective coefficients are the same.

Let f and g be two polynomials from $\mathbb{F}[x]$ of n and m degrees, respectively. Then:

$$deg(f + g) \leq \text{Max}\{deg\ f, deg\ g\}$$

$$def(f \cdot g) = deg(f) + deg(g).$$

Let $\mathbb{F}$ be a field and $f \in \mathbb{F}[x]$ be a non constant polynomial. we say that f is *reducible* in $\mathbb{F}[x]$ if there exist two non constants polynomials $g, h \in \mathbb{F}[x]$ such that $f = g \cdot h$. Otherwise, f is called *irreducible* over $\mathbb{F}$.

Note that every polynomial over $\mathbb{F}$ of degree 1 is irreducible.

Theorem 2.4. For any field $\mathbb{F}$, a non-zero polynomial $f \in \mathbb{F}[x]$ with degree n has a most n roots in $\mathbb{F}$.

Theorem 2.5. *Fundamental theorem of algebra*

Every non-constant polynomial f over $\mathbb{C}$ has a root in $\mathbb{C}$.

Corollary 2.6. *Every non constant polynomial f over $\mathbb{C}$ of degree n has n roots in $\mathbb{C}$.*

Theorem 2.7. Let f be a polynomial over $\mathbb{R}$. Then f is reducible, or f is linear, or f is quadratic such that it has a negative discriminant.

Theorem 2.8. Let α be an *algebraic element* over a field $\mathbb{F}$, and let $p(x)$ be the *minimal polynomial* for α over $\mathbb{F}$. If $f(x) \in \mathbb{F}[x]$ and $f(\alpha) = 0$, then $p(x)$ divides $f(x)$ in $\mathbb{F}[x]$.

Theorem 2.9. *Let $f(x)$ be an irreducible polynomial over a field $\mathbb{F}$. If $\mathbb{F}$ has characteristic 0, then $f(x)$ has no multiple zeros.*

Definition 2.10. The *prime (base) subfield* of a field $\mathbb{F}$ is the subfield of $\mathbb{F}$ generated by the multiplicative identity 1_F of $\mathbb{F}$. It is (isomorphic to) either $\mathbb{Q}$ (if $ch(\mathbb{F}) = 0$) or $\mathbb{Z}_p($ if $ch(\mathbb{F}) = p$).

Example 2.11.

The prime subfield of $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ is $\mathbb{Q}$.

Definition 2.12. If $\mathbb{K}$ is a field containing the subfield $\mathbb{F}$, then $\mathbb{K}$ is said to be an *extension field* of $\mathbb{F}$.

Definition 2.13. If $\mathbb{F}$ is an extension field of $\mathbb{E}$, then $\mathbb{F}$ is a vector space over $\mathbb{E}$.

Definition 2.14. The *degree of a field extension* $\mathbb{K}$ *over* $\mathbb{F}$, denoted by $[\mathbb{K} : \mathbb{F}]$, is the dimension of $\mathbb{K}$ as a vector space over $\mathbb{F}$ (i.e $[\mathbb{K} : \mathbb{F}]$=$\dim_{\mathbb{F}} \mathbb{K}$). The extension is said to be finite if $[\mathbb{K} : \mathbb{F}] < \infty$.

Definition 2.15. Let $\mathbb{K}$ be an extension of the field $\mathbb{F}$, and let $\alpha, \beta, ... \in \mathbb{K}$ be a collection of elements of $\mathbb{K}$. Then the smallest subfield of $\mathbb{K}$ containing both $\mathbb{F}$ and the elements $\alpha, \beta, ...$ denoted by $\mathbb{F}(\alpha, \beta, ...)$ is called the *field generated by* $\alpha, \beta, ...$.

Definition 2.16. If the field $\mathbb{K}$ is generated by a single element α over $\mathbb{F}$, $\mathbb{K} = \mathbb{F}(\alpha)$, then $\mathbb{K}$ is said to be *a simple extension* of $\mathbb{F}$ and the element α is called a *primitive element* for the extension.

Definition 2.17. The element $\alpha \in \mathbb{K}$ is said to be *algebraic element* over $\mathbb{F}$, if α is a root of some non zero polynomial $f(x) \in \mathbb{F}[x]$. If α is not algebraic over $\mathbb{F}$, then it is said to be *transcendental* over $\mathbb{F}$.

Definition 2.18. An extension field $\mathbb{K}$ of a field $\mathbb{F}$ is said to be *an algebraic extension* if every element of $\mathbb{K}$ is algebraic over $\mathbb{F}$.

Definition 2.19. Let $\mathbb{E}$ be an extension field of a field $\mathbb{F}$. We say that $\mathbb{E}$ has *degree* n over $\mathbb{F}$ and write $[\mathbb{E} : \mathbb{F}] = n$, if $\mathbb{E}$ has dimension n as a vector space over $\mathbb{F}$. If $[\mathbb{E} : \mathbb{F}]$ is finite, $\mathbb{E}$ is called a finite extension of $\mathbb{F}$; otherwise, we say that $\mathbb{E}$ is an infinite extension of $\mathbb{F}$.

Example 2.20.

The field of complex numbers has degree 2 over the field of real numbers, $[\mathbb{C} : \mathbb{R}] = 2$, because $\{1, i\}$ is a basis.

The field of real numbers is an infinite extension over the field of rational numbers $[\mathbb{R} : \mathbb{Q}] = \infty$.

Theorem 2.21. *Let* $[\mathbb{F} : \mathbb{K}] = m$ *and* $[\mathbb{E} : \mathbb{F}] = n$*, where* $\mathbb{K} \subseteq \mathbb{F} \subseteq \mathbb{E}$ *(tower fields). Then,* $[\mathbb{E} : \mathbb{K}] = m \cdot n$.

Corollary 2.22. Let $\mathbb{K} \subseteq \mathbb{F} \subseteq \mathbb{E}$ be a tower fields, then, $[\mathbb{E} : \mathbb{K}] = \infty$ if and only if one of $[\mathbb{E} : \mathbb{F}] = \infty$ or $[\mathbb{F} : \mathbb{K}] = \infty$.

Theorem 2.23. *Every finite extension is algebraic.*

Definition 2.24. Let $a \in \mathbb{E}$ be an algebraic element over $\mathbb{F}$, then a satisfies a non constant polynomial $f \in \mathbb{F}[x]$. The set $\{g \in \mathbb{F}[x] : g(a) = 0\}$ is not empty and thus $\{deg(g) : g(a) = 0, g \in \mathbb{F}[x]\} \subseteq \mathbb{N}$ is a nonempty set. By well ordering principle, there is a polynomial $\overline{g} \in \mathbb{F}[x]$ such that $deg(\overline{g})$ is the least among all polynomials $g \in \mathbb{F}[x]$ satisfying $g(a) = 0$.

$\overline{g}$ is called the *minimal polynomial* of the element a over the field $\mathbb{F}$.

Corollary 2.25. *Any two minimal polynomials of an element a differ at most by a scalar multiple.*

Theorem 2.26.

A minimal polynomial of an element a in $\mathbb{E}$ over $\mathbb{F}$ is an irreducible polynomial over $\mathbb{F}$.

Conversely, Let f be an irreducible polynomial over $\mathbb{F}$ such that $f(a) = 0$, then f is a minimal polynomial.

Definition 2.27. If α is an algebraic element over $\mathbb{F}$, then the *degree of* α, is the degree of the minimal polynomial of α.

Theorem 2.28. The least field containing both $\mathbb{F}$ and algebraic element α of degree n, is a field denoted by $\mathbb{F}(\alpha)$.

$\mathbb{F}(\alpha) = \{a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} : \alpha_i \in \mathbb{F}\}$, where $[\mathbb{F}(\alpha) : \mathbb{F}] = n$.

Theorem 2.29. *Let $\mathbb{K} \subseteq \mathbb{F} \subseteq \mathbb{E}$ be a field tower. If $\mathbb{E}$ is an algebraic extension over $\mathbb{F}$, and $\mathbb{F}$ is an algebraic extension over $\mathbb{K}$. Then $\mathbb{E}$ is an algebraic extension over $\mathbb{K}$.*

Theorem 2.30. *Let $f \in \mathbb{F}[x]$ be an irreducible polynomial such that $\mathbb{Q} \subseteq \mathbb{F} \subseteq \mathbb{C}$, then f has no multiple roots. In other words, if f has multiple roots then it is reducible.*

Definition 2.31. Let $\mathbb{E}$ be an extension field of $\mathbb{F}$, and let $f(x) \in \mathbb{F}[x]$. We say that $f(x)$ *splits* in $\mathbb{E}$ if $f(x)$ can be factored as a product of linear factors in $\mathbb{E}[x]$. We call $\mathbb{E}$ a *splitting field* for $f(x)$ over $\mathbb{F}$ if $f(x)$ splits in $\mathbb{E}$ but in no proper subfield of $\mathbb{E}$.

Definition 2.32. A *separable* extension is an algebraic field extension $\mathbb{E}$ over $\mathbb{F}$, such that for every $\alpha \in \mathbb{E}$, the minimal polynomial of α over $\mathbb{F}$ is a separable polynomial, i.e all its roots are distinct. Otherwise, the extension is called *inseparable*.

Theorem 2.33. All algebraic extensions of $\mathbb{F}$, with *char* $\mathbb{F} = 0$, are *separable extensions.*

Chapter 3

Introductory Part

In this part, in the first section will recall the Primitive Element Theorem, its proof, and a remark about its uses in our research. After that, the second section will introduce two methods that we will use later in proving $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha + \beta)$. Moreover, the third section will include some basic results that are related to the dimension of $\mathbb{Q}(\sqrt{a + b\sqrt{p}})$ over $\mathbb{Q}$. These lemmas are widely used in the proof of the main theorems. The last section, will introduce one important lemma indicating the necessary condition for $\mathbb{Q}(\sqrt{a + b\sqrt{p}}) = \mathbb{Q}(\sqrt{a - b\sqrt{p}})$.

3.1 The Primitive Element Theorem.

The proofs of our main theorems depend on the Primitive Element Theorem. So, we will introduce its full proof, in addition to a remark about its application.

Theorem 3.1. *Primitive Element Theorem*

If $\mathbb{F}$ is a subfield of $\mathbb{C}$, and α and β are algebraic over $\mathbb{F}$, then there is an element γ in $\mathbb{F}(\alpha, \beta)$ such that $\mathbb{F}(\alpha, \beta) = \mathbb{F}(\gamma)$.

Proof. Let $p(x)$ and $q(x)$ be the minimal polynomials over $\mathbb{F}$ for α and β, respectively. Then in $\mathbb{C}$, let $\alpha_1, \alpha_2, ..., \alpha_m$ and $\beta_1, \beta_2, ..., \beta_n$ be all the distinct zeros of $p(x)$ and $q(x)$, respectively, where $\alpha = \alpha_1$ and $\beta = \beta_{\mathbf{1}}$. Note that the roots are distinct because of the irreducibility of polynomials over a numeric field $\mathbb{F}$ (Theorem 2.9).

Consider the finite set

$$C = \left\{ \frac{\alpha_i - \alpha}{\beta - \beta_j},\ i \geq 1 \text{ and } j > 1 \right\}.$$

Among the infinitely many elements of $\mathbb{F}$, choose an element $\eta \in \mathbb{F}$ that does not belong to the set C.

In particular,

$$\alpha_i \neq \alpha + \eta(\beta - \beta_j)$$

for $j > 1$ and $i \geq 1$.

We shall show that $\gamma = \alpha + \eta\beta$ has the property that $\mathbb{F}(\alpha, \beta) = \mathbb{F}(\gamma)$. Certainly, $\mathbb{F}(\gamma) \subseteq \mathbb{F}(\alpha, \beta)$. To verify that $\mathbb{F}(\alpha, \beta) \subseteq \mathbb{F}(\gamma)$, it suffices to prove that $\beta \in \mathbb{F}(\gamma)$, for then β, γ, and η belong to $\mathbb{F}(\gamma)$ and so $\alpha = \gamma - \eta\beta$ belongs there too. We will obtain this by proving that the minimal polynomial of β over $\mathbb{F}(\gamma)$ is linear.

Consider the polynomials $q(x)$ and $r(x) = p(\gamma - \eta x)$ over $\mathbb{F}(\gamma)$. Since $q(\beta) = 0$ and $r(\beta) = p(\gamma - \eta\beta) = p(\alpha) = 0$, both $q(x)$ and $r(x)$ are divisible by the minimal polynomial $s(x)$ for β over $\mathbb{F}(\gamma)$. Because $s(x) \in \mathbb{F}(\gamma)[x]$, we may complete the proof by proving that $s(x) = x - \beta$, which would show that $\beta \in \mathbb{F}(\gamma)$. Since $s(x)$ is a common divisor of $q(x)$ and $r(x)$, the only possible zeros of $s(x)$ in $\mathbb{C}$ are the zeros of $q(x)$ that are also zeros of $r(x)$. But $r(\beta_j) = p(\gamma - \eta\beta_j) = p(\alpha + \eta\beta - \eta\beta_j) = p(\alpha + \eta(\beta - \beta_j))$ and η was chosen such that $\alpha + \eta(\beta - \beta_j) \neq \alpha_i$ for $j > 1$. It follows that β is the only zero of $s(x)$ in $\mathbb{C}[x]$, and, therefore $s(x) = (x - \beta)^u$. Since $s(x)$ is irreducible and $\mathbb{F}$ has characteristic 0, then $u = 1$. So, $s(x) = x - \beta$.

□

Remark 3.2. Let $\mathbb{F}$ be a field of characteristic 0, and α and β are algebraic elements over $\mathbb{F}$.

Choose η to be any element in $\mathbb{F}$.

- If $\eta \notin$C, then $\mathbb{F}(\alpha, \beta) = \mathbb{F}(\alpha + \eta\beta)$ by the Primitive Element Theorem.

- If $\eta \in$C, then it is inconclusive.

3.2 How to prove $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha + \beta)$?

In this section, we will present two methods that will be used in proving $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha+\beta)$.

Proof by using Primitive Element Theorem

Since $\mathbb{Q}$ is a subfield of $\mathbb{C}$, and let α, β are two algebraic elements over $\mathbb{Q}$, then we can use the primitive element theorem to prove $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha + \beta)$. Consider the set C defined in the proof of the primitive element theorem. If we guarantee that $1 \notin$ C , then we are done. What will be the result if $1 \in$C? In this case, we still have a hope to prove the claim directly.

Proof directly

Since $\alpha + \beta \in \mathbb{Q}(\alpha, \beta)$, then $\mathbb{Q}(\alpha + \beta)$ is a subfield of $\mathbb{Q}(\alpha, \beta)$. Thus, we have the fields tower $\mathbb{Q} \subseteq \mathbb{Q}(\alpha + \beta) \subseteq \mathbb{Q}(\alpha, \beta)$.

Therefore, in order to prove that $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha+\beta)$, it is sufficient to have $[\mathbb{Q}(\alpha + \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$.

3.3 Some lemmas related to the dimension of $\mathbb{Q}(\sqrt{a+b\sqrt{p}})$ over $\mathbb{Q}$.

In this section, we present some results related to the dimension of $\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right)$ over $\mathbb{Q}$. Since the polynomial $x^4 - 2ax^2 + a^2 - pb^2$ has $\sqrt{a+b\sqrt{p}}$ one of its roots, then $\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right) : \mathbb{Q}\right] \leq 4$.

Lemma 3.3. For $a, b \neq 0$ rational numbers and p a prime number,

$$\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right) : \mathbb{Q}\right] \neq 1.$$

Proof. Assume that $\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right) : \mathbb{Q}\right] = 1$, then $\sqrt{a+b\sqrt{p}} = \alpha$, for $\alpha \in \mathbb{Q}$. Then,

$$a + b\sqrt{p} = \alpha^2$$

This contradicts with the assumption that $b \neq 0$ and p is a prime number.

