Field Extensions and Splitting Fields

Bernd Schröder
Introduction
Introduction

1. What do we do when we “use a formula”? 

We take coefficients and perform algebraic operations (including root extractions) with them.

It turns out that most complex numbers cannot be reached that way.

So it makes sense to focus on fields that contain “just enough” to allow the operations we need.

For a “formula” to solve $p(x) = 0$ with $p \in \mathbb{Z}[x]$, we start with $\mathbb{Q}$.

Every time we extract a root, we may need to enlarge our scope.

This presentation makes the statement in 5 more precise.
Introduction

1. What do we do when we “use a formula”? We take coefficients and perform algebraic operations (including root extractions) with them.
Introduction

1. What do we do when we “use a formula”? We take coefficients and perform algebraic operations (including root extractions) with them.

2. It turns out that most complex numbers cannot be reached that way.
Introduction

1. What do we do when we “use a formula”? We take coefficients and perform algebraic operations (including root extractions) with them.

2. It turns out that most complex numbers cannot be reached that way.

3. So it makes sense to focus on fields that contain “just enough” to allow the operations we need.
Introduction

1. What do we do when we “use a formula”? We take coefficients and perform algebraic operations (including root extractions) with them.

2. It turns out that most complex numbers cannot be reached that way.

3. So it makes sense to focus on fields that contain “just enough” to allow the operations we need.

4. For a “formula” to solve $p(x) = 0$ with $p \in \mathbb{Z}[x]$
Introduction

1. What do we do when we “use a formula”? We take coefficients and perform algebraic operations (including root extractions) with them.

2. It turns out that most complex numbers cannot be reached that way.

3. So it makes sense to focus on fields that contain “just enough” to allow the operations we need.

4. For a “formula” to solve $p(x) = 0$ with $p \in \mathbb{Z}[x]$, we start with $\mathbb{Q}$. 

Bernd Schröder
Louisiana Tech University, College of Engineering and Science
Field Extensions and Splitting Fields
Introduction

1. What do we do when we “use a formula”? We take coefficients and perform algebraic operations (including root extractions) with them.

2. It turns out that most complex numbers cannot be reached that way.

3. So it makes sense to focus on fields that contain “just enough” to allow the operations we need.

4. For a “formula” to solve $p(x) = 0$ with $p \in \mathbb{Z}[x]$, we start with $\mathbb{Q}$.

5. Every time we extract a root, we may need to enlarge our scope.
Introduction

1. What do we do when we “use a formula”? We take coefficients and perform algebraic operations (including root extractions) with them.

2. It turns out that most complex numbers cannot be reached that way.

3. So it makes sense to focus on fields that contain “just enough” to allow the operations we need.

4. For a “formula” to solve $p(x) = 0$ with $p \in \mathbb{Z}[x]$, we start with $\mathbb{Q}$.

5. Every time we extract a root, we may need to enlarge our scope.

6. This presentation makes the statement in 5 more precise.
Definition.
Definition. Let \((\mathbb{E}, +, \cdot)\) be a field
Definition. Let $(\mathbb{E}, +, \cdot)$ be a field and let $\mathbb{F} \subseteq \mathbb{E}$ be a subset.
**Definition.** Let $(\mathbb{E}, +, \cdot)$ be a field and let $F \subseteq \mathbb{E}$ be a subset so that the restricted operations $+|_{F \times F}$ and $\cdot|_{F \times F}$ both map into $F$. Then $F$ is called a subfield of $\mathbb{E}$ and $\mathbb{E}$ is called an extension of $F$. We denote this situation more briefly by $F \subseteq \mathbb{E}$. 
**Definition.** Let \((\mathbb{E}, +, \cdot)\) be a field and let \(F \subseteq \mathbb{E}\) be a subset so that the restricted operations \(+|_{F \times F}\) and \(\cdot|_{F \times F}\) both map into \(F\) and so that \((F, +, \cdot)\) is a field whose identity element for addition is \(0 \in \mathbb{E}\) and whose identity element with respect to multiplication is \(1 \in \mathbb{E}\).
Definition. Let \((\mathbb{E}, +, \cdot)\) be a field and let \(\mathbb{F} \subseteq \mathbb{E}\) be a subset so that the restricted operations \(+|_{\mathbb{F} \times \mathbb{F}}\) and \(\cdot|_{\mathbb{F} \times \mathbb{F}}\) both map into \(\mathbb{F}\) and so that \((\mathbb{F}, +, \cdot)\) is a field whose identity element for addition is \(0 \in \mathbb{E}\) and whose identity element with respect to multiplication is \(1 \in \mathbb{E}\). Then \(\mathbb{F}\) is called a **subfield** of \(\mathbb{E}\).
Definition. Let $(\mathbb{E}, +, \cdot)$ be a field and let $F \subseteq \mathbb{E}$ be a subset so that the restricted operations $+|_{F \times F}$ and $\cdot|_{F \times F}$ both map into $F$ and so that $(F, +, \cdot)$ is a field whose identity element for addition is $0 \in \mathbb{E}$ and whose identity element with respect to multiplication is $1 \in \mathbb{E}$. Then $F$ is called a subfield of $\mathbb{E}$ and $\mathbb{E}$ is called an extension of $F$. 
Definition. Let \((\mathbb{E}, +, \cdot)\) be a field and let \(F \subseteq \mathbb{E}\) be a subset so that the restricted operations \(+|_{F\times F}\) and \(\cdot|_{F\times F}\) both map into \(F\) and so that \((F, +, \cdot)\) is a field whose identity element for addition is \(0 \in \mathbb{E}\) and whose identity element with respect to multiplication is \(1 \in \mathbb{E}\). Then \(F\) is called a subfield of \(\mathbb{E}\) and \(\mathbb{E}\) is called an extension of \(F\). We denote this situation more briefly by \(F \subseteq \mathbb{E}\).
<table>
<thead>
<tr>
<th>Subfields</th>
<th>Splitting Fields</th>
<th>Adjoining Elements</th>
</tr>
</thead>
</table>

**Definition.**

Let \((F, +, \cdot)\) be a field of characteristic zero and let \(p \in F[x]\) be a polynomial of positive degree. The equation \(p(x) = 0\) is solvable by radicals iff all its solutions can be calculated from its coefficients in a finite number of steps using field operations (addition, multiplication, additive and multiplicative inversion) and root extractions. The root extractions are allowed to yield elements that are not in \(F\), but in an extension field \(E\) of \(F\). Note that solvability by radicals does not mean there is a general formula. It means that there is some way to express the zeros of the polynomial under investigation.
Definition. Let $(\mathbb{F}, +, \cdot)$ be a field of characteristic zero.
Definition. Let $(\mathbb{F}, +, \cdot)$ be a field of characteristic zero and let $p \in \mathbb{F}[x]$ be a polynomial of positive degree.
Definition. Let \((\mathbb{F}, +, \cdot)\) be a field of characteristic zero and let \(p \in \mathbb{F}[x]\) be a polynomial of positive degree. The equation \(p(x) = 0\) is **solvable by radicals** iff all its solutions can be calculated from its coefficients in a finite number of steps using field operations (addition, multiplication, additive and multiplicative inversion) and root extractions. The root extractions are allowed to yield elements that are not in \(\mathbb{F}\), but in an extension field \(E\) of \(\mathbb{F}\). Note that solvability by radicals does not mean there is a general formula. It means that there is some way to express the zeros of the polynomial under investigation.
**Definition.** Let $(\mathbb{F}, +, \cdot)$ be a field of characteristic zero and let $p \in \mathbb{F}[x]$ be a polynomial of positive degree. The equation $p(x) = 0$ is **solvable by radicals** iff all its solutions can be calculated from its coefficients in a finite number of steps using field operations.
Definition. Let $(\mathbb{F}, +, \cdot)$ be a field of characteristic zero and let $p \in \mathbb{F}[x]$ be a polynomial of positive degree. The equation $p(x) = 0$ is solvable by radicals iff all its solutions can be calculated from its coefficients in a finite number of steps using field operations (addition, multiplication, additive and multiplicative inversion).
**Definition.** Let $(\mathbb{F}, +, \cdot)$ be a field of characteristic zero and let $p \in \mathbb{F}[x]$ be a polynomial of positive degree. The equation $p(x) = 0$ is **solvable by radicals** iff all its solutions can be calculated from its coefficients in a finite number of steps using field operations (addition, multiplication, additive and multiplicative inversion) and root extractions.
Definition. Let $(\mathbb{F}, +, \cdot)$ be a field of characteristic zero and let $p \in \mathbb{F}[x]$ be a polynomial of positive degree. The equation $p(x) = 0$ is solvable by radicals iff all its solutions can be calculated from its coefficients in a finite number of steps using field operations (addition, multiplication, additive and multiplicative inversion) and root extractions. The root extractions are allowed to yield elements that are not in $\mathbb{F}$, but in an extension field $\mathbb{E}$ of $\mathbb{F}$.
**Definition.** Let $(\mathbb{F}, +, \cdot)$ be a field of characteristic zero and let $p \in \mathbb{F}[x]$ be a polynomial of positive degree. The equation $p(x) = 0$ is **solvable by radicals** iff all its solutions can be calculated from its coefficients in a finite number of steps using field operations (addition, multiplication, additive and multiplicative inversion) and root extractions. The root extractions are allowed to yield elements that are not in $\mathbb{F}$, but in an extension field $\mathbb{E}$ of $\mathbb{F}$.