□

Lemma 3.4. For $a, b \neq 0$ rational numbers and p a prime number,

$$\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right) : \mathbb{Q}\right] \neq 3.$$

Proof.

Assume that $\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right) : \mathbb{Q}\right] = 3$. Since $\sqrt{p} \in \mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right)$, then we have the fields tower

$$\mathbb{Q} \subset \mathbb{Q}\left(\sqrt{p}\right) \subseteq \mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right).$$

So,

$$\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right) : \mathbb{Q}\left(\sqrt{p}\right)\right] \cdot \left[\mathbb{Q}\left(\sqrt{p}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right) : \mathbb{Q}\right].$$

Since $\left[\mathbb{Q}\left(\sqrt{p}\right):\mathbb{Q}\right]=2$, and we assume that $\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\right]=3$, then

$$\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\left(\sqrt{p}\right)\right]=\frac{3}{2} \text{ which is contradiction.}$$

Therefore,

$$\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\right]\neq 3.$$

□

The above two lemmas guaranteed under their assumptions that $\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\right]$ is 2 or 4. The coming lemmas will present under what conditions $\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\right]$ is 2 or 4.

Lemma 3.5. Let $a,b\neq 0$ be rational numbers and p a prime number.
If $\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\right]=2$, then $\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right)=\mathbb{Q}\left(\sqrt{p}\right)$.

Proof. The minimal polynomial of $\sqrt{p}$ over $\mathbb{Q}$ is x^2-p, so $\left[\mathbb{Q}\left(\sqrt{p}\right):\mathbb{Q}\right]=2$.

Since $\sqrt{p}\in\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right)$, then $\mathbb{Q}\left(\sqrt{p}\right)$ is a subfield of $\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right)$, and

$$\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\left(\sqrt{p}\right)\right]\cdot\left[\mathbb{Q}\left(\sqrt{p}\right):\mathbb{Q}\right]=\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\right].$$

Thus, $\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\left(\sqrt{p}\right)\right]=1$.

Therefore,

$$\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right)=\mathbb{Q}\left(\sqrt{p}\right).$$

□

Lemma 3.6. For any rational numbers a and $b\neq 0$, and a prime number p:

$\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\right]=2$ if and only if $\sqrt{\frac{a+\sqrt{a^2-pb^2}}{2p}}\in\mathbb{Q}$ *or* $\sqrt{\frac{a-\sqrt{a^2-pb^2}}{2p}}\in\mathbb{Q}$.

Proof. Assume that $\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\right]=2$, then by Lemma 3.5,

$$\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right)=\mathbb{Q}\left(\sqrt{p}\right),$$

So,

$$\sqrt{a+b\sqrt{p}}=\alpha+\beta\sqrt{p} \text{ for some rational numbers } \alpha,\beta.$$

By squaring both sides, we get

$$a+b\sqrt{p}=\alpha^2+2\alpha\beta\sqrt{p}+p\beta^2$$

Thus,

$$a=\alpha^2+p\beta^2 \text{ and } b=2\alpha\beta.$$

It follows that

$$b^2=(2\alpha\beta)^2=4\alpha^2\beta^2=4(a-p\beta^2)\beta^2$$

By rearranging this fourth degree equation in β we will get:

$$4p\beta^4-4a\beta^2+b^2=0$$

Its solution is

$$\beta=\pm\sqrt{\frac{a\pm\sqrt{a^2-pb^2}}{2p}}$$

Since β is a rational number, we conclude that at least one of $\sqrt{\frac{a+\sqrt{a^2-pb^2}}{2p}}$ and $\sqrt{\frac{a-\sqrt{a^2-pb^2}}{2p}}$ is rational.

Conversely, let us assume that $\sqrt{\frac{a+\sqrt{a^2-pb^2}}{2p}}\in\mathbb{Q}$, the proof for the other case is

similar.

We have

$$a+b\sqrt{p}=(a+b\sqrt{p})\cdot\left(\frac{2\left(a+\sqrt{a^2-pb^2}\right)}{2\left(a+\sqrt{a^2-pb^2}\right)}\right)$$

$$=\frac{2a^2+2ab\sqrt{p}+2a\sqrt{a^2-pb^2}+2b\sqrt{p}\sqrt{a^2-pb^2}}{2\left(a+\sqrt{a^2-pb^2}\right)}$$

By adding and subtracting pb^2 in the numerator, we get

$$=\frac{2a^2+2ab\sqrt{p}+2a\sqrt{a^2-pb^2}+2b\sqrt{p}\sqrt{a^2-pb^2}+(pb^2-pb^2)}{2\left(a+\sqrt{a^2-pb^2}\right)}$$

$$=\frac{pb^2+2b\sqrt{p}\left(a+\sqrt{a^2-pb^2}\right)+\left(a+\sqrt{a^2-pb^2}\right)^2}{2\left(a+\sqrt{a^2-pb^2}\right)}$$

$$=\frac{b^2}{2}\cdot\frac{p}{a+\sqrt{a^2-pb^2}}+b\sqrt{p}+\frac{a+\sqrt{a^2-pb^2}}{2}$$

$$=\left(\frac{b}{2}\cdot\sqrt{\frac{2p}{a+\sqrt{a^2-pb^2}}}+\sqrt{p}\cdot\sqrt{\frac{a+\sqrt{a^2-pb^2}}{2p}}\right)^2.$$

Thus,

$$\sqrt{a+b\sqrt{p}}=\pm\left(\frac{b}{2}\cdot\sqrt{\frac{2p}{a+\sqrt{a^2-pb^2}}}+\sqrt{p}\cdot\sqrt{\frac{a+\sqrt{a^2-pb^2}}{2p}}\right)=\alpha+\beta\sqrt{p}$$

Where $\alpha=\pm\frac{b}{2}\cdot\sqrt{\frac{2p}{a+\sqrt{a^2-pb^2}}}$ and $\beta=\pm\sqrt{\frac{a+\sqrt{a^2-pb^2}}{2p}}$.

Using the assumption $\sqrt{\frac{a+\sqrt{a^2-pb^2}}{2p}}$ is a rational number, we conclude that $\alpha,\beta\in\mathbb{Q}$, and thus

$$\sqrt{a+b\sqrt{p}}\in\mathbb{Q}\left(\sqrt{p}\right)$$

Therefore

$$\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\right]=2.$$

□

Lemma 3.7. For $a, b \neq 0$ rational numbers and p a prime number,

$\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\right]=4$ if and only if $\sqrt{\frac{a+\sqrt{a^2-pb^2}}{2p}} \notin \mathbb{Q}$ *and* $\sqrt{\frac{a-\sqrt{a^2-pb^2}}{2p}} \notin \mathbb{Q}$.

Proof. Assume that $\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\right]=4$, then $\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\right]\neq 2$, so by Lemma 3.6,

$$\sqrt{\frac{a+\sqrt{a^2-pb^2}}{2p}} \notin \mathbb{Q} \text{ and } \sqrt{\frac{a-\sqrt{a^2-pb^2}}{2p}} \notin \mathbb{Q}.$$

Conversely, since $\sqrt{\frac{a+\sqrt{a^2-pb^2}}{2p}} \notin \mathbb{Q}$ and $\sqrt{\frac{a-\sqrt{a^2-pb^2}}{2p}} \notin \mathbb{Q}$, then by Lemma 3.6,

$$\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\right]\neq 2.$$

Moreover, $\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\right]$ does not equal to 1 or 3, by lemmas 3.3 and 3.4.

But $\sqrt{a+b\sqrt{p}}$ satisfies a fourth degree polynomial $x^4-2ax^2+a^2-pb^2$.

Therefore

$$\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\right]=4$$

□

The following two lemmas are direct results from the lemma. These will help the reader easily to determine the dimension of $\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right)$ over $\mathbb{Q}$.

Lemma 3.8. Let $a, b \neq 0$ be rational numbers and p a prime number.

If $\sqrt{a^2-pb^2} \notin \mathbb{Q}$, then $\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\right]=4$.

Proof. If $\sqrt{a^2-pb^2} \notin \mathbb{Q}$, we will show that both $\sqrt{\frac{a \pm \sqrt{a^2-pb^2}}{2p}} \notin \mathbb{Q}$, and by Lemma 3.7, we will conclude that $\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\right]=4$.

Assume that at least one of $\sqrt{\frac{a \pm \sqrt{a^2-pb^2}}{2p}} \in \mathbb{Q}$, then $\frac{a \pm \sqrt{a^2-pb^2}}{2p} \in \mathbb{Q}$, and thus $\sqrt{a^2-pb^2} \in \mathbb{Q}$, contradiction.

□

Lemma 3.9. Let $a, b \neq 0$ be rational numbers and p a prime number.

If $a<0$, then $\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\right]=4$.

Proof. Since $b \neq 0$, then $a^2 > a^2-pb^2$, and thus $|a| > \sqrt{a^2-pb^2}$.

- If $\sqrt{a^2-pb^2} \notin \mathbb{Q}$, then both of $\sqrt{\frac{a \pm \sqrt{a^2-pb^2}}{2p}} \notin \mathbb{Q}$.
- If $\sqrt{a^2-pb^2} \in \mathbb{Q}$, so by using the assumption that $a<0$, we get

$$\frac{a \pm \sqrt{a^2-pb^2}}{2p} < 0$$

This means that both

$$\sqrt{\frac{a \pm \sqrt{a^2-pb^2}}{2p}} \notin \mathbb{Q}$$

Therefore, in the above two cases, by Lemma 3.7 we conclude

$$\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\right]=4.$$

□

3.4 Under what condition $\mathbb{Q}(\sqrt{a+b\sqrt{p}}) = \mathbb{Q}(\sqrt{a-b\sqrt{p}})$?

In this section, we will present the necessary condition for $\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right) = \mathbb{Q}\left(\sqrt{a-b\sqrt{p}}\right)$. This lemma is widely used in the proofs of the main results in the main part.

Lemma 3.10. For any rational numbers a, $b \neq 0$, and prime p,

If $a^2 - pb^2 = \begin{cases} m^2 \\ \underline{or} \\ pm^2 \end{cases}$, where m is a rational number, then $\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right) = \mathbb{Q}\left(\sqrt{a-b\sqrt{p}}\right)$.

Proof.

Case 1 Assume $a^2 - pb^2 = m^2$.

Since $\sqrt{a+b\sqrt{p}} \in \mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right)$, so $\dfrac{1}{\sqrt{a+b\sqrt{p}}} \in \mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right)$. Then,

$$\frac{\sqrt{a-b\sqrt{p}}}{m} = \frac{\sqrt{a-b\sqrt{p}}}{\sqrt{a^2-pb^2}} = \frac{1}{\sqrt{a+b\sqrt{p}}} \cdot \frac{\sqrt{a-b\sqrt{p}}}{\sqrt{a-b\sqrt{p}}} = \frac{1}{\sqrt{a+b\sqrt{p}}} \in \mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right)$$

Thus

$$\sqrt{a-b\sqrt{p}} \in \mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right)$$

$$\mathbb{Q}\left(\sqrt{a-b\sqrt{p}}\right) \subseteq \mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right).$$

Similarly, since $\sqrt{a-b\sqrt{p}} \in \mathbb{Q}\left(\sqrt{a-b\sqrt{p}}\right)$, so $\dfrac{1}{\sqrt{a-b\sqrt{p}}} \in \mathbb{Q}\left(\sqrt{a-b\sqrt{p}}\right)$. Then,

$$\frac{\sqrt{a+b\sqrt{p}}}{m} = \frac{\sqrt{a+b\sqrt{p}}}{\sqrt{a^2-pb^2}} = \frac{1}{\sqrt{a-b\sqrt{p}}} \cdot \frac{\sqrt{a+b\sqrt{p}}}{\sqrt{a+b\sqrt{p}}} = \frac{1}{\sqrt{a-b\sqrt{p}}} \in \mathbb{Q}\left(\sqrt{a-b\sqrt{p}}\right)$$

Thus

$$\sqrt{a+b\sqrt{p}} \in \mathbb{Q}\left(\sqrt{a-b\sqrt{p}}\right)$$

$$\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right) \subseteq \mathbb{Q}\left(\sqrt{a-b\sqrt{p}}\right).$$

Therefore, $\mathbb{Q}\left(\sqrt{a-b\sqrt{p}}\right) = \mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right)$.

Case 2 Assume $a^2 - pb^2 = pm^2$.

Since $\sqrt{a+b\sqrt{p}} \in \mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right)$, so $\dfrac{1}{\sqrt{a+b\sqrt{p}}} \in \mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right)$. Then,

$$\frac{\sqrt{a-b\sqrt{p}}}{m\sqrt{p}} = \frac{\sqrt{a-b\sqrt{p}}}{\sqrt{a^2-pb^2}} = \frac{1}{\sqrt{a+b\sqrt{p}}} \cdot \frac{\sqrt{a-b\sqrt{p}}}{\sqrt{a-b\sqrt{p}}} = \frac{1}{\sqrt{a+b\sqrt{p}}} \in \mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right)$$

But $\sqrt{p} \in \mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right)$, so

$$\sqrt{a-b\sqrt{p}} \in \mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right)$$

$$\mathbb{Q}\left(\sqrt{a-b\sqrt{p}}\right) \subseteq \mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right).$$

Similarly, since $\sqrt{a-b\sqrt{p}} \in \mathbb{Q}\left(\sqrt{a-b\sqrt{p}}\right)$, so $\dfrac{1}{\sqrt{a-b\sqrt{p}}} \in \mathbb{Q}\left(\sqrt{a-b\sqrt{p}}\right)$. Then,

$$\frac{\sqrt{a+b\sqrt{p}}}{m\sqrt{p}} = \frac{\sqrt{a+b\sqrt{p}}}{\sqrt{a^2-pb^2}} = \frac{1}{\sqrt{a-b\sqrt{p}}} \cdot \frac{\sqrt{a+b\sqrt{p}}}{\sqrt{a+b\sqrt{p}}} = \frac{1}{\sqrt{a-b\sqrt{p}}} \in \mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right)$$

But $\sqrt{p} \in \mathbb{Q}\left(\sqrt{a-b\sqrt{p}}\right)$, so

$$\sqrt{a+b\sqrt{p}} \in \mathbb{Q}\left(\sqrt{a-b\sqrt{p}}\right)$$

$$\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right) \subseteq \mathbb{Q}\left(\sqrt{a-b\sqrt{p}}\right).$$

Therefore, $\mathbb{Q}\left(\sqrt{a-b\sqrt{p}}\right) = \mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right)$.

□

Chapter 4

Main part

The main part includes four sections.

The first section will present an important result that will be used in the proof of the main results. It states that, for any non zero rational numbers α, β, δ and η, such that $\sqrt{\delta} \notin \mathbb{Q}$ and $\sqrt{\eta} \notin \mathbb{Q}$,

$$\mathbb{Q}\left(\alpha\sqrt{\delta}, \beta\sqrt{\eta}\right) = \mathbb{Q}\left(\alpha\sqrt{\delta} + \beta\sqrt{\eta}\right).$$

The second section includes some lemmas in its first subsection that will help in understanding the proof of the first main theorem (Theorem 4.10), which states that

$$\mathbb{Q}\left(\sqrt{a + b\sqrt{p}}, \sqrt{q}\right) = \mathbb{Q}\left(\sqrt{a + b\sqrt{p}} + \sqrt{q}\right)$$

for every $a, b \neq 0 \in \mathbb{Q}$ and p, q are any prime numbers.