Note that solvability by radicals does not mean there is a general formula.
**Definition.** Let \((\mathbb{F}, +, \cdot)\) be a field of characteristic zero and let \(p \in \mathbb{F}[x]\) be a polynomial of positive degree. The equation \(p(x) = 0\) is **solvable by radicals** iff all its solutions can be calculated from its coefficients in a finite number of steps using field operations (addition, multiplication, additive and multiplicative inversion) and root extractions. The root extractions are allowed to yield elements that are not in \(\mathbb{F}\), but in an extension field \(\mathbb{E}\) of \(\mathbb{F}\).

Note that solvability by radicals does not mean there is a general formula. It means that there is *some* way to express the zeros of the polynomial under investigation.
Proposition.
Proposition. Let \((\mathbb{E}, +, \cdot)\) be a field and let \(\{\mathbb{F}_j\}_{j \in J}\) be a family of subfields of \(\mathbb{E}\).
Proposition. Let \((E, +, \cdot)\) be a field and let \(\{F_j\}_{j \in J}\) be a family of subfields of \(E\). Then \(\bigcap_{j \in J} F_j\) is a subfield of \(E\).
**Proposition.** Let $(\mathbb{E}, +, \cdot)$ be a field and let $\{F_j\}_{j \in J}$ be a family of subfields of $\mathbb{E}$. Then $\bigcap_{j \in J} F_j$ is a subfield of $\mathbb{E}$.

**Proof.**
**Proposition.** Let \((\mathbb{E}, +, \cdot)\) be a field and let \(\{\mathbb{F}_j\}_{j \in J}\) be a family of subfields of \(\mathbb{E}\). Then \(\bigcap_{j \in J} \mathbb{F}_j\) is a subfield of \(\mathbb{E}\).

**Proof.** By assumption, 0, 1 \(\in\) \(\bigcap_{j \in J} \mathbb{F}_j\).
**Proposition.** Let \((\mathbb{E}, +, \cdot)\) be a field and let \(\{\mathbb{F}_j\}_{j \in J}\) be a family of subfields of \(\mathbb{E}\). Then \(\bigcap_{j \in J} \mathbb{F}_j\) is a subfield of \(\mathbb{E}\).

**Proof.** By assumption, \(0, 1 \in \bigcap_{j \in J} \mathbb{F}_j\). Because the \(\mathbb{F}_j\) are subfields, sums and products of elements of \(\mathbb{F}_j\) are in \(\mathbb{F}_j\), too.
**Proposition.** Let \((E, +, \cdot)\) be a field and let \(\{F_j\}_{j \in J}\) be a family of subfields of \(E\). Then \(\bigcap_{j \in J} F_j\) is a subfield of \(E\).

**Proof.** By assumption, \(0, 1 \in \bigcap_{j \in J} F_j\). Because the \(F_j\) are subfields, sums and products of elements of \(F_j\) are in \(F_j\), too. The binary operations on \(\bigcap_{j \in J} F_j\) are the restrictions of the binary operations in \(E\). 0 and 1 are identity elements for addition and multiplication in \(E\). Hence they are the identity elements for addition and multiplication in \(\bigcap_{j \in J} F_j\).
**Proposition.** Let \((\mathbb{E}, +, \cdot)\) be a field and let \(\{\mathbb{F}_j\}_{j \in J}\) be a family of subfields of \(\mathbb{E}\). Then \(\bigcap_{j \in J} \mathbb{F}_j\) is a subfield of \(\mathbb{E}\).

**Proof.** By assumption, \(0, 1 \in \bigcap_{j \in J} \mathbb{F}_j\). Because the \(\mathbb{F}_j\) are subfields, sums and products of elements of \(\mathbb{F}_j\) are in \(\mathbb{F}_j\), too. The binary operations on \(\bigcap_{j \in J} \mathbb{F}_j\) are the restrictions of the binary operations in \(\mathbb{E}\) and they map into \(\bigcap_{j \in J} \mathbb{F}_j\).
Proposition. Let $(\mathbb{E}, +, \cdot)$ be a field and let $\{F_j\}_{j \in J}$ be a family of subfields of $\mathbb{E}$. Then $\bigcap_{j \in J} F_j$ is a subfield of $\mathbb{E}$.

Proof. By assumption, $0, 1 \in \bigcap_{j \in J} F_j$. Because the $F_j$ are subfields, sums and products of elements of $F_j$ are in $F_j$, too. The binary operations on $\bigcap_{j \in J} F_j$ are the restrictions of the binary operations in $\mathbb{E}$ and they map into $\bigcap_{j \in J} F_j$. Moreover, 0 and 1 are identity elements for addition and multiplication in $\mathbb{E}$, and they are the identity elements for addition and multiplication in $\bigcap_{j \in J} F_j$. Hence, $\bigcap_{j \in J} F_j$ is a subfield of $\mathbb{E}$. 
**Proposition.** Let $(\mathbb{E}, +, \cdot)$ be a field and let $\{\mathbb{F}_j\}_{j \in J}$ be a family of subfields of $\mathbb{E}$. Then $\bigcap_{j \in J} \mathbb{F}_j$ is a subfield of $\mathbb{E}$.

**Proof.** By assumption, $0, 1 \in \bigcap_{j \in J} \mathbb{F}_j$. Because the $\mathbb{F}_j$ are subfields, sums and products of elements of $\mathbb{F}_j$ are in $\mathbb{F}_j$, too. The binary operations on $\bigcap_{j \in J} \mathbb{F}_j$ are the restrictions of the binary operations in $\mathbb{E}$ and they map into $\bigcap_{j \in J} \mathbb{F}_j$. Moreover, associativity
**Proposition.** Let \((\mathbb{E}, +, \cdot)\) be a field and let \(\{\mathbb{F}_j\}_{j \in J}\) be a family of subfields of \(\mathbb{E}\). Then \(\bigcap_{j \in J} \mathbb{F}_j\) is a subfield of \(\mathbb{E}\).

**Proof.** By assumption, \(0, 1 \in \bigcap_{j \in J} \mathbb{F}_j\). Because the \(\mathbb{F}_j\) are subfields, sums and products of elements of \(\mathbb{F}_j\) are in \(\mathbb{F}_j\), too. The binary operations on \(\bigcap_{j \in J} \mathbb{F}_j\) are the restrictions of the binary operations in \(\mathbb{E}\) and they map into \(\bigcap_{j \in J} \mathbb{F}_j\). Moreover, associativity, commutativity...
Proposition. Let \((\mathbb{E}, +, \cdot)\) be a field and let \(\{\mathbb{F}_j\}_{j \in J}\) be a family of subfields of \(\mathbb{E}\). Then \(\bigcap_{j \in J} \mathbb{F}_j\) is a subfield of \(\mathbb{E}\).

Proof. By assumption, \(0, 1 \in \bigcap_{j \in J} \mathbb{F}_j\). Because the \(\mathbb{F}_j\) are subfields, sums and products of elements of \(\mathbb{F}_j\) are in \(\mathbb{F}_j\), too. The binary operations on \(\bigcap_{j \in J} \mathbb{F}_j\) are the restrictions of the binary operations in \(\mathbb{E}\) and they map into \(\bigcap_{j \in J} \mathbb{F}_j\). Moreover, associativity, commutativity and distributivity of multiplication over addition hold in \(\bigcap_{j \in J} \mathbb{F}_j\), too.
Proposition. Let $(\mathbb{E}, +, \cdot)$ be a field and let $\{\mathbb{F}_j\}_{j \in J}$ be a family of subfields of $\mathbb{E}$. Then $\bigcap_{j \in J} \mathbb{F}_j$ is a subfield of $\mathbb{E}$.

Proof. By assumption, $0, 1 \in \bigcap_{j \in J} \mathbb{F}_j$. Because the $\mathbb{F}_j$ are subfields, sums and products of elements of $\mathbb{F}_j$ are in $\mathbb{F}_j$, too. The binary operations on $\bigcap_{j \in J} \mathbb{F}_j$ are the restrictions of the binary operations in $\mathbb{E}$ and they map into $\bigcap_{j \in J} \mathbb{F}_j$. Moreover, associativity, commutativity and distributivity of multiplication over addition hold in $\bigcap_{j \in J} \mathbb{F}_j$, too. $0$ and $1$ are identity elements for addition and multiplication in $\mathbb{E}$. 
**Proposition.** Let \((\mathbb{E}, +, \cdot)\) be a field and let \(\{\mathbb{F}_j\}_{j \in J}\) be a family of subfields of \(\mathbb{E}\). Then \(\bigcap_{j \in J} \mathbb{F}_j\) is a subfield of \(\mathbb{E}\).