Similarly, the third section includes some lemmas also in its first subsection that will help in understanding the proof of the second main theorem (Theorem 4.18), which states that:

If $a \neq c$ or $b \neq -d$ such that $a \pm \sqrt{a^2 - pb^2} \neq c \pm \sqrt{c^2 - pd^2}$, then

$$\mathbb{Q}\left(\sqrt{a + b\sqrt{p}}, \sqrt{c + d\sqrt{p}}\right) = \mathbb{Q}\left(\sqrt{a + b\sqrt{p}} + \sqrt{c + d\sqrt{p}}\right).$$

Finally, in the fourth section, we negate the necessary conditions $a \neq c$ or $b \neq -d$ of the second main theorem, and the results will be presented in Theorems 4.21, 4.23, 4.25 and 4.27.

4.1 The case $\mathbb{Q}\left(\alpha\sqrt{\delta}, \beta\sqrt{\eta}\right) = \mathbb{Q}\left(\alpha\sqrt{\delta} + \beta\sqrt{\eta}\right)$

In this section, we will study under what conditions $\mathbb{Q}\left(\alpha\sqrt{\delta}, \beta\sqrt{\eta}\right)$ and $\mathbb{Q}\left(\alpha\sqrt{\delta} + \beta\sqrt{\eta}\right)$ are equal, such that $\alpha, \beta, \delta, \eta \in \mathbb{Q}$, both of $\sqrt{\delta}$ and $\sqrt{\eta}$ are not rational numbers.

First of all, we will introduce a basic lemma that will help us in developing the proofs of the coming theorems in the later sections.

Lemma 4.1. For any rational numbers α, β and x,

$$\mathbb{Q}\left(\alpha + \beta\sqrt{x}\right) = \mathbb{Q}\left(\sqrt{x}\right).$$

Proof. Since α, β and $\sqrt{x}$ all lie in $\mathbb{Q}(\sqrt{x})$, then $\alpha + \beta\sqrt{x} \in \mathbb{Q}\left(\sqrt{x}\right)$,

$$\mathbb{Q}\left(\alpha + \beta\sqrt{x}\right) \subseteq \mathbb{Q}\left(\sqrt{x}\right).$$

On the other hand, since the field $\mathbb{Q}\left(\alpha + \beta\sqrt{x}\right)$ contains $\alpha + \beta\sqrt{x}$, and the rational numbers α and $\dfrac{1}{\beta}$, then

$$\sqrt{x} = \frac{1}{\beta}\left(\alpha + \beta\sqrt{x} - \alpha\right)$$

$$\mathbb{Q}\left(\sqrt{x}\right) \subseteq \mathbb{Q}\left(\alpha + \beta\sqrt{x}\right).$$

□

Theorem 4.2. *For any non zero rational numbers α, β, δ and η, such that $\sqrt{\delta} \notin \mathbb{Q}$ and $\sqrt{\eta} \notin \mathbb{Q}$,*

$$\mathbb{Q}\left(\alpha\sqrt{\delta}, \beta\sqrt{\eta}\right) = \mathbb{Q}\left(\alpha\sqrt{\delta} + \beta\sqrt{\eta}\right).$$

Proof. The minimal polynomial over $\mathbb{Q}$ for $\alpha\sqrt{\delta}$ is $x^2 - \delta\alpha^2$. Its roots are $x_1 = \alpha\sqrt{\delta}$ and $x_2 = -\alpha\sqrt{\delta}$.

The minimal polynomial over $\mathbb{Q}$ for $\beta\sqrt{\eta}$ is $x^2 - \eta\beta^2$. Its roots are $x_3 = \beta\sqrt{\eta}$ and $x_4 = -\beta\sqrt{\eta}$.

Consider the finite set C defined in the proof of the primitive element theorem.

$$C = \left\{ \frac{x_1 - x_2}{x_3 - x_4}, \frac{x_1 - x_2}{x_4 - x_3} \right\}.$$

We will suppose that $1 \in$ C, then 1 will be equal to at least one of the elements of the finite set C. Thus, we will have the finite set of equations: $\left\{ \alpha\sqrt{\delta} = \beta\sqrt{\eta}, \alpha\sqrt{\delta} = -\beta\sqrt{\eta} \right\}$, that are equivalent to $\delta = \dfrac{\beta^2 \cdot \eta}{\alpha^2}$. Note that if $\delta \neq \dfrac{\beta^2 \cdot \eta}{\alpha^2}$, then $1 \notin$ C by contrapositive.

We will consider two cases in proving $\mathbb{Q}\left(\alpha\sqrt{\delta}, \beta\sqrt{\eta}\right) = \mathbb{Q}\left(\alpha\sqrt{\delta} + \beta\sqrt{\eta}\right)$.

Case 1: The case $\delta \neq \dfrac{\beta^2 \cdot \eta}{\alpha^2}$:

Since $\delta \neq \dfrac{\beta^2 \cdot \eta}{\alpha^2}$, then by contrapositive we get that $1 \notin$ C, and thus by the primitive element theorem we get $\mathbb{Q}\left(\alpha\sqrt{\delta}, \beta\sqrt{\eta}\right) = \mathbb{Q}\left(\alpha\sqrt{\delta} + \beta\sqrt{\eta}\right)$.

Case 2: The case $\delta = \dfrac{\beta^2 \cdot \eta}{\alpha^2}$:

$$\begin{aligned}
\mathbb{Q}\left(\alpha\sqrt{\delta}, \beta\sqrt{\eta}\right) &= \mathbb{Q}\left(\alpha\sqrt{\frac{\beta^2 \cdot \eta}{\alpha^2}}, \beta\sqrt{\eta}\right) \\
&= \mathbb{Q}\left(\alpha \cdot \left(\pm\frac{\beta}{\alpha}\sqrt{\eta}\right), \beta\sqrt{\eta}\right) \\
&= \mathbb{Q}\left(\pm\beta\sqrt{\eta}, \beta\sqrt{\eta}\right) = \mathbb{Q}\left(\beta\sqrt{\eta}\right) \\
&= \mathbb{Q}\left(2\beta\sqrt{\eta}\right) \\
&= \mathbb{Q}\left(\beta\sqrt{\eta} + \beta\sqrt{\eta}\right) \\
&= \mathbb{Q}\left(\alpha\sqrt{\frac{\eta\beta^2}{\alpha^2}} + \beta\sqrt{\eta}\right) \\
&= \mathbb{Q}\left(\alpha\sqrt{\delta} + \beta\sqrt{\eta}\right)
\end{aligned}$$

Therefore, in both cases we conclude that:

$$\mathbb{Q}\left(\alpha\sqrt{\delta}, \beta\sqrt{\eta}\right) = \mathbb{Q}\left(\alpha\sqrt{\delta} + \beta\sqrt{\eta}\right).$$

□

Note that δ and η in Theorem 4.2 are not necessarily positive rational numbers.

The following examples are direct applications for the previous theorem.

Example 4.3. $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) = \mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right)$.

Example 4.4. $\mathbb{Q}\left(\sqrt{-2}, \sqrt{3}\right) = \mathbb{Q}\left(\sqrt{-2} + \sqrt{3}\right)$.

Example 4.5. $\mathbb{Q}\left(\sqrt{-2}, \sqrt{-3}\right) = \mathbb{Q}\left(\sqrt{-2} + \sqrt{-3}\right)$.

4.2 The case $\mathbb{Q}\left(\sqrt{a+b\sqrt{p}},\sqrt{q}\right)=\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}+\sqrt{q}\right)$

In the first subsection, we will introduce three useful lemmas that help in proving Theorem 4.9. This theorem plays a great role in proving the fist main theorem (Theorem 4.10).

The second section includes the first main theorem (Theorem 4.10) in our research, in addition to its complete proof.

Some useful lemmas.

Lemma 4.6. Let $a,b\neq 0,\alpha,\beta,m$ be rational numbers and p a prime number such that $\alpha^2\neq\beta^2$ and $m=\sqrt{a^2-pb^2}\in\mathbb{Q}$.

If $\left[\mathbb{Q}\left(\alpha\sqrt{a+b\sqrt{p}}+\beta\sqrt{a-b\sqrt{p}}\right):\mathbb{Q}\right]=2$, then

$$\mathbb{Q}\left(\alpha\sqrt{a+b\sqrt{p}}+\beta\sqrt{a-b\sqrt{p}}\right)=\mathbb{Q}\left(\sqrt{p}\right).$$

Proof. The minimal polynomial of $\sqrt{p}$ over $\mathbb{Q}$ is x^2-p, so $\left[\mathbb{Q}\left(\sqrt{p}\right):\mathbb{Q}\right]=2$.
Claim: $\sqrt{p}\in\mathbb{Q}\left(\alpha\sqrt{a+b\sqrt{p}}+\beta\sqrt{a-b\sqrt{p}}\right)$.
Proof: Let $\psi=\alpha\sqrt{a+b\sqrt{p}}+\beta\sqrt{a-b\sqrt{p}}$. Then

$$\psi^2=\alpha^2\left(a+b\sqrt{p}\right)+2\alpha\beta\sqrt{a^2-pb^2}+\beta^2\left(a-b\sqrt{p}\right)$$

$$\psi^2-a\left(\alpha^2+\beta^2\right)-2\alpha\beta m=b\sqrt{p}\left(\alpha^2-\beta^2\right).$$

Since $m\in\mathbb{Q}$, $\alpha^2-\beta^2\neq 0$, and $\left[\mathbb{Q}\left(\psi\right):\mathbb{Q}\right]=2$, then

$$\sqrt{p}\in\mathbb{Q}\left(\psi\right),$$

$$\sqrt{p}\in\mathbb{Q}\left(\alpha\sqrt{a+b\sqrt{p}}+\beta\sqrt{a-b\sqrt{p}}\right).$$

■

Therefore, $\mathbb{Q}\left(\sqrt{p}\right)$ is a subfield of $\mathbb{Q}\left(\alpha\sqrt{a+b\sqrt{p}}+\beta\sqrt{a-b\sqrt{p}}\right)$, and

$$\left[\mathbb{Q}\left(\alpha\sqrt{a+b\sqrt{p}}+\beta\sqrt{a-b\sqrt{p}}\right):\mathbb{Q}\left(\sqrt{p}\right)\right]\cdot\left[\mathbb{Q}\left(\sqrt{p}\right):\mathbb{Q}\right]=\left[\mathbb{Q}\left(\alpha\sqrt{a+b\sqrt{p}}+\beta\sqrt{a-b\sqrt{p}}\right):\mathbb{Q}\right]$$

Thus, $\left[\mathbb{Q}\left(\alpha\sqrt{a+b\sqrt{p}}+\beta\sqrt{a-b\sqrt{p}}\right):\mathbb{Q}\left(\sqrt{p}\right)\right]=1$.

We conclude that

$$\mathbb{Q}\left(\alpha\sqrt{a+b\sqrt{p}}+\beta\sqrt{a-b\sqrt{p}}\right)=\mathbb{Q}\left(\sqrt{p}\right).$$

□

Lemma 4.7. For $a,\ b\neq 0$ rational numbers and p a prime number such that $m=\sqrt{a^2-pb^2}\in\mathbb{Q}$,

$$\left[\mathbb{Q}\left(3\sqrt{a+b\sqrt{p}}-\sqrt{a-b\sqrt{p}}\right):\mathbb{Q}\right]=2 \text{ if and only if } \sqrt{\frac{2\left(a+\sqrt{a^2-pb^2}\right)}{p}}\in\mathbb{Q} \text{ or } \sqrt{\frac{2\left(a-\sqrt{a^2-pb^2}\right)}{p}}\in\mathbb{Q}.$$

and

$$\left[\mathbb{Q}\left(3\sqrt{a+b\sqrt{p}}+\sqrt{a-b\sqrt{p}}\right):\mathbb{Q}\right]=2 \text{ if and only if } \sqrt{\frac{2\left(a+\sqrt{a^2-pb^2}\right)}{p}}\in\mathbb{Q} \text{ or } \sqrt{\frac{2\left(a-\sqrt{a^2-pb^2}\right)}{p}}\in\mathbb{Q}.$$

Proof.

We will prove the first part of the lemma, and then the second part can be proved by the same argument.

$\left[\mathbb{Q}\left(3\sqrt{a+b\sqrt{p}}-\sqrt{a-b\sqrt{p}}\right):\mathbb{Q}\right]=2$ if and only if $\sqrt{\frac{2\left(a+\sqrt{a^2-pb^2}\right)}{p}}\in\mathbb{Q}$ or $\sqrt{\frac{2\left(a-\sqrt{a^2-pb^2}\right)}{p}}\in\mathbb{Q}$

Assume that $\left[\mathbb{Q}\left(3\sqrt{a+b\sqrt{p}}-\sqrt{a-b\sqrt{p}}\right):\mathbb{Q}\right]=2$, then by lemma 4.6,

$$\mathbb{Q}\left(3\sqrt{a+b\sqrt{p}}-\sqrt{a-b\sqrt{p}}\right)=\mathbb{Q}\left(\sqrt{p}\right)$$

So,

$$3\sqrt{a+b\sqrt{p}}-\sqrt{a-b\sqrt{p}}=\alpha+\beta\sqrt{p} \text{ for some rational numbers } \alpha,\ \beta$$

By squaring both sides, we get

$$9\left(a+b\sqrt{p}\right)-6\left(\sqrt{a^2-pb^2}\right)+\left(a-b\sqrt{p}\right)=\alpha^2+2\alpha\beta\sqrt{p}+p\beta^2$$
$$10a+8b\sqrt{p}-6m=\alpha^2+2\alpha\beta\sqrt{p}+p\beta^2.$$

By comparing the coefficients of $\left\{1,\sqrt{p}\right\}$, we get

$$10a-6m=\alpha^2+p\beta^2 \text{ and } 4b=\alpha\beta$$

It follows that

$$16b^2=(4b)^2=(\alpha\beta)^2=\alpha^2\beta^2=(10a-6m-p\beta^2)\beta^2$$

By rearranging this fourth degree equation in β we will get:

$$p\beta^4+\beta^2(6m-10a)+16b^2=0$$

Then,

$$\begin{aligned}\triangle_{\beta^2}&=(6m-10a)^2-4(p)(16b^2)\\&=36m^2-120am+100a^2-64pb^2\\&=36(a^2-pb^2)-120am+100a^2-64pb^2\\&=100\left(a^2-pb^2\right)-120am+36a^2\\&=(10m-6a)^2\end{aligned}$$

So,

$$\beta^2=\frac{-(6m-10a)\pm\sqrt{(10m-6a)^2}}{2p}$$

$$\beta^2 = \frac{10a - 6m \pm (10m - 6a)}{2p}$$

Therefore,

$$\beta_1 = \pm\sqrt{\frac{2(a+m)}{p}}\ ,\ \beta_2 = \pm 2\sqrt{\frac{2(a-m)}{p}}.$$

Since β is a rational number, we conclude that at least one of $\sqrt{\frac{2(a+\sqrt{a^2-pb^2})}{p}}$ and $\sqrt{\frac{2(a-\sqrt{a^2-pb^2})}{p}}$ is a rational number.