**Proof.** By assumption, \(0, 1 \in \bigcap_{j \in J} \mathbb{F}_j\). Because the \(\mathbb{F}_j\) are subfields, sums and products of elements of \(\mathbb{F}_j\) are in \(\mathbb{F}_j\), too. The binary operations on \(\bigcap_{j \in J} \mathbb{F}_j\) are the restrictions of the binary operations in \(\mathbb{E}\) and they map into \(\bigcap_{j \in J} \mathbb{F}_j\). Moreover, associativity, commutativity and distributivity of multiplication over addition hold in \(\bigcap_{j \in J} \mathbb{F}_j\), too. 0 and 1 are identity elements for addition and multiplication in \(\mathbb{E}\). Hence they are the identity elements for addition and multiplication in \(\bigcap_{j \in J} \mathbb{F}_j\).
Proof (concl.).
Proof (concl.). For inverses, let $x \in \bigcap_{j \in J} F_j$.

Then $x$ has a unique additive inverse $-x$ in $E$. Let $j \in J$ and let $y$ be the additive inverse of $x$ in $F_j$. Then $y = y + 0 = y + (x + (-x)) = (y + x) + (-x) = 0 + (-x) = -x$.

Because $j \in J$ was arbitrary, we conclude that $-x \in \bigcap_{j \in J} F_j$.

Thus $\bigcap_{j \in J} F_j$ contains additive inverses. Multiplicative inverses are handled similarly.
Proof (concl.). For inverses, let $x \in \bigcap_{j \in J} F_j$. Then $x$ has a unique additive inverse $-x$ in $E$. 
Proof (concl.). For inverses, let $x \in \bigcap_{j \in J} F_j$. Then $x$ has a unique additive inverse $-x$ in $E$. Let $j \in J$ and let $y$ be the additive inverse of $x$ in $F_j$. Then

$$y = y + 0 = y + (x + (-x)) = (y + x) + (-x) = 0 + (-x) = -x.$$ 

Because $j \in J$ was arbitrary, we conclude that $-x \in \bigcap_{j \in J} F_j$. Thus $\bigcap_{j \in J} F_j$ contains additive inverses. Multiplicative inverses are handled similarly.
**Proof (concl.).** For inverses, let $x \in \bigcap_{j \in J} \mathbb{F}_j$. Then $x$ has a unique additive inverse $-x$ in $\mathbb{E}$. Let $j \in J$ and let $y$ be the additive inverse of $x$ in $\mathbb{F}_j$. Then

$$y = y + 0 = y + (x + (-x)) = (y + x) + (-x) = 0 + (-x) = -x.$$
Proof (concl.). For inverses, let \( x \in \bigcap_{j \in J} F_j \). Then \( x \) has a unique additive inverse \( -x \) in \( E \). Let \( j \in J \) and let \( y \) be the additive inverse of \( x \) in \( F_j \). Then
\[
y = y + 0
\]
**Proof (concl.).** For inverses, let $x \in \bigcap_{j \in J} \mathbb{F}_j$. Then $x$ has a unique additive inverse $-x$ in $\mathbb{E}$. Let $j \in J$ and let $y$ be the additive inverse of $x$ in $\mathbb{F}_j$. Then

$$y = y + 0 = y + (x + (-x))$$
Proof (concl.). For inverses, let $x \in \bigcap_{j \in J} F_j$. Then $x$ has a unique additive inverse $-x$ in $E$. Let $j \in J$ and let $y$ be the additive inverse of $x$ in $F_j$. Then

$$y = y + 0 = y + (x + (-x)) = (y + x) + (-x)$$
Proof (concl.). For inverses, let $x \in \bigcap_{j \in J} \mathbb{F}_j$. Then $x$ has a unique additive inverse $-x$ in $\mathbb{E}$. Let $j \in J$ and let $y$ be the additive inverse of $x$ in $\mathbb{F}_j$. Then

$$y = y + 0 = y + (x + (-x)) = (y + x) + (-x) = 0 + (-x)$$
Proof (concl.). For inverses, let $x \in \bigcap_{j \in J} F_j$. Then $x$ has a unique additive inverse $-x$ in $E$. Let $j \in J$ and let $y$ be the additive inverse of $x$ in $F_j$. Then

\[ y = y + 0 = y + (x + (-x)) = (y + x) + (-x) = 0 + (-x) = -x. \]
Proof (concl.). For inverses, let $x \in \bigcap_{j \in J} F_j$. Then $x$ has a unique additive inverse $-x$ in $E$. Let $j \in J$ and let $y$ be the additive inverse of $x$ in $F_j$. Then

$$y = y + 0 = y + (x + (-x)) = (y + x) + (-x) = 0 + (-x) = -x.$$ 

Because $j \in J$ was arbitrary, we conclude that $-x \in \bigcap_{j \in J} F_j$. 

Thus $\bigcap_{j \in J} F_j$ contains additive inverses. Multiplicative inverses are handled similarly.
**Proof (concl.).** For inverses, let \( x \in \bigcap_{j \in J} F_j \). Then \( x \) has a unique additive inverse \(-x\) in \( \mathbb{E} \). Let \( j \in J \) and let \( y \) be the additive inverse of \( x \) in \( F_j \). Then

\[
y = y + 0 = y + (x + (-x)) = (y + x) + (-x) = 0 + (-x) = -x.
\]

Because \( j \in J \) was arbitrary, we conclude that \(-x \in \bigcap_{j \in J} F_j \). Thus \( \bigcap_{j \in J} F_j \) contains additive inverses.
Proof (concl.). For inverses, let $x \in \bigcap_{j \in J} \mathbb{F}_j$. Then $x$ has a unique additive inverse $-x$ in $\mathbb{E}$. Let $j \in J$ and let $y$ be the additive inverse of $x$ in $\mathbb{F}_j$. Then

$$y = y + 0 = y + (x + (-x)) = (y + x) + (-x) = 0 + (-x) = -x.$$ 

Because $j \in J$ was arbitrary, we conclude that $-x \in \bigcap_{j \in J} \mathbb{F}_j$. Thus $\bigcap_{j \in J} \mathbb{F}_j$ contains additive inverses. Multiplicative inverses are handled similarly.
Proof (concl.). For inverses, let \( x \in \bigcap_{j \in J} F_j \). Then \( x \) has a unique additive inverse \(-x\) in \( E \). Let \( j \in J \) and let \( y \) be the additive inverse of \( x \) in \( F_j \). Then
\[
y = y + 0 = y + (x + (-x)) = (y + x) + (-x) = 0 + (-x) = -x.
\]
Because \( j \in J \) was arbitrary, we conclude that \(-x \in \bigcap_{j \in J} F_j \). Thus \( \bigcap_{j \in J} F_j \) contains additive inverses. Multiplicative inverses are handled similarly.

\[\blacksquare\]
Definition.

Let \((F, +, \cdot)\) be a field, let \(p \in F[x]\) be a polynomial over \(F\) and let \(E\) be an extension of \(F\). Then \(f\) splits in the extension field \(E \supseteq F\) iff \(p\) can be factored into linear factors with coefficients in \(E[x]\).

Now let \(F\) be a field, let \(p \in F[x]\) and let \(E\) be an extension field in which \(p\) splits. Then the field \(S := \bigcap\{D : D\ is\ an\ extension\ field\ of\ F, \ D \subseteq E, \ p\ splits\ in\ D\}\) is called the splitting field for \(p\) over \(F\).

(We will address the fact that we say "the" in the next presentation.)
Definition. Let \((\mathbb{F}, +, \cdot)\) be a field, let \(p \in \mathbb{F}[x]\) be a polynomial over \(\mathbb{F}\) and let \(\mathbb{E}\) be an extension of \(\mathbb{F}\).
**Definition.** Let \((\mathbb{F}, +, \cdot)\) be a field, let \(p \in \mathbb{F}[x]\) be a polynomial over \(\mathbb{F}\) and let \(\mathbb{E}\) be an extension of \(\mathbb{F}\). Then \(f\) **splits** in the extension field \(\mathbb{E} \supseteq \mathbb{F}\) iff \(p\) can be factored into linear factors with coefficients in \(\mathbb{E}[x]\).
**Definition.** Let \((\mathbb{F}, +, \cdot)\) be a field, let \(p \in \mathbb{F}[x]\) be a polynomial over \(\mathbb{F}\) and let \(\mathbb{E}\) be an extension of \(\mathbb{F}\). Then \(f\) **splits** in the extension field \(\mathbb{E} \supseteq \mathbb{F}\) iff \(p\) can be factored into linear factors with coefficients in \(\mathbb{E}[x]\).