Conversely, suppose that $\beta = \sqrt{\frac{2(a+\sqrt{a^2-pb^2})}{p}}$ is a rational number, and

$$\alpha = \frac{4b}{\beta} = \frac{4b\sqrt{p}}{\sqrt{2(a+\sqrt{a^2-pb^2})}} \in \mathbb{Q}. \tag{4.1}$$

So, we have

$$\begin{aligned}
\alpha^2 + p\beta^2 &= \frac{16b^2p}{2(a+\sqrt{a^2-pb^2})} + p \cdot \frac{2(a+\sqrt{a^2-pb^2})}{p} \\
&= \frac{16b^2p + 4\left(a+\sqrt{a^2-pb^2}\right)^2}{2(a+\sqrt{a^2-pb^2})} \\
&= \frac{16b^2p + 4\left(a^2+2a\sqrt{a^2-pb^2}+a^2-pb^2\right)}{2(a+\sqrt{a^2-pb^2})} \\
&= \frac{16b^2p + 8a^2 - 4pb^2 + 8a\sqrt{a^2-pb^2}}{2(a+\sqrt{a^2-pb^2})} \\
&= \frac{6b^2p + 4a^2 + 4a\sqrt{a^2-pb^2}}{(a+\sqrt{a^2-pb^2})} \\
&= \frac{\left(10a - 6\sqrt{a^2-pb^2}\right)\left(a+\sqrt{a^2-pb^2}\right)}{(a+\sqrt{a^2-pb^2})} \\
&= 10a - 6\sqrt{a^2-pb^2}
\end{aligned}$$

Then, adding $8b\sqrt{p}$ on both sides, we get

$$10a - 6\sqrt{a^2-pb^2} + 8b\sqrt{p} = \alpha^2 + p\beta^2 + 8b\sqrt{p}$$

But $8b\sqrt{p} = 2\alpha\beta\sqrt{p}$ using equation 4.1, so

$$\begin{aligned}
10a - 6\sqrt{a^2-pb^2} + 8b\sqrt{p} &= \alpha^2 + p\beta^2 + 2\alpha\beta\sqrt{p} \\
9\left(a+b\sqrt{p}\right) - 6\sqrt{a^2-pb^2} + \left(a-b\sqrt{p}\right) &= \left(\alpha+\beta\sqrt{p}\right)^2 \\
\left(3\sqrt{a+b\sqrt{p}} - \sqrt{a-b\sqrt{p}}\right)^2 &= \left(\alpha+\beta\sqrt{p}\right)^2
\end{aligned}$$

Therefore,

$$3\sqrt{a+b\sqrt{p}} - \sqrt{a-b\sqrt{p}} = \pm\left(\alpha+\beta\sqrt{p}\right)$$

We conclude that $\left[\mathbb{Q}\left(3\sqrt{a+b\sqrt{p}} - \sqrt{a-b\sqrt{p}}\right) : \mathbb{Q}\right] = 2$.

By similar argument, if $\beta = 2\sqrt{\dfrac{2(a-\sqrt{a^2-pb^2})}{p}}$ is a rational number, then

$$3\sqrt{a+b\sqrt{p}} - \sqrt{a-b\sqrt{p}} = \pm(\alpha+\beta\sqrt{p})$$

We conclude that $\left[\mathbb{Q}\left(3\sqrt{a+b\sqrt{p}} - \sqrt{a-b\sqrt{p}}\right) : \mathbb{Q}\right] = 2$.

□

Lemma 4.8. Let $a, b \neq 0$ be rational numbers and p a prime number, such that $m = \sqrt{a^2-pb^2} \in \mathbb{Q}$.

$\left[\mathbb{Q}\left(3\sqrt{a+b\sqrt{p}} - \sqrt{a-b\sqrt{p}}\right) : \mathbb{Q}\right] = 4$ if and only if $\sqrt{\dfrac{2\left(a+\sqrt{a^2-pb^2}\right)}{p}} \notin \mathbb{Q}$ and $\sqrt{\dfrac{2\left(a-\sqrt{a^2-pb^2}\right)}{p}} \notin \mathbb{Q}$

and

$\left[\mathbb{Q}\left(3\sqrt{a+b\sqrt{p}} + \sqrt{a-b\sqrt{p}}\right) : \mathbb{Q}\right] = 4$ if and only if $\sqrt{\dfrac{2\left(a+\sqrt{a^2-pb^2}\right)}{p}} \notin \mathbb{Q}$ and $\sqrt{\dfrac{2\left(a-\sqrt{a^2-pb^2}\right)}{p}} \notin \mathbb{Q}$

Proof. We will prove the first part of the lemma, and the second part can be proved by similar argument.

$[\mathbb{Q}(3\sqrt{a+b\sqrt{p}} - \sqrt{a-b\sqrt{p}}) : \mathbb{Q}] = 4$ if and only if $\sqrt{\frac{2\left(a+\sqrt{a^2-pb^2}\right)}{p}} \notin \mathbb{Q}$ and $\sqrt{\frac{2\left(a-\sqrt{a^2-pb^2}\right)}{p}} \notin \mathbb{Q}$

Assume that $\left[\mathbb{Q}\left(3\sqrt{a+b\sqrt{p}} - \sqrt{a-b\sqrt{p}}\right) : \mathbb{Q}\right] = 4$, then by lemma 4.7, we conclude that

$$\sqrt{\frac{2\left(a+\sqrt{a^2-pb^2}\right)}{p}} \notin \mathbb{Q} \text{ and } \sqrt{\frac{2\left(a-\sqrt{a^2-pb^2}\right)}{p}} \notin \mathbb{Q}.$$

Conversely, since $\sqrt{\dfrac{2\left(a+\sqrt{a^2-pb^2}\right)}{p}} \notin \mathbb{Q}$ and $\sqrt{\dfrac{2\left(a-\sqrt{a^2-pb^2}\right)}{p}} \notin \mathbb{Q}$, then by lemma 4.7,

$$\left[\mathbb{Q}\left(3\sqrt{a+b\sqrt{p}} - \sqrt{a-b\sqrt{p}}\right) : \mathbb{Q}\right] \neq 2.$$

Moreover, $\left[\mathbb{Q}\left(3\sqrt{a+b\sqrt{p}} - \sqrt{a-b\sqrt{p}}\right) : \mathbb{Q}\right]$ does not equal to 1 or 3**.**

But $3\sqrt{a+b\sqrt{p}}-\sqrt{a-b\sqrt{p}}$ satisfies a fourth degree polynomial

$$\left(x^2-10a+6m\right)^2-64pb^2$$

.

Therefore $\left[\mathbb{Q}\left(3\sqrt{a+b\sqrt{p}}-\sqrt{a-b\sqrt{p}}\right):\mathbb{Q}\right]=4$.

□

Theorem 4.9. *For $a,b\neq 0$ rational numbers and p a prime number such that $m=\sqrt{a^2-pb^2}\in\mathbb{Q}$,*

$$\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\,,\ \frac{\sqrt{a+b\sqrt{p}}-\sqrt{a-b\sqrt{p}}}{2}\right)=\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}+\frac{\sqrt{a+b\sqrt{p}}-\sqrt{a-b\sqrt{p}}}{2}\right)$$

and

$$\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\,,\ \frac{\sqrt{a+b\sqrt{p}}+\sqrt{a-b\sqrt{p}}}{2}\right)=\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}+\frac{\sqrt{a+b\sqrt{p}}+\sqrt{a-b\sqrt{p}}}{2}\right)$$

Proof. We will prove the first part of the lemma, and the other part can be proved by similar argument.

$$\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\,,\ \frac{\sqrt{a+b\sqrt{p}}-\sqrt{a-b\sqrt{p}}}{2}\right)=\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}+\frac{\sqrt{a+b\sqrt{p}}-\sqrt{a-b\sqrt{p}}}{2}\right)$$

Since $m=\sqrt{a^2-pb^2}\in\mathbb{Q}$, then by lemma 3.10,

$$\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right)=\mathbb{Q}\left(\sqrt{a-b\sqrt{p}}\right)$$

So,

$$\frac{\sqrt{a+b\sqrt{p}}-\sqrt{a-b\sqrt{p}}}{2}\in\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right)$$

$$\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\,,\ \frac{\sqrt{a+b\sqrt{p}}-\sqrt{a-b\sqrt{p}}}{2}\right)=\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right).$$

On the other hand,

$$\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}+\frac{\sqrt{a+b\sqrt{p}}-\sqrt{a-b\sqrt{p}}}{2}\right)$$

$$=\mathbb{Q}\left(\frac{3\sqrt{a+b\sqrt{p}}-\sqrt{a-b\sqrt{p}}}{2}\right)$$

$$=\mathbb{Q}\left(3\sqrt{a+b\sqrt{p}}-\sqrt{a-b\sqrt{p}}\right)$$

So, it is sufficient to show

$$\mathbb{Q}\left(3\sqrt{a+b\sqrt{p}}-\sqrt{a-b\sqrt{p}}\right)=\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right).$$

Since $m=\sqrt{a^2-pb^2}\in\mathbb{Q}$, then

$$\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right)=\mathbb{Q}\left(\sqrt{a-b\sqrt{p}}\right)$$

So, $3\sqrt{a+b\sqrt{p}}-\sqrt{a-b\sqrt{p}}\in\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right)$

$$\mathbb{Q}\left(3\sqrt{a+b\sqrt{p}}-\sqrt{a-b\sqrt{p}}\right) \text{ is a subfield of } \mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right).$$

If we assume that $\left[\mathbb{Q}\left(3\sqrt{a+b\sqrt{p}}-\sqrt{a-b\sqrt{p}}\right):\mathbb{Q}\right]=2$, then by lemma 4.7, at least one of $\sqrt{\dfrac{2\left(a\pm\sqrt{a^2-pb^2}\right)}{p}}$ is a rational number.

But $\sqrt{\dfrac{a\pm\sqrt{a^2-pb^2}}{2p}}\in\mathbb{Q}$ if and only if $\sqrt{\dfrac{2\left(a\pm\sqrt{a^2-pb^2}\right)}{p}}\in\mathbb{Q}$.

So, by lemma 3.6,

$$\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\right]=2.$$

Thus,

$$\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\left(3\sqrt{a+b\sqrt{p}}-\sqrt{a-b\sqrt{p}}\right)\right]=1$$

$$\mathbb{Q}\left(3\sqrt{a+b\sqrt{p}}-\sqrt{a-b\sqrt{p}}\right)=\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right).$$

On the other hand, if we assume $\left[\mathbb{Q}\left(3\sqrt{a+b\sqrt{p}}-\sqrt{a-b\sqrt{p}}\right):\mathbb{Q}\right]=4$, then by lemma 4.8, both of $\sqrt{\dfrac{2\left(a\pm\sqrt{a^2-pb^2}\right)}{p}}\notin\mathbb{Q}$, and then both of $\sqrt{\dfrac{a\pm\sqrt{a^2-pb^2}}{2p}}\notin\mathbb{Q}$.

By lemma 3.7, we have

$$\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\right]=4$$

Thus,

$$\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\left(3\sqrt{a+b\sqrt{p}}-\sqrt{a-b\sqrt{p}}\right)\right]=1$$

Therefore, in both cases

$$\mathbb{Q}\left(3\sqrt{a+b\sqrt{p}}-\sqrt{a-b\sqrt{p}}\right)=\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right).$$

□

The proof of the first main theorem.

Theorem 4.10. *Suppose that $a, b \in \mathbb{Q}$, p and q are prime numbers. Then:*

$$\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}, \sqrt{q}\right) = \mathbb{Q}\left(\sqrt{a+b\sqrt{p}} + \sqrt{q}\right)$$

Proof. Note that if $b = 0$, then the theorem is true by lemma 4.2. Now, lets assume that $b \neq 0$.

The minimal polynomial over $\mathbb{Q}$ for $\sqrt{q}$ is of degree 2, while the minimal polynomial for $\sqrt{a+b\sqrt{p}}$ is either of degree 4 or degree 2.

Case 1: Assume that the minimal polynomial for $\sqrt{a+b\sqrt{p}}$ is of degree 2.

By lemma 3.5, we get that

$$\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right) = \mathbb{Q}\left(\sqrt{p}\right)$$
$$\sqrt{a+b\sqrt{p}} = \alpha + \beta\sqrt{p} \text{ for some } \alpha,\beta \in \mathbb{Q}.$$

Then,

$$\begin{aligned}\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}, \sqrt{q}\right) &= \mathbb{Q}(\alpha + \beta\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\beta\sqrt{p}, \sqrt{q}) \\ &= \mathbb{Q}\left(\beta\sqrt{p} + \sqrt{q}\right) \text{ by using lemma 4.2} \\ &= \mathbb{Q}\left(\alpha + \beta\sqrt{p} + \sqrt{q}\right) \\ &= \mathbb{Q}\left(\sqrt{a+b\sqrt{p}} + \sqrt{q}\right)\end{aligned}$$

Therefore,

$$\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}, \sqrt{q}\right) = \mathbb{Q}\left(\sqrt{a+b\sqrt{p}} + \sqrt{q}\right)$$

Case 2: Assume that the minimal polynomial for $\sqrt{a+b\sqrt{p}}$ is of degree 4.

The minimal polynomial of $\sqrt{a+b\sqrt{p}}$ over $\mathbb{Q}$ is $x^4-2ax^2+a^2-pb^2$. Its roots are:

$$\beta_1=\sqrt{a+b\sqrt{p}},\ \beta_2=-\sqrt{a+b\sqrt{p}},\ \beta_3=\sqrt{a-b\sqrt{p}},\ \beta_4=-\sqrt{a-b\sqrt{p}}.$$

The minimal polynomial of $\sqrt{q}$ over $\mathbb{Q}$ is x^2-q. Its roots are:

$$\alpha_1=\sqrt{q},\ \alpha_2=-\sqrt{q}.$$

Consider the finite set C defined in the proof of the primitive element theorem,

$$C=\left\{\frac{\beta_i-\beta_j}{\alpha_m-\alpha_n}:\ 1\le i,j\le 4,\ 1\le m,n\le 2\ and\ i\ne j, m\ne n\right\}$$
$$C=\left\{\frac{\beta_1-\beta_2}{\alpha_1-\alpha_2},\ \frac{\beta_1-\beta_3}{\alpha_1-\alpha_2},\ \frac{\beta_1-\beta_4}{\alpha_1-\alpha_2},\ \frac{\beta_2-\beta_3}{\alpha_1-\alpha_2},\ \frac{\beta_2-\beta_4}{\alpha_1-\alpha_2},\ \frac{\beta_3-\beta_4}{\alpha_1-\alpha_2}\right\}.$$

Suppose that $1\in$ C, then 1 will be equal to at least one element of the finite set C. Thus, we will have a finite set of equations.

$$1=\frac{\beta_i-\beta_j}{\alpha_1-\alpha_2},$$

which is equivalent to

$$2\sqrt{q}=\beta_i-\beta_j$$

such that $1\le i,j\le 4$ and $i\ne j$.

If none of those equations is satisfied, then by contrapositive $1\notin$ C, and thus by primitive element theorem we get $\mathbb{Q}\left(\sqrt{a+b\sqrt{p}},\sqrt{q}\right)=\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}+\sqrt{q}\right)$.

On the other hand, if any of the above equations is satisfied, then it will be proved directly in the following cases:

Case 1 $2\sqrt{q} = \beta_1 - \beta_2 \Longleftrightarrow 2\sqrt{q} = 2\sqrt{a + b\sqrt{p}} \Longleftrightarrow \sqrt{q} = \sqrt{a + b\sqrt{p}}$.

By squaring both sides, we get $q = a + b\sqrt{p}$. This contradicts the assumption that p is prime number and b is a non zero rational number.

Case 2 $2\sqrt{q} = \beta_3 - \beta_4 \Longleftrightarrow 2\sqrt{q} = 2\sqrt{a - b\sqrt{p}} \Longleftrightarrow \sqrt{q} = \sqrt{a + b\sqrt{p}}$.

By squaring both sides, we get $q = a - b\sqrt{p}$. This contradicts the assumption that p is prime number and b is a non zero rational number.

Case 3 $2\sqrt{q} = \beta_1 - \beta_3 \Longleftrightarrow 2\sqrt{q} = \sqrt{a + b\sqrt{p}} - \sqrt{a - b\sqrt{p}}$.