Now let \(\mathbb{F}\) be a field, let \(p \in \mathbb{F}[x]\) and let \(\mathbb{E}\) be an extension field in which \(p\) splits.
Definition. Let \((F, +, \cdot)\) be a field, let \(p \in F[x]\) be a polynomial over \(F\) and let \(E\) be an extension of \(F\). Then \(f\) \textbf{splits in the} extension field \(E \supseteq F\) iff \(p\) can be factored into linear factors with coefficients in \(E[x]\).

Now let \(F\) be a field, let \(p \in F[x]\) and let \(E\) be an extension field in which \(p\) splits. Then the field
\[
S := \bigcap \{D : D \text{ is an extension field of } F, D \subseteq E, p \text{ splits in } D\}
\]
**Definition.** Let \((\mathbb{F}, +, \cdot)\) be a field, let \(p \in \mathbb{F}[x]\) be a polynomial over \(\mathbb{F}\) and let \(\mathbb{E}\) be an extension of \(\mathbb{F}\). Then \(f\) **splits in the extension field** \(\mathbb{E} \supseteq \mathbb{F}\) iff \(p\) can be factored into linear factors with coefficients in \(\mathbb{E}[x]\).

Now let \(\mathbb{F}\) be a field, let \(p \in \mathbb{F}[x]\) and let \(\mathbb{E}\) be an extension field in which \(p\) splits. Then the field
\[
S := \bigcap \{D : D \text{ is an extension field of } \mathbb{F}, D \subseteq \mathbb{E}, p \text{ splits in } D\}
\]
is called the **splitting field** for \(p\) over \(\mathbb{F}\).
**Definition.** Let \((F, +, \cdot)\) be a field, let \(p \in F[x]\) be a polynomial over \(F\) and let \(E\) be an extension of \(F\). Then \(f\) splits in the extension field \(E \supseteq F\) iff \(p\) can be factored into linear factors with coefficients in \(E[x]\).

Now let \(F\) be a field, let \(p \in F[x]\) and let \(E\) be an extension field in which \(p\) splits. Then the field
\[
S := \bigcap \{D : D\text{ is an extension field of } F, D \subseteq E, p\text{ splits in } D\}
\]
is called the **splitting field** for \(p\) over \(F\).

(We will address the fact that we say “the” in the next presentation.)
Definition.

Let \((F, +, \cdot)\) be a field, let \(E\) be an extension of \(F\) and let \(\theta_1, \ldots, \theta_n \in E \setminus F\).

We define \(F(\theta_1, \ldots, \theta_n)\) to be the intersection of all subfields of \(E\) that contain \(F\) and \(\theta_1, \ldots, \theta_n\).

Then \(F(\theta_1, \ldots, \theta_n)\) is called the field \(F\) with the elements \(\theta_1, \ldots, \theta_n\) adjoined.

Example. \(\mathbb{C} = \mathbb{R}(i)\).

Theorem. Let \((F, +, \cdot)\) be a field, let \(E\) be an extension of \(F\) and let \(\theta_1, \ldots, \theta_n \in E \setminus F\).

Then the elements of \(F(\theta_1, \ldots, \theta_n)\) are rational combinations of the \(\theta_j\), where a rational combination is formed from elements of \(F\) and the \(\theta_1, \ldots, \theta_n\) using sums, products, additive inversions and multiplicative inversions (except divisions by zero).
**Definition.** Let \((\mathbb{F}, +, \cdot)\) be a field, let \(\mathbb{E}\) be an extension of \(\mathbb{F}\) and let \(\theta_1, \ldots, \theta_n \in \mathbb{E} \setminus \mathbb{F}\). Then \(\mathbb{F}(\theta_1, \ldots, \theta_n)\) is called the field with the elements \(\theta_1, \ldots, \theta_n\) adjoined.
**Definition.** Let \((\mathbb{F}, +, \cdot)\) be a field, let \(\mathbb{E}\) be an extension of \(\mathbb{F}\) and let \(\theta_1, \ldots, \theta_n \in \mathbb{E} \setminus \mathbb{F}\). We define \(\mathbb{F}(\theta_1, \ldots, \theta_n)\) to be the intersection of all subfields of \(\mathbb{E}\) that contain \(\mathbb{F}\) and \(\theta_1, \ldots, \theta_n\).
**Definition.** Let \((F, +, \cdot)\) be a field, let \(E\) be an extension of \(F\) and let \(\theta_1, \ldots, \theta_n \in E \setminus F\). We define \(F(\theta_1, \ldots, \theta_n)\) to be the intersection of all subfields of \(E\) that contain \(F\) and \(\theta_1, \ldots, \theta_n\). Then \(F(\theta_1, \ldots, \theta_n)\) is called the field \(F\) with the elements \(\theta_1, \ldots, \theta_n\) adjoined.
**Definition.** Let \((F, +, \cdot)\) be a field, let \(E\) be an extension of \(F\) and let \(\theta_1, \ldots, \theta_n \in E \setminus F\). We define \(F(\theta_1, \ldots, \theta_n)\) to be the intersection of all subfields of \(E\) that contain \(F\) and \(\theta_1, \ldots, \theta_n\). Then \(F(\theta_1, \ldots, \theta_n)\) is called the field \(F\) with the elements \(\theta_1, \ldots, \theta_n\) adjoined.