By squaring both sides we get $4q = \left(a + b\sqrt{p}\right) - 2\left(\sqrt{a^2 - pb^2}\right) + \left(a - b\sqrt{p}\right)$.

After simplification, we get

$$a - 2q = \sqrt{a^2 - pb^2}.$$

So, $\sqrt{a^2 - pb^2} \in \mathbb{Q}$.

But

$$\sqrt{q} = \frac{\sqrt{a + b\sqrt{p}} - \sqrt{a - b\sqrt{p}}}{2}$$

So, we have

$$\mathbb{Q}\left(\sqrt{a + b\sqrt{p}}\ ,\ \sqrt{q}\right) = \mathbb{Q}\left(\sqrt{a + b\sqrt{p}}\ ,\ \frac{\sqrt{a + b\sqrt{p}} - \sqrt{a - b\sqrt{p}}}{2}\right).$$

By lemma 4.9,

$$\mathbb{Q}\left(\sqrt{a + b\sqrt{p}}\ ,\ \frac{\sqrt{a + b\sqrt{p}} - \sqrt{a - b\sqrt{p}}}{2}\right) = \mathbb{Q}\left(\sqrt{a + b\sqrt{p}} + \frac{\sqrt{a + b\sqrt{p}} - \sqrt{a - b\sqrt{p}}}{2}\right)$$

Case 4 $2\sqrt{q} = \beta_1 - \beta_4 \Longleftrightarrow 2\sqrt{q} = \sqrt{a + b\sqrt{p}} + \sqrt{a - b\sqrt{p}}$.

By squaring both sides we get $4q = \left(a + b\sqrt{p}\right) + 2\left(\sqrt{a^2 - pb^2}\right) + \left(a - b\sqrt{p}\right)$

After simplification, we get

$$2q - a = \sqrt{a^2 - pb^2}$$

So, $m = \sqrt{a^2 - pb^2} \in \mathbb{Q}$.

But

$$\sqrt{q} = \frac{\sqrt{a + b\sqrt{p}} + \sqrt{a - b\sqrt{p}}}{2}$$

So, we have

$$\mathbb{Q}\left(\sqrt{a + b\sqrt{p}}\ ,\ \sqrt{q}\right) = \mathbb{Q}\left(\sqrt{a + b\sqrt{p}}\ ,\ \frac{\sqrt{a + b\sqrt{p}} + \sqrt{a - b\sqrt{p}}}{2}\right).$$

By lemma 4.9,

$$\mathbb{Q}\left(\sqrt{a + b\sqrt{p}}\ ,\ \frac{\sqrt{a + b\sqrt{p}} + \sqrt{a - b\sqrt{p}}}{2}\right) = \mathbb{Q}\left(\sqrt{a + b\sqrt{p}} + \frac{\sqrt{a + b\sqrt{p}} + \sqrt{a - b\sqrt{p}}}{2}\right)$$

All the remaining cases are similar to the above four cases.

Hence,

$$\mathbb{Q}\left(\sqrt{a + b\sqrt{p}}, \sqrt{q}\right) = \mathbb{Q}\left(\sqrt{a + b\sqrt{p}} + \sqrt{q}\right).$$

□

The following examples are direct applications of the above theorem.

Example 4.11. $\mathbb{Q}\left(\sqrt{1 + \sqrt{2}}\ ,\ \sqrt{3}\right) = \mathbb{Q}\left(\sqrt{1 + \sqrt{2}}\ +\ \sqrt{3}\right)$.

Example 4.12. $\mathbb{Q}\left(i\sqrt{1 + \sqrt{2}}\ ,\ \sqrt{3}\right) = \mathbb{Q}\left(i\sqrt{1 + \sqrt{2}}\ +\ \sqrt{3}\right)$.

Example 4.13. $\mathbb{Q}\left(i\sqrt{\sqrt{2}}\ ,\ \sqrt{3}\right) = \mathbb{Q}\left(i\sqrt{\sqrt{2}}\ +\ \sqrt{3}\right)$.

4.3 The case $\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}, \sqrt{c+d\sqrt{p}}\right)$

The first subsection presents four useful lemmas that will help in proving the second main Theorem (Theorem 4.18).

The second section includes the second main theorem (Theorem 4.18) in our research, in addition to its complete proof.

Some useful lemmas

Lemma 4.14. For any prime number p and any rational number x,

$$\sqrt{x} \in \mathbb{Q}(\sqrt{p}) \text{ if and only if } x = \begin{cases} pm^2 \\ m^2 \end{cases} \text{, where m is a rational number}$$

Proof. Assume $\sqrt{x} \in \mathbb{Q}(\sqrt{p})$, then there are α and β rational numbers such that $\sqrt{x} = \alpha + \beta\sqrt{p}$.

By squaring both sides, we get

$$x = \alpha^2 + p\beta^2 + 2\alpha\beta\sqrt{p}$$

By comparing the coefficient of the basis $1, \sqrt{p}$ on both sides, we get

$$x = \alpha^2 + p\beta^2 \text{ and } \alpha\beta = 0$$

If $\alpha = 0$, then $x = p\beta^2$, and if $\beta = 0$, then $x = \alpha^2$.

Therefore,

$$x = \begin{cases} pm^2 \\ m^2 \end{cases} \text{, where m is a rational number}$$

Conversely, assume that $x = \begin{cases} pm^2 \\ m^2 \end{cases}$, where m is a rational number, then

$$\sqrt{x} = \begin{cases} \pm m\sqrt{p} \\ \pm m \end{cases}$$

and $\sqrt{x} \in \mathbb{Q}(\sqrt{p})$ in either case.

□

Lemma 4.15. Let $a, b \neq 0, m, \alpha, \beta$ be rational numbers and p a prime number, such that $a^2 - pb^2 = pm^2$.

If $\left[\mathbb{Q}\left(\alpha\sqrt{a+b\sqrt{p}} + \beta\sqrt{p}\sqrt{a+b\sqrt{p}}\right) : \mathbb{Q}\right] = 2$, then

$$\mathbb{Q}\left(\alpha\sqrt{a+b\sqrt{p}} + \beta\sqrt{p}\sqrt{a+b\sqrt{p}}\right) = \mathbb{Q}\left(\sqrt{p}\right)$$

Proof. The minimal polynomial of $\sqrt{p}$ over $\mathbb{Q}$ is $x^2 - p$, then $\left[\mathbb{Q}\left(\sqrt{p}\right) : \mathbb{Q}\right] = 2$.
Claim: $\sqrt{p} \in \mathbb{Q}\left(\alpha\sqrt{a+b\sqrt{p}} + \beta\sqrt{p}\sqrt{a+b\sqrt{p}}\right)$.

Proof: Let $\psi = \alpha\sqrt{a+b\sqrt{p}} + \beta\sqrt{p}\sqrt{a+b\sqrt{p}}$. Then,

$$\psi^2 = \alpha^2\left(a+b\sqrt{p}\right) + 2\alpha\beta\sqrt{p}\left(a+b\sqrt{p}\right) + p\beta^2\left(a+b\sqrt{p}\right)$$

$$\psi^2 - a\left(\alpha^2 + p\beta^2\right) - 2\alpha\beta bp = \sqrt{p}\left(b\alpha^2 + bp\beta^2 + 2a\alpha\beta\right)$$

Since $b\alpha^2 + 2a\alpha\beta + bp\beta^2 \neq 0$, and $\left[\mathbb{Q}\left(\psi\right) : \mathbb{Q}\right] = 2$, then $\sqrt{p} \in \mathbb{Q}\left(\psi\right)$.

$$\sqrt{p} \in \mathbb{Q}\left(\alpha\sqrt{a+b\sqrt{p}} + \beta\sqrt{p}\sqrt{a+b\sqrt{p}}\right).$$

■

Claim: For $\alpha, \beta, a, b \neq 0$ rational numbers, p prime numbers,

$$b\alpha^2 + 2a\alpha\beta + bp\beta^2 \neq 0$$

Proof: Assume $b\alpha^2 + 2a\alpha\beta + bp\beta^2 = 0$, then

$$\beta = \frac{-a\alpha \pm \sqrt{\alpha^2\left(a^2 - pb^2\right)}}{bp} = \frac{-a\alpha \pm \sqrt{\alpha^2\left(pm^2\right)}}{bp}$$

$$\beta = \frac{-a\alpha \pm \alpha m\sqrt{p}}{bp}$$

This contradicts the assumption that $\beta \in \mathbb{Q}$, because $\alpha m \neq 0$. Otherwise, if $m = 0$, then $p = \left(\frac{a}{b}\right)^2$ contradicts the assumption that p is prime number, and if $\alpha = 0$, then $\beta = \frac{-a\alpha \pm \alpha m\sqrt{p}}{bp} = 0$.

■

Therefore, $\mathbb{Q}\left(\sqrt{p}\right)$ is a subfield of $\mathbb{Q}\left(\alpha\sqrt{a + b\sqrt{p}} + \beta\sqrt{p}\sqrt{a + b\sqrt{p}}\right)$, and

$$\left[\mathbb{Q}\left(\alpha\sqrt{a + b\sqrt{p}} + \beta\sqrt{p}\sqrt{a + b\sqrt{p}}\right) : \mathbb{Q}\left(\sqrt{p}\right)\right] \cdot \left[\mathbb{Q}\left(\sqrt{p}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\alpha\sqrt{a + b\sqrt{p}} + \beta\sqrt{p}\sqrt{a + b\sqrt{p}}\right) : \mathbb{Q}\right]$$

Thus, $\left[\mathbb{Q}\left(\alpha\sqrt{a + b\sqrt{p}} + \beta\sqrt{p}\sqrt{a + b\sqrt{p}}\right) : \mathbb{Q}\left(\sqrt{p}\right)\right] = 1$.

We conclude that,

$$\mathbb{Q}\left(\alpha\sqrt{a + b\sqrt{p}} + \beta\sqrt{p}\sqrt{a + b\sqrt{p}}\right) = \mathbb{Q}\left(\sqrt{p}\right)$$

□

Lemma 4.16. For $a, b \neq 0, m$ rational numbers and p a prime number, such that $a^2 - pb^2 = pm^2$,

$$\sqrt{2}\sqrt{a + m\sqrt{p}} \in \mathbb{Q}\left(\sqrt{a + b\sqrt{p}}\right).$$

Proof. In order to show that $\sqrt{2}\sqrt{a + m\sqrt{p}} \in \mathbb{Q}\left(\sqrt{a + b\sqrt{p}}\right)$, we will find rational num-

bers α, β, δ and ζ such that

$$\sqrt{2}\sqrt{a+m\sqrt{p}} = \delta + \zeta\sqrt{p} + \alpha\sqrt{a+b\sqrt{p}} + \beta\sqrt{p}\sqrt{a+b\sqrt{p}}$$

We have $2\left(a+m\sqrt{p}\right) =$

$$\begin{aligned}
&= \frac{1}{pm^2} \cdot \left(2a\left(pm^2\right) + 2m\sqrt{p}\left(pm^2\right)\right) \\
&= \frac{1}{pm^2} \cdot \left(2apm^2 + 2m\sqrt{p}\left(a^2 - pb^2\right)\right) \\
&= \frac{1}{pm^2} \cdot \left(2apm^2 + 2a^2m\sqrt{p} - 2mpb^2\sqrt{p}\right)
\end{aligned}$$

By adding and subtracting apb^2, we get

$$\begin{aligned}
&= \frac{1}{pm^2} \cdot \left(2apm^2 + 2a^2m\sqrt{p} - 2mpb^2\sqrt{p} + \left(apb^2 - apb^2\right)\right) \\
&= \frac{1}{pm^2} \cdot \left(apm^2 + 2a^2m\sqrt{p} - 2pmb^2\sqrt{p} - apb^2 + a\left(pm^2 + pb^2\right)\right) \\
&= \frac{1}{pm^2} \cdot \left(apm^2 + 2a^2m\sqrt{p} - 2pmb^2\sqrt{p} - apb^2 + a^3\right)
\end{aligned}$$

By adding and subtracting $2ambp + a^2b\sqrt{p} + b^3p\sqrt{p}$

$$\begin{aligned}
&= \frac{1}{pm^2} \cdot \left(apm^2 + 2a^2m\sqrt{p} - 2pmb^2\sqrt{p} - apb^2 + a^3 + \left(2ambp + a^2b\sqrt{p} + b^3p\sqrt{p}\right) - \left(2ambp + a^2b\sqrt{p} + b^3p\sqrt{p}\right)\right) \\
&= \frac{1}{pm^2} \cdot \left(a + b\sqrt{p}\right)\left(pm^2 + pb^2 - 2pmb + a^2 + 2am\sqrt{p} - 2ab\sqrt{p}\right)
\end{aligned}$$

So,

$$\begin{aligned}
2\left(a+m\sqrt{p}\right) &= \frac{1}{pm^2}\left(a+b\sqrt{p}\right)\left(pm^2+pb^2-2pmb+a^2+2am\sqrt{p}-2ab\sqrt{p}\right) \\
&= \left(a+b\sqrt{p}\right)\left(\frac{pm^2+pb^2-2pmb}{pm^2}+\frac{a^2}{pm^2}+\frac{2am\sqrt{p}}{pm^2}-\frac{2ab\sqrt{p}}{pm^2}\right) \\
&= \left(a+b\sqrt{p}\right)\left(\frac{m^2+b^2-2mb}{m^2}+\frac{a^2}{pm^2}+\frac{2a\sqrt{p}}{pm}-\frac{2ab\sqrt{p}}{pm^2}\right) \\
&= \left(a+b\sqrt{p}\right)\left(\left(\frac{m-b}{m}\right)^2+p\left(\frac{a}{pm}\right)^2+\frac{2a}{pm}\cdot\left(1-\frac{b}{m}\right)\sqrt{p}\right) \\
&= \left(a+b\sqrt{p}\right)\left(\left(\frac{m-b}{m}\right)^2+p\left(\frac{a}{pm}\right)^2+2\cdot\frac{a}{pm}\cdot\left(\frac{m-b}{m}\right)\sqrt{p}\right) \\
&= \left(a+b\sqrt{p}\right)\cdot\left(\frac{m-b}{m}+\frac{a}{pm}\sqrt{p}\right)^2
\end{aligned}$$

By taking square roots of both sides, we get:

$$\begin{aligned}
\sqrt{2}\cdot\sqrt{a+m\sqrt{p}} &= \pm\sqrt{a+b\sqrt{p}}\cdot\left(\frac{m-b}{m}+\frac{a}{pm}\sqrt{p}\right) \\
\sqrt{2}\cdot\sqrt{a+m\sqrt{p}} &= \pm\left(\frac{m-b}{m}\cdot\sqrt{a+b\sqrt{p}}+\frac{a}{pm}\sqrt{p}\cdot\sqrt{a+b\sqrt{p}}\right).
\end{aligned}$$

Therefore, $\sqrt{2}\sqrt{a+m\sqrt{p}} \in \mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right)$ with $\delta=0, \zeta=0, \alpha=\pm\dfrac{m-b}{m}$ and $\beta=\pm\dfrac{a}{pm}$.
□

Lemma 4.17. For $a, b \neq 0, m$ rational numbers and p a prime number,
such that $a^2-pb^2=pm^2$,

$$\left[\mathbb{Q}\left(\sqrt{2}\cdot\sqrt{a+m\sqrt{p}}+\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\right]=4$$

Proof. Since $b \neq 0$ and $\sqrt{a^2 - pb^2} \notin \mathbb{Q}$, then by lemma 3.8,

$$\left[\mathbb{Q}\left(\sqrt{a + b\sqrt{p}}\right) : \mathbb{Q}\right] = 4.$$

By lemma 4.16, we have $\sqrt{2} \cdot \sqrt{a + m\sqrt{p}} \in \mathbb{Q}\left(\sqrt{a + b\sqrt{p}}\right)$, and

$$\sqrt{2} \cdot \sqrt{a + m\sqrt{p}} = \pm\left(\frac{m - b}{m} \cdot \sqrt{a + b\sqrt{p}} + \frac{a}{p \cdot m}\sqrt{p} \cdot \sqrt{a + b\sqrt{p}}\right).$$

Case 1: $\sqrt{2} \cdot \sqrt{a + m\sqrt{p}} = \dfrac{m - b}{m} \cdot \sqrt{a + b\sqrt{p}} + \dfrac{a}{p \cdot m}\sqrt{p} \cdot \sqrt{a + b\sqrt{p}}$

Then, by adding $\sqrt{a + b\sqrt{p}}$ to both sides,

$$\begin{aligned}\sqrt{2} \cdot \sqrt{a + m\sqrt{p}} + \sqrt{a + b\sqrt{p}} &= \left(\frac{m - b}{m} \cdot \sqrt{a + b\sqrt{p}} + \frac{a}{p \cdot m}\sqrt{p} \cdot \sqrt{a + b\sqrt{p}}\right) + \sqrt{a + b\sqrt{p}} \\ &= \frac{2m - b}{m} \cdot \sqrt{a + b\sqrt{p}} + \frac{a}{p \cdot m}\sqrt{p} \cdot \sqrt{a + b\sqrt{p}}\end{aligned}$$

Thus, $\mathbb{Q}\left(\sqrt{2} \cdot \sqrt{a + m\sqrt{p}} + \sqrt{a + b\sqrt{p}}\right)$ is a subfield of $\mathbb{Q}\left(\sqrt{a + b\sqrt{p}}\right)$.

We will show that

$$\left[\mathbb{Q}\left(\sqrt{2} \cdot \sqrt{a + m\sqrt{p}} + \sqrt{a + b\sqrt{p}}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt{a + b\sqrt{p}}\right) : \mathbb{Q}\right].$$

First, suppose that $\left[\mathbb{Q}\left(\sqrt{2} \cdot \sqrt{a + m\sqrt{p}} + \sqrt{a + b\sqrt{p}}\right) : \mathbb{Q}\right] = 2$.

Since

$$\mathbb{Q}\left(\sqrt{2} \cdot \sqrt{a + m\sqrt{p}} + \sqrt{a + b\sqrt{p}}\right) = \mathbb{Q}\left(\frac{2m - b}{m} \cdot \sqrt{a + b\sqrt{p}} + \frac{a}{p \cdot m}\sqrt{p} \cdot \sqrt{a + b\sqrt{p}}\right)$$

then by lemma 4.15,

$$\mathbb{Q}\left(\frac{2m-b}{m}\cdot\sqrt{a+b\sqrt{p}}+\frac{a}{p\cdot m}\sqrt{p}\cdot\sqrt{a+b\sqrt{p}}\right)=\mathbb{Q}\left(\sqrt{p}\right)$$

So,

$$\frac{2m-b}{m}\cdot\sqrt{a+b\sqrt{p}}+\frac{a}{p\cdot m}\sqrt{p}\cdot\sqrt{a+b\sqrt{p}}=\alpha+\beta\sqrt{p}$$

By squaring both sides we get

$$\left(\left(\frac{2m-b}{m}\right)^2+\frac{2a}{pm}\left(\frac{2m-b}{m}\right)\sqrt{p}+\left(\frac{a}{p\cdot m}\right)^2 p\right)(a+b\sqrt{p})=\alpha^2+2\alpha\beta\sqrt{p}+p\beta^2$$

So,

$$\alpha^2+p\beta^2=a\left(\left(\frac{2m-b}{m}\right)^2+\frac{2a}{pm}\left(\frac{2m-b}{m}\right)\sqrt{p}+\left(\frac{a}{p\cdot m}\right)^2 p\right)$$

and

$$2\alpha\beta=b\left(\left(\frac{2m-b}{m}\right)^2+\frac{2a}{pm}\left(\frac{2m-b}{m}\right)\sqrt{p}+\left(\frac{a}{p\cdot m}\right)^2 p\right).$$

Then, $\alpha^2+p\beta^2=a\left(\frac{2\alpha\beta}{b}\right)$. So, we have the second degree equation in β.

$$bp\beta^2-2\alpha a\beta+b\alpha^2=0$$

$$\beta=\frac{\alpha a\pm\alpha\sqrt{a^2-pb^2}}{pb}$$

But $\sqrt{a^2-pb^2}\notin\mathbb{Q}$, so this contradicts the assumption that $\beta\in\mathbb{Q}$.

Therefore,

$$\left[\mathbb{Q}\left(\sqrt{2}\cdot\sqrt{a+m\sqrt{p}}+\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\right]\neq 2.$$

But $\mathbb{Q}\left(\sqrt{2}\cdot\sqrt{a+m\sqrt{p}}+\sqrt{a+b\sqrt{p}}\right)$ is a subfield of $\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right)$ which is of degree 4 over $\mathbb{Q}$.

Note that $\left[\mathbb{Q}\left(\sqrt{2}\cdot\sqrt{a+m\sqrt{p}}+\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\right]$ does not equal 1 or 3. We conclude that

$$\left[\mathbb{Q}\left(\sqrt{2}\cdot\sqrt{a+m\sqrt{p}}+\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\right]=4$$

Case 2: $\sqrt{2}\cdot\sqrt{a+m\sqrt{p}}=-\left(\frac{m-b}{m}\cdot\sqrt{a+b\sqrt{p}}+\frac{a}{p\cdot m}\sqrt{p}\cdot\sqrt{a+b\sqrt{p}}\right)$

Then,

$$\begin{aligned}\sqrt{2}\cdot\sqrt{a+m\sqrt{p}}+\sqrt{a+b\sqrt{p}}&=-\left(\frac{m-b}{m}\cdot\sqrt{a+b\sqrt{p}}+\frac{a}{p\cdot m}\sqrt{p}\cdot\sqrt{a+b\sqrt{p}}\right)+\sqrt{a+b\sqrt{p}}\\&=\frac{b}{m}\cdot\sqrt{a+b\sqrt{p}}-\frac{a}{p\cdot m}\sqrt{p}\cdot\sqrt{a+b\sqrt{p}}\end{aligned}$$

Thus, $\mathbb{Q}\left(\sqrt{2}\cdot\sqrt{a+m\sqrt{p}}+\sqrt{a+b\sqrt{p}}\right)$ is a subfield of $\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right)$.

We will show that

$$\left[\mathbb{Q}\left(\sqrt{2}\cdot\sqrt{a+m\sqrt{p}}+\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\right]=\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\right].$$

First, suppose that $\left[\mathbb{Q}\left(\sqrt{2}\cdot\sqrt{a+m\sqrt{p}}+\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\right]=2$, so

$$\left[\mathbb{Q}\left(\frac{b}{m}\cdot\sqrt{a+b\sqrt{p}}-\frac{a}{p\cdot m}\sqrt{p}\cdot\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\right]=2$$

So, by lemma 4.15,

$$\mathbb{Q}\left(\frac{b}{m}\cdot\sqrt{a+b\sqrt{p}}-\frac{a}{p\cdot m}\sqrt{p}\cdot\sqrt{a+b\sqrt{p}}\right)=\mathbb{Q}\left(\sqrt{p}\right)$$

$$\frac{b}{m} \cdot \sqrt{a + b\sqrt{p}} - \frac{a}{p \cdot m}\sqrt{p} \cdot \sqrt{a + b\sqrt{p}} = \alpha + \beta\sqrt{p}$$

By squaring both sides we get

$$\left(\frac{b^2}{m^2} - \frac{2ab\sqrt{p}}{pm^2} + \frac{a^2}{pm^2}\right)(a + b\sqrt{p}) = \alpha^2 + 2\alpha\beta\sqrt{p} + p\beta^2$$

So,

$$\alpha^2 + p\beta^2 = a\left(\frac{a^2}{pm^2} - \frac{b^2}{m^2}\right)$$

and

$$2\alpha\beta = -b\left(\frac{a^2}{pm^2} - \frac{b^2}{m^2}\right)$$

Then, $\alpha^2 + p\beta^2 = a\left(\frac{2\alpha\beta}{-b}\right)$. So, we have the second degree equation

$$bp\beta^2 + 2\alpha a\beta + b\alpha^2 = 0$$

$$\beta = \frac{-\alpha a \pm \alpha\sqrt{a^2 - pb^2}}{bp}$$

But $\sqrt{a^2 - pb^2} \notin \mathbb{Q}$, this contradicts the assumption that $\beta \in \mathbb{Q}$.

Therefore,

$$\left[\mathbb{Q}\left(\sqrt{2} \cdot \sqrt{a + m\sqrt{p}} + \sqrt{a + b\sqrt{p}}\right) : \mathbb{Q}\right] \neq 2.$$

But $\mathbb{Q}\left(\sqrt{2} \cdot \sqrt{a + m\sqrt{p}} + \sqrt{a + b\sqrt{p}}\right)$ is a subfield of $\mathbb{Q}\left(\sqrt{a + b\sqrt{p}}\right)$ which is of degree 4 over $\mathbb{Q}$.

Note that $\left[\mathbb{Q}\left(\sqrt{2} \cdot \sqrt{a + m\sqrt{p}} + \sqrt{a + b\sqrt{p}}\right) : \mathbb{Q}\right]$ does not equal 1 or 3. We conclude that

$$\left[\mathbb{Q}\left(\sqrt{2} \cdot \sqrt{a + m\sqrt{p}} + \sqrt{a + b\sqrt{p}}\right) : \mathbb{Q}\right] = 4.$$

□

The proof of the second main theorem.

Theorem 4.18. *Let $a, b \neq 0, c, d \neq 0$ be any rational numbers and p a prime number. If $a \neq c$ or $b \neq -d$ such that $a \pm \sqrt{a^2 - pb^2} \neq c \pm \sqrt{c^2 - pd^2}$, then*

$$\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}, \sqrt{c+d\sqrt{p}}\right) = \mathbb{Q}\left(\sqrt{a+b\sqrt{p}} + \sqrt{c+d\sqrt{p}}\right).$$

Proof. The proof of this theorem will be of three cases. In the first case we will assume that $\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right) : \mathbb{Q}\right] = 2$ and $\left[\mathbb{Q}\left(\sqrt{c+d\sqrt{p}}\right) : \mathbb{Q}\right] = 2$. In the second case, we will assume that degree of one of $\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right)$ and $\mathbb{Q}\left(\sqrt{c+d\sqrt{p}}\right)$ is 4 and the other is 2. The last case, we will assume that the degree of both of them is 4.

Case 1: Assume that the minimal polynomial over $\mathbb{Q}$ for each of $\sqrt{a+b\sqrt{p}}$ and $\sqrt{c+d\sqrt{p}}$ is of degree 2:

So, $\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right) : \mathbb{Q}\right] = 2$ and $\left[\mathbb{Q}\left(\sqrt{c+d\sqrt{p}}\right) : \mathbb{Q}\right] = 2$.

Then by lemma 3.5,

$$\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right) = \mathbb{Q}\left(\sqrt{p}\right) \text{ and } \mathbb{Q}\left(\sqrt{c+d\sqrt{p}}\right) = \mathbb{Q}\left(\sqrt{p}\right).$$

So,

$$\sqrt{a+b\sqrt{p}} = a_0 + a_1\sqrt{p} \text{ and } \sqrt{c+d\sqrt{p}} = c_0 + c_1\sqrt{p}$$

for some rational numbers a_0, a_1, c_0, c_1.

Thus,

$$\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\ ,\ \sqrt{c+d\sqrt{p}}\right) = \mathbb{Q}\left(\sqrt{p}\ ,\ \sqrt{p}\right) = \mathbb{Q}\left(\sqrt{p}\right).$$

On the other hand, we have

$$\begin{aligned}\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\ +\ \sqrt{c+d\sqrt{p}}\right) &= \mathbb{Q}\left(a_0+a_1\sqrt{p}+c_0+c_1\sqrt{p}\right)\\ &= \mathbb{Q}\left((a_0+c_0)+(a_1+c_1)\sqrt{p}\right)\\ &= \mathbb{Q}\left(\sqrt{p}\right)\ \text{since } a_1\neq -c_1,\ \text{and } a_0+c_0, a_1+c_1\in\mathbb{Q}.\end{aligned}$$

Therefore,

$$\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\ ,\ \sqrt{c+d\sqrt{p}}\right) = \mathbb{Q}\left(\sqrt{a+b\sqrt{p}}+\sqrt{c+d\sqrt{p}}\right).$$

We have claimed that $a_1 \neq -c_1$. The following is it proof. By using the proof of lemma 3.6, we conclude that $a_1 = \pm\sqrt{\dfrac{a\pm\sqrt{a^2-pb^2}}{2p}}$ and $c_1 = \pm\sqrt{\dfrac{c\pm\sqrt{c^2-pd^2}}{2p}}$. Suppose that $a_1 = -c_1$, then $a_1^2 = c_1^2$, and thus

$$\frac{a\pm\sqrt{a^2-pb^2}}{2p} = \frac{c\pm\sqrt{c^2-pd^2}}{2p}$$

$$a\pm\sqrt{a^2-pb^2} = c\pm\sqrt{c^2-pd^2}$$

This contradicts the initial assumption.

Case 2: Assume that the minimal polynomial over $\mathbb{Q}$ for one of them is of degree 4, and the other is of degree 2.

Without loss of generality, assume that $\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\right]=4$ and $\left[\mathbb{Q}\left(\sqrt{c+d\sqrt{p}}\right):\mathbb{Q}\right]=2$.

Then by lemma 3.5, we get

$$\mathbb{Q}\left(\sqrt{c+d\sqrt{p}}\right) = \mathbb{Q}\left(\sqrt{p}\right).$$

So, in this case $\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}, \sqrt{c+d\sqrt{p}}\right) = \mathbb{Q}\left(\sqrt{a+b\sqrt{p}}, \sqrt{p}\right)$.

By theorem 4.10, we have

$$\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\ ,\ \sqrt{p}\right) = \mathbb{Q}\left(\sqrt{a+b\sqrt{p}}+\sqrt{p}\right)$$

Therefore,

$$\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\ ,\ \sqrt{c+d\sqrt{p}}\right) = \mathbb{Q}\left(\sqrt{a+b\sqrt{p}}+\sqrt{c+d\sqrt{p}}\right).$$

Case 3: Finally, assume that the minimal polynomials for both $\sqrt{a+b\sqrt{p}}$ and $\sqrt{c+d\sqrt{p}}$ are of degree 4.

The minimal polynomial of $\sqrt{a+b\sqrt{p}}$ over $\mathbb{Q}$ is $x^4-2ax^2+a^2-pb^2$. Its roots are:

$$\alpha_1 = -\sqrt{a-b\sqrt{p}}, \alpha_2 = \sqrt{a-b\sqrt{p}}, \alpha_3 = -\sqrt{a+b\sqrt{p}}, \alpha_4 = \sqrt{a+b\sqrt{p}}.$$

The minimal polynomial of $\sqrt{c+d\sqrt{p}}$ over $\mathbb{Q}$ is $x^4-2cx^2+c^2-pd^2$. Its roots are:

$$\beta_1 = -\sqrt{c-d\sqrt{p}}, \beta_2 = \sqrt{c-d\sqrt{p}}, \beta_3 = -\sqrt{c+d\sqrt{p}}, \beta_4 = \sqrt{c+d\sqrt{p}}.$$

Consider the finite set C defined in the proof of the primitive element theorem. Suppose that $1 \in$ C, then 1 will be equal to at least one element of the finite set C. Thus we will have finite set of equations.

If none of the above equations is satisfied, then by contrapositive $1 \notin$ C, and thus by the primitive element theorem we get $\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}, \sqrt{c+d\sqrt{p}}\right) = \mathbb{Q}\left(\sqrt{a+b\sqrt{p}}+\sqrt{c+d\sqrt{p}}\right)$.

On the other hand, if any of the above equations is satisfied, then it will be proved directly in the following cases:

Case i: $\frac{\alpha_1-\alpha_2}{\beta_1-\beta_2}=1 \implies \frac{-\sqrt{a-b\sqrt{p}}-\sqrt{a-b\sqrt{p}}}{-\sqrt{c-d\sqrt{p}}-\sqrt{c-d\sqrt{p}}} = 1 \implies \frac{-2\sqrt{a-b\sqrt{p}}}{-2\sqrt{c-d\sqrt{p}}} = 1 \implies$
$\frac{\sqrt{a-b\sqrt{p}}}{\sqrt{c-d\sqrt{p}}}=1 \implies \sqrt{a-b\sqrt{p}}=\sqrt{c-d\sqrt{p}}$

By squaring both sides, we get:

$$a-b\sqrt{p}=c-d\sqrt{p}$$

So $b=d$ and $a=c$. Thus,

$$\sqrt{a+b\sqrt{p}}=\sqrt{c+d\sqrt{p}}$$

Then, $\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\ ,\ \sqrt{c+d\sqrt{p}}\right)=\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\ ,\ \sqrt{a+b\sqrt{p}}\right)=\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right)=$
$\mathbb{Q}\left(2\sqrt{a+b\sqrt{p}}\right)=\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}+\sqrt{a+b\sqrt{p}}\right)=\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}+\sqrt{c+d\sqrt{p}}\right)$

Case ii: $\frac{\alpha_1-\alpha_2}{\beta_1-\beta_3}=1 \implies \frac{-\sqrt{a-b\sqrt{p}}-\sqrt{a-b\sqrt{p}}}{-\sqrt{c-d\sqrt{p}}+\sqrt{c+d\sqrt{p}}}=1 \implies -2\sqrt{a-b\sqrt{p}}=-\sqrt{c-d\sqrt{p}}+$
$\sqrt{c+d\sqrt{p}}$

By squaring both sides, we get

$$4\left(a-b\sqrt{p}\right)=2c-2\sqrt{c^2-pd^2}$$

$$2\left(a-b\sqrt{p}\right)=c-\sqrt{c^2-pd^2} \tag{4.2}$$

Thus, $\sqrt{c^2-pd^2}\in\mathbb{Q}\left(\sqrt{p}\right)$.

By lemma 4.14, $c^2-pd^2=\begin{cases} m^2 \\ pm^2 \end{cases}$, where $m\geq 0$ is a rational number.

1. If $c^2-pd^2=m^2$

   Substituting $c^2-pd^2=m^2$ in the equation 4.2,we get:

$$2a-2b\sqrt{p}=c-m$$

This contradicts the assumption that b is a non-zero rational number.

2. If $c^2 - pd^2 = pm^2$

   Substituting $c^2 - pd^2 = pm^2$ in equation 4.2,we get:

$$2a - 2b\sqrt{p} = c - m\sqrt{p} \tag{4.3}$$

   so,

$$c = 2a \text{ and } m = 2b$$

   Substituting these values in $c^2 - pd^2 = pm^2$, we get

$$4a^2 - pd^2 = 4pb^2$$
$$4\left(a^2 - pb^2\right) = pd^2$$

   By rearranging its terms, we get

$$a^2 - pb^2 = p\left(\frac{d}{2}\right)^2$$
$$a^2 - pb^2 = pk^2 \text{ for } k = \frac{d}{2} \in \mathbb{Q}.$$

   Now, using $4\left(a^2 - pb^2\right) = pd^2$,

$$\mathbb{Q}\left(\sqrt{c + d\sqrt{p}}\right) = \mathbb{Q}\left(\sqrt{c + \sqrt{pd^2}}\right) = \mathbb{Q}\left(\sqrt{2a + \sqrt{4\left(a^2 - pb^2\right)}}\right)$$

$$= \mathbb{Q}\left(\sqrt{2a + 2\sqrt{\left(a^2 - pb^2\right)}}\right) = \mathbb{Q}\left(\sqrt{2} \cdot \sqrt{a + \sqrt{pk^2}}\right) = \mathbb{Q}\left(\sqrt{2} \cdot \sqrt{a + |k|\sqrt{p}}\right).$$

So,

$$\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\,,\,\sqrt{c+d\sqrt{p}}\right)=\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\,,\,\sqrt{2}\cdot\sqrt{a+|k|\sqrt{p}}\right).$$

By lemma 4.17, and the assumption $a^2-pb^2=pk^2$, we have

$$\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}+\sqrt{2}\cdot\sqrt{a+|k|\sqrt{p}}\right):\mathbb{Q}\right]=4.$$

By lemma 4.16, $\sqrt{2}\cdot\sqrt{a+|k|\sqrt{p}}\in\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right)$, and then

$$\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\,,\;\sqrt{2}\cdot\sqrt{a+|k|\sqrt{p}}\right)=\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right).$$

Also,

$$\mathbb{Q}\left(\sqrt{2}\cdot\sqrt{a+|k|\sqrt{p}}+\sqrt{a+b\sqrt{p}}\right)\text{ is a subfield of }\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right)$$

Since we have $\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}+\sqrt{2}\cdot\sqrt{a+|k|\sqrt{p}}\right):\mathbb{Q}\right]=4$ and the assumption $\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\right]=4$, then

$$\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\,,\;\sqrt{2}\cdot\sqrt{a+|k|\sqrt{p}}\right)=\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}+\sqrt{2}\cdot\sqrt{a+|k|\sqrt{p}}\right).$$

But

$$\mathbb{Q}\left(\sqrt{c+d\sqrt{p}}\right)=\mathbb{Q}\left(\sqrt{2}\cdot\sqrt{a+|k|\sqrt{p}}\right),$$

So,

$$\mathbb{Q}\left(\sqrt{a+b\sqrt{p}},\sqrt{c+d\sqrt{p}}\right)=\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}+\sqrt{c+d\sqrt{p}}\right)$$

Case iii: $\dfrac{\alpha_1-\alpha_2}{\beta_3-\beta_4}=1 \Longrightarrow \dfrac{-\sqrt{a-b\sqrt{p}}-\sqrt{a-b\sqrt{p}}}{-\sqrt{c+d\sqrt{p}}-\sqrt{c+d\sqrt{p}}}=1$

$$-2\sqrt{a-b\sqrt{p}}=-2\sqrt{c+d\sqrt{p}}$$

By squaring both sides, we get

$$4\left(a-b\sqrt{p}\right)=4\left(c+d\sqrt{p}\right)$$

$$a-b\sqrt{p}=c+d\sqrt{p}$$

Then, $a=c$ and $b=-d$.

This contradicts the assumption that $a\neq c$ or $b\neq -d$.

Case iv: $\dfrac{\alpha_1-\alpha_3}{\beta_1-\beta_3}=1 \Longrightarrow \dfrac{-\sqrt{a-b\sqrt{p}}+\sqrt{a+b\sqrt{p}}}{-\sqrt{c-d\sqrt{p}}+\sqrt{c+d\sqrt{p}}}=1$

$$-\sqrt{a-b\sqrt{p}}+\sqrt{a+b\sqrt{p}}=-\sqrt{c-d\sqrt{p}}+\sqrt{c+d\sqrt{p}}$$

By squaring both sides, we get

$$2a-2\sqrt{a^2-pb^2}=2c-2\sqrt{c^2-pd^2}$$

$$a-\sqrt{a^2-pb^2}=c-\sqrt{c^2-pd^2}$$

This contradicts the initial assumption.

Case v: $\dfrac{\alpha_1-\alpha_3}{\beta_1-\beta_4}=1 \Longrightarrow \dfrac{-\sqrt{a-b\sqrt{p}}+\sqrt{a+b\sqrt{p}}}{-\sqrt{c-d\sqrt{p}}-\sqrt{c+d\sqrt{p}}}=1$

$$-\sqrt{a-b\sqrt{p}}+\sqrt{a+b\sqrt{p}}=-\sqrt{c-d\sqrt{p}}-\sqrt{c+d\sqrt{p}}$$

By squaring both sides, we get

$$2a - 2\sqrt{a^2 - b^2p} = 2c + 2\sqrt{c^2 - d^2p}$$

$$a - \sqrt{a^2 - b^2p} = c + \sqrt{c^2 - d^2p}$$

This contradicts the initial assumption.

Case vi: $\dfrac{\alpha_1 - \alpha_4}{\beta_1 - \beta_3} = 1 \Longrightarrow \dfrac{-\sqrt{a - b\sqrt{p}} - \sqrt{a + b\sqrt{p}}}{-\sqrt{c - d\sqrt{p}} + \sqrt{c + d\sqrt{p}}} = 1$

$$-\sqrt{a - b\sqrt{p}} - \sqrt{a + b\sqrt{p}} = -\sqrt{c - d\sqrt{p}} + \sqrt{c + d\sqrt{p}}$$

By squaring both sides, we get

$$2a + 2\sqrt{a^2 - pb^2} = 2c - 2\sqrt{c^2 - pd^2}$$

$$a + \sqrt{a^2 - pb^2} = c - \sqrt{c^2 - pd^2}$$

This contradicts the initial assumption.

Case vii: $\dfrac{\alpha_1 - \alpha_4}{\beta_1 - \beta_4} = 1 \Longrightarrow \dfrac{-\sqrt{a - b\sqrt{p}} - \sqrt{a + b\sqrt{p}}}{-\sqrt{c - d\sqrt{p}} - \sqrt{c + d\sqrt{p}}} = 1$

$$-\sqrt{a - b\sqrt{p}} - \sqrt{a + b\sqrt{p}} = -\sqrt{c - d\sqrt{p}} - \sqrt{c + d\sqrt{p}}$$

By squaring both sides, we get

$$2a + 2\sqrt{a^2 - b^2p} = 2c + 2\sqrt{c^2 - d^2p}$$

$$a + \sqrt{a^2 - b^2p} = c + \sqrt{c^2 - d^2p}$$

This contradicts the initial assumption.

All the other remaining cases are similar to the above.

□

Example 4.19. In the notations of the previous theorem, $a = 0, b = -1, c = 2, d = -1, p = 3$ satisfy the assumptions. Therefore

$$\mathbb{Q}\left(\sqrt{-\sqrt{3}}\,,\ \sqrt{2-\sqrt{3}}\right) = \mathbb{Q}\left(\sqrt{-\sqrt{3}}\ +\ \sqrt{2-\sqrt{3}}\right).$$

We will also show this directly as an exercise.

Clearly we have $\mathbb{Q}\left(i\sqrt{\sqrt{3}}\ +\ \sqrt{2-\sqrt{3}}\right) \subseteq \mathbb{Q}\left(i\sqrt{\sqrt{3}}\,,\ \sqrt{2-\sqrt{3}}\right)$. We will show that $\mathbb{Q}\left(i\sqrt{\sqrt{3}}\,,\ \sqrt{2-\sqrt{3}}\right) \subseteq \mathbb{Q}\left(i\sqrt{\sqrt{3}}\ +\ \sqrt{2-\sqrt{3}}\right)$.

The minimal polynomial of $i\sqrt{\sqrt{3}}\ +\ \sqrt{2-\sqrt{3}}$ over $\mathbb{Q}$ is

$$x^8 - 8x^6 - 24x^4 - 32x^2 + 16.$$

and $\psi = \sqrt{2\left(1-\sqrt{3}+i\sqrt{-3+2\sqrt{3}}\right)}$ satisfies the minimal polynomial. So,

$$\mathbb{Q}\left(i\sqrt{\sqrt{3}}\ +\ \sqrt{2-\sqrt{3}}\right) = \mathbb{Q}\left(\sqrt{2\left(1-\sqrt{3}+i\sqrt{-3+2\sqrt{3}}\right)}\right).$$

Thus, the basis of $\mathbb{Q}\left(i\sqrt{\sqrt{3}}\ +\ \sqrt{2-\sqrt{3}}\right)$ is

$$\left\{1, \psi, \psi^2, \psi^3, \psi^4, \psi^5, \psi^6, \psi^7\right\}.$$

But we have

$$i\sqrt{\sqrt{3}} = \frac{-3}{2}\psi - \frac{3}{2}\psi^3 - \frac{1}{2}\psi^5 + \frac{1}{16}\psi^7$$

So, $i\sqrt{\sqrt{3}} \in \mathbb{Q}\left(i\sqrt{\sqrt{3}}\ +\ \sqrt{2-\sqrt{3}}\right)$, and thus $\sqrt{2-\sqrt{3}} \in \mathbb{Q}\left(i\sqrt{\sqrt{3}}\ +\ \sqrt{2-\sqrt{3}}\right)$. Therefore

$$\mathbb{Q}\left(i\sqrt{\sqrt{3}}\,,\ \sqrt{2-\sqrt{3}}\right) \subseteq \mathbb{Q}\left(i\sqrt{\sqrt{3}}\ +\ \sqrt{2-\sqrt{3}}\right).$$

4.4 The case $\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}, \sqrt{a-b\sqrt{p}}\right)$

In Theorem 4.18, we had found the necessary conditions for $\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}, \sqrt{c+d\sqrt{p}}\right) = \mathbb{Q}\left(\sqrt{a+b\sqrt{p}}+\sqrt{c+d\sqrt{p}}\right)$. What will be the result if $a=c$ and $b=-d$? Would we get $\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}, \sqrt{c-d\sqrt{p}}\right) \neq \mathbb{Q}\left(\sqrt{a+b\sqrt{p}}+\sqrt{c-d\sqrt{p}}\right)$? we will present some situations when this is true, and others which is not true.

Lemma 4.20. Let $a, b \neq 0, m$ be rational numbers and p a prime number, such that $\sqrt{a^2-pb^2} = m\sqrt{p}$.

If $\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}+\sqrt{a-b\sqrt{p}}\right) : \mathbb{Q}\right] = 2$, then $\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}+\sqrt{a-b\sqrt{p}}\right) = \mathbb{Q}\left(\sqrt{p}\right)$.

Proof. The minimal polynomial of $\sqrt{p}$ over $\mathbb{Q}$ is x^2-p, so $\left[\mathbb{Q}\left(\sqrt{p}\right) : \mathbb{Q}\right] = 2$.
Claim: $\sqrt{p} \in \mathbb{Q}\left(\sqrt{a+b\sqrt{p}}+\sqrt{a-b\sqrt{p}}\right)$

Proof: Let $\psi = \sqrt{a+b\sqrt{p}}+\sqrt{a-b\sqrt{p}}$, then

$$\begin{aligned} \psi^2 &= 2a + 2\sqrt{a^2-pb^2} \\ \psi^2 &= 2a + 2m\sqrt{p} \\ \psi^2 - 2a &= 2m\sqrt{p} \end{aligned}$$

By squaring both sides we get

$$\begin{aligned} \psi^4 - 4a\psi^2 + 4a^2 &= 4pm^2 \\ \psi^4 - 4a\psi^2 + 4\left(a^2 - pm^2\right) &= 0 \\ \psi^4 - 4a\psi^2 + 4pb^2 &= 0 \end{aligned}$$

Thus,

$$\psi = \pm\sqrt{2a \pm 2\sqrt{a^2 - pb^2}}$$
$$\psi = \pm\sqrt{2a \pm 2m\sqrt{p}}.$$

So,

$$\sqrt{p} \in \mathbb{Q}\left(\sqrt{2a + 2m\sqrt{p}}\right).$$

But $\mathbb{Q}\left(\sqrt{a + b\sqrt{p}} + \sqrt{a - b\sqrt{p}}\right) = \mathbb{Q}\left(\sqrt{2a + 2m\sqrt{p}}\right)$, so

$$\sqrt{p} \in \mathbb{Q}\left(\sqrt{a + b\sqrt{p}} + \sqrt{a - b\sqrt{p}}\right).$$

■

Therefore, $\mathbb{Q}\left(\sqrt{p}\right)$ is a subfield of $\mathbb{Q}\left(\sqrt{a + b\sqrt{p}} + \sqrt{a - b\sqrt{p}}\right)$, and

$$\left[\mathbb{Q}\left(\sqrt{a + b\sqrt{p}} + \sqrt{a - b\sqrt{p}}\right) : \mathbb{Q}\left(\sqrt{p}\right)\right] \cdot \left[\mathbb{Q}\left(\sqrt{p}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt{a + b\sqrt{p}} + \sqrt{a - b\sqrt{p}}\right) : \mathbb{Q}\right].$$

Thus, $\left[\mathbb{Q}\left(\sqrt{a + b\sqrt{p}} + \sqrt{a - b\sqrt{p}}\right) : \mathbb{Q}\left(\sqrt{p}\right)\right] = 1$.

We conclude that,

$$\mathbb{Q}\left(\sqrt{a + b\sqrt{p}} + \sqrt{a - b\sqrt{p}}\right) = \mathbb{Q}\left(\sqrt{p}\right).$$

□

Theorem 4.21. *Let $a, b \neq 0$ be rational numbers, and p a prime number such that $\sqrt{a^2 - pb^2} \in \mathbb{Q}$.*

If both of $\sqrt{\dfrac{a \pm \sqrt{a^2 - pb^2}}{2p}} \notin \mathbb{Q}$, then

$$\mathbb{Q}\left(\sqrt{a + b\sqrt{p}}, \sqrt{a - b\sqrt{p}}\right) \neq \mathbb{Q}\left(\sqrt{a + b\sqrt{p}} + \sqrt{a - b\sqrt{p}}\right).$$

Proof. Since $\sqrt{a^2 - pb^2} \in \mathbb{Q}$, then by lemma 3.10

$$\mathbb{Q}\left(\sqrt{a + b\sqrt{p}}\right) = \mathbb{Q}\left(\sqrt{a - b\sqrt{p}}\right),$$

So,

$$\mathbb{Q}\left(\sqrt{a + b\sqrt{p}}, \sqrt{a - b\sqrt{p}}\right) = \mathbb{Q}\left(\sqrt{a + b\sqrt{p}}\right).$$

By lemma 3.7, and the assumption that both of $\sqrt{\dfrac{a \pm \sqrt{a^2 - pb^2}}{2p}} \notin \mathbb{Q}$, we have

$$\left[\mathbb{Q}\left(\sqrt{a + b\sqrt{p}}, \sqrt{a - b\sqrt{p}}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt{a + b\sqrt{p}}\right) : \mathbb{Q}\right] = 4.$$

On the other hand, $\sqrt{a + b\sqrt{p}} + \sqrt{a - b\sqrt{p}}$ has a minimal polynomial $x^2 - 2a - \sqrt{a^2 - pb^2}$. Thus,

$$\left[\mathbb{Q}\left(\sqrt{a + b\sqrt{p}} + \sqrt{a - b\sqrt{p}}\right) : \mathbb{Q}\right] = 2.$$

Therefore,

$$\mathbb{Q}\left(\sqrt{a + b\sqrt{p}}, \sqrt{a - b\sqrt{p}}\right) \neq \mathbb{Q}\left(\sqrt{a + b\sqrt{p}} + \sqrt{a - b\sqrt{p}}\right).$$

□

Example 4.22. $\mathbb{Q}\left(\sqrt{9 + 6\sqrt{2}}, \sqrt{9 - 6\sqrt{2}}\right) \neq \mathbb{Q}\left(\sqrt{9 + 6\sqrt{2}} + \sqrt{9 - 6\sqrt{2}}\right)$ as a direct application of the previous theorem.

Theorem 4.23. *Let $a, b \neq 0$ be rational numbers, and p a prime number such that $\sqrt{a^2 - pb^2} \in \mathbb{Q}$.*

If at least one of $\sqrt{\dfrac{a \pm \sqrt{a^2 - pb^2}}{2p}} \in \mathbb{Q}$, then

$$\mathbb{Q}\left(\sqrt{a + b\sqrt{p}}, \sqrt{a - b\sqrt{p}}\right) = \mathbb{Q}\left(\sqrt{a + b\sqrt{p}} + \sqrt{a - b\sqrt{p}}\right).$$

Proof. Since $\sqrt{a^2 - pb^2} \in \mathbb{Q}$, then by lemma 3.10

$$\mathbb{Q}\left(\sqrt{a + b\sqrt{p}}\right) = \mathbb{Q}\left(\sqrt{a - b\sqrt{p}}\right),$$

So,

$$\mathbb{Q}\left(\sqrt{a + b\sqrt{p}}, \sqrt{a - b\sqrt{p}}\right) = \mathbb{Q}\left(\sqrt{a + b\sqrt{p}}\right).$$

By lemma 3.6, and the assumption that at least one of $\sqrt{\dfrac{a \pm \sqrt{a^2 - pb^2}}{2p}} \in \mathbb{Q}$, we have

$$\left[\mathbb{Q}\left(\sqrt{a + b\sqrt{p}}, \sqrt{a - b\sqrt{p}}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt{a + b\sqrt{p}}\right) : \mathbb{Q}\right] = 2.$$

On the other hand, $\sqrt{a + b\sqrt{p}} + \sqrt{a - b\sqrt{p}}$ has a minimal polynomial $x^2 - 2a - \sqrt{a^2 - pb^2}$. Thus,

$$\left[\mathbb{Q}\left(\sqrt{a + b\sqrt{p}} + \sqrt{a - b\sqrt{p}}\right) : \mathbb{Q}\right] = 2.$$

So, $\mathbb{Q}\left(\sqrt{a + b\sqrt{p}} + \sqrt{a - b\sqrt{p}}\right)$ is a subfield of $\mathbb{Q}\left(\sqrt{a + b\sqrt{p}}, \sqrt{a - b\sqrt{p}}\right)$, and both are of degree 2 over $\mathbb{Q}$.

Therefore,

$$\mathbb{Q}\left(\sqrt{a + b\sqrt{p}}, \sqrt{a - b\sqrt{p}}\right) = \mathbb{Q}\left(\sqrt{a + b\sqrt{p}} + \sqrt{a - b\sqrt{p}}\right).$$

□

Example 4.24. $\mathbb{Q}\left(\sqrt{3 + 2\sqrt{2}}, \sqrt{3 - 2\sqrt{2}}\right) = \mathbb{Q}\left(\sqrt{3 + 2\sqrt{2}} + \sqrt{3 - 2\sqrt{2}}\right)$ as a direct application of the previous theorem.

Theorem 4.25. *Let $a, b \neq 0, m$ be rational numbers, and p a prime number.*

If $a^2 - pb^2 = pm^2$, then

$$\mathbb{Q}\left(\sqrt{a + b\sqrt{p}}, \sqrt{a - b\sqrt{p}}\right) = \mathbb{Q}\left(\sqrt{a + b\sqrt{p}} + \sqrt{a - b\sqrt{p}}\right).$$

Proof.

Note that $\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\right]$ is 2 or 4, because $b \neq 0$. Using lemma 3.6, and the fact $\sqrt{a^2-pb^2} = \sqrt{pm^2} \notin \mathbb{Q}$,

$$\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\right] \neq 2$$

So,

$$\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\right] = 4.$$

On the other hand, since $a^2 - pb^2 = pm^2$, then by lemma 3.10,

$$\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right) = \mathbb{Q}\left(\sqrt{a-b\sqrt{p}}\right).$$

So,

$$\sqrt{a+b\sqrt{p}} + \sqrt{a-b\sqrt{p}} \in \mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right).$$

Thus,

$$\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}, \sqrt{a-b\sqrt{p}}\right):\mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right):\mathbb{Q}\right] = 4.$$

But $\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}} + \sqrt{a-b\sqrt{p}}\right):\mathbb{Q}\right]$ is 2 or 4, because $\mathbb{Q}\left(\sqrt{a+b\sqrt{p}} + \sqrt{a-b\sqrt{p}}\right)$ is a subfield of $\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}, \sqrt{a-b\sqrt{p}}\right)$.

Assume that $\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}} + \sqrt{a-b\sqrt{p}}\right):\mathbb{Q}\right] = 2$. Then by lemma 4.20

$$\mathbb{Q}\left(\sqrt{a+b\sqrt{p}} + \sqrt{a-b\sqrt{p}}\right) = \mathbb{Q}\left(\sqrt{p}\right),$$

So

$$\sqrt{a+b\sqrt{p}} + \sqrt{a-b\sqrt{p}} = \alpha + \beta\sqrt{p} \text{ for some } \alpha, \beta \in \mathbb{Q}.$$

By squaring both sides, we get

$$2a + 2m\sqrt{p} = \alpha^2 + 2\alpha\beta\sqrt{p} + p\beta^2$$

Thus,

$$2a = \alpha^2 + p\beta^2 \text{ and } m = \alpha\beta$$

So, we will have a fourth degree equation in β

$$p^2\beta^4 - 2ap\beta^2 + a^2 - pb^2 = 0$$

Solving for β, we get

$$\beta = \pm\sqrt{\frac{ap \pm bp\sqrt{p}}{a^2 - pb^2}} \notin \mathbb{Q} \text{ because } b \neq 0$$

This contradicts the assumption $\left[\mathbb{Q}\left(\sqrt{a + b\sqrt{p}} + \sqrt{a - b\sqrt{p}}\right) : \mathbb{Q}\right] = 2$.
So, $\left[\mathbb{Q}\left(\sqrt{a + b\sqrt{p}} + \sqrt{a - b\sqrt{p}}\right) : \mathbb{Q}\right] \neq 2$.
Thus $\left[\mathbb{Q}\left(\sqrt{a + b\sqrt{p}} + \sqrt{a - b\sqrt{p}}\right) : \mathbb{Q}\right] = 4$.

Now, we have that $\mathbb{Q}\left(\sqrt{a + b\sqrt{p}} + \sqrt{a - b\sqrt{p}}\right)$ is a subfield of $\mathbb{Q}\left(\sqrt{a + b\sqrt{p}}, \sqrt{a - b\sqrt{p}}\right)$, and both have degree 4 over $\mathbb{Q}$.

Therefore,

$$\mathbb{Q}\left(\sqrt{a + b\sqrt{p}}, \sqrt{a - b\sqrt{p}}\right) = \mathbb{Q}\left(\sqrt{a + b\sqrt{p}} + \sqrt{a - b\sqrt{p}}\right).$$

□

Example 4.26. As an immediate application we have

$$\mathbb{Q}\left(\sqrt{2 + \sqrt{2}}\,,\ \sqrt{2 - \sqrt{2}}\right) = \mathbb{Q}\left(\sqrt{2 + \sqrt{2}}\ +\ \sqrt{2 - \sqrt{2}}\right).$$

Theorem 4.27. *Let $a, b > 0$ be rational numbers, and p a prime number.*

If $-b\sqrt{p} < a < b\sqrt{p}$, then

$$\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}, \sqrt{a-b\sqrt{p}}\right) \neq \mathbb{Q}\left(\sqrt{a+b\sqrt{p}} + \sqrt{a-b\sqrt{p}}\right).$$

Proof. Since $-b\sqrt{p} < a < b\sqrt{p}$, then $a^2 - pb^2 < 0$. So, by lemma 3.8,

$$\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right) : \mathbb{Q}\right] = 4 \text{ and } \left[\mathbb{Q}\left(\sqrt{a-b\sqrt{p}}\right) : \mathbb{Q}\right] = 4.$$

Since $a < b\sqrt{p}$, then $\mathbb{Q}\left(\sqrt{a-b\sqrt{p}}\right) = \mathbb{Q}\left(i\sqrt{-a+b\sqrt{p}}\right)$.

Since $-b\sqrt{p} < a < b\sqrt{p}$, where $b > 0$, then $\sqrt{-a+b\sqrt{p}} \in \mathbb{R}$ and $\sqrt{a+b\sqrt{p}} \in \mathbb{R}$. So, $i\sqrt{-a+b\sqrt{p}} \notin \mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right)$. Then,

$$\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}\right) \neq \mathbb{Q}\left(\sqrt{a-b\sqrt{p}}\right).$$

Thus,

$$\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}, \sqrt{a-b\sqrt{p}}\right) : \mathbb{Q}\right] > 4.$$

On the other hand , $\sqrt{a+b\sqrt{p}} + \sqrt{a-b\sqrt{p}}$ is a root of $x^4 - 4ax^2 + 4pb^2$, so

$$\left[\mathbb{Q}\left(\sqrt{a+b\sqrt{p}} + \sqrt{a-b\sqrt{p}}\right) : \mathbb{Q}\right] \leq 4.$$

Since $\mathbb{Q}\left(\sqrt{a+b\sqrt{p}} + \sqrt{a-b\sqrt{p}}\right)$ is a subfield of $\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}, \sqrt{a-b\sqrt{p}}\right)$ and having different degrees over $\mathbb{Q}$, then

$$\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}, \sqrt{a-b\sqrt{p}}\right) \neq \mathbb{Q}\left(\sqrt{a+b\sqrt{p}} + \sqrt{a-b\sqrt{p}}\right).$$

□

Example 4.28. $\mathbb{Q}\left(\sqrt{\sqrt{2}}, \sqrt{-\sqrt{2}}\right) \neq \mathbb{Q}\left(\sqrt{\sqrt{2}} + \sqrt{-\sqrt{2}}\right)$ as a direct application of the previous theorem.

Chapter 5

Future Work

We are looking forward to prove under what conditions we have:

$$\mathbb{Q}\left(\sqrt{a+b\sqrt{p}},\sqrt{c+d\sqrt{q}}\right)=\mathbb{Q}\left(\sqrt{a+b\sqrt{p}}+\sqrt{c+d\sqrt{q}}\right)$$

where $a,b,c,d\in\mathbb{Q}$ and p and q are different prime numbers.

Moreover, extension fields adjoint by n^{th} root elements will be more interesting. For example studying under what conditions we have:

$$\mathbb{Q}\left(\sqrt[n]{a+b\sqrt{p}},\sqrt[m]{c+d\sqrt{q}}\right)=\mathbb{Q}\left(\sqrt[n]{a+b\sqrt{p}}+\sqrt[m]{c+d\sqrt{q}}\right)$$

where $a,b,c,d\in\mathbb{Q}$, $m,n\in\mathbb{N}$, and p and q are different prime numbers.

References

[1] Gallian Joseph, *CONTEMPORARY ABSTRACT ALGEBRA*, Houghton Mifflin Company, Boston, MA, 2006.

[2] Dummit, David and Foote, Richard, *ABSTRACT ALGEBRA, 3rd edition*, Wiley India Pvt. Limited, 2004.

Curriculum Vitae

Mohamad Medhat Moussa was born on Febraury 7^{th}, 1986 in Doha, Qatar. He entered Beirut Arab University (Beirut, Lebanon) in the Fall of 2005, and graduated in the spring of 2009 with a Bachelor degree BSc in Mathematics . After that, he traveled to United Arab Emirates (UAE) in August 2009 to start his job as a high school teacher at Alworood Private Academy for 4 years. In the fall of 2013, Mohamad started his graduate study (MSc in Mathematics) at the University of Texas at El Paso.

Permenent address: Beirut, Lebanon.
mohamadmoussa7@hotmail.com
mmmoussa@miners.utep.edu