**Example.**
**Definition.** Let \((F, +, \cdot)\) be a field, let \(E\) be an extension of \(F\) and let \(\theta_1, \ldots, \theta_n \in E \setminus F\). We define \(F(\theta_1, \ldots, \theta_n)\) to be the intersection of all subfields of \(E\) that contain \(F\) and \(\theta_1, \ldots, \theta_n\). Then \(F(\theta_1, \ldots, \theta_n)\) is called the field \(F\) with the elements \(\theta_1, \ldots, \theta_n\) adjoined.

**Example.** \(\mathbb{C} = \mathbb{R}(i)\).
**Definition.** Let $(\mathbb{F}, +, \cdot)$ be a field, let $\mathbb{E}$ be an extension of $\mathbb{F}$ and let $\theta_1, \ldots, \theta_n \in \mathbb{E} \setminus \mathbb{F}$. We define $\mathbb{F}(\theta_1, \ldots, \theta_n)$ to be the intersection of all subfields of $\mathbb{E}$ that contain $\mathbb{F}$ and $\theta_1, \ldots, \theta_n$. Then $\mathbb{F}(\theta_1, \ldots, \theta_n)$ is called the field $\mathbb{F}$ with the elements $\theta_1, \ldots, \theta_n$ adjoined.

**Example.** $\mathbb{C} = \mathbb{R}(i)$.

**Theorem.**
**Definition.** Let \((F, +, \cdot)\) be a field, let \(E\) be an extension of \(F\) and let \(\theta_1, \ldots, \theta_n \in E \setminus F\). We define \(F(\theta_1, \ldots, \theta_n)\) to be the intersection of all subfields of \(E\) that contain \(F\) and \(\theta_1, \ldots, \theta_n\). Then \(F(\theta_1, \ldots, \theta_n)\) is called the field \(F\) with the elements \(\theta_1, \ldots, \theta_n\) adjoined.

**Example.** \(C = \mathbb{R}(i)\).

**Theorem.** Let \((F, +, \cdot)\) be a field, let \(E\) be an extension of \(F\) and let \(\theta_1, \ldots, \theta_n \in E \setminus F\).
Definition. Let \((\mathbb{F}, +, \cdot)\) be a field, let \(\mathbb{E}\) be an extension of \(\mathbb{F}\) and let \(\theta_1, \ldots, \theta_n \in \mathbb{E} \setminus \mathbb{F}\). We define \(\mathbb{F}(\theta_1, \ldots, \theta_n)\) to be the intersection of all subfields of \(\mathbb{E}\) that contain \(\mathbb{F}\) and \(\theta_1, \ldots, \theta_n\). Then \(\mathbb{F}(\theta_1, \ldots, \theta_n)\) is called the field \(\mathbb{F}\) with the elements \(\theta_1, \ldots, \theta_n\) adjoined.

Example. \(\mathbb{C} = \mathbb{R}(i)\).

Theorem. Let \((\mathbb{F}, +, \cdot)\) be a field, let \(\mathbb{E}\) be an extension of \(\mathbb{F}\) and let \(\theta_1, \ldots, \theta_n \in \mathbb{E} \setminus \mathbb{F}\). Then the elements of \(\mathbb{F}(\theta_1, \ldots, \theta_n)\) are rational combinations of the \(\theta_j\).
**Definition.** Let $(F, +, ·)$ be a field, let $E$ be an extension of $F$ and let $\theta_1, \ldots, \theta_n \in E \setminus F$. We define $F(\theta_1, \ldots, \theta_n)$ to be the intersection of all subfields of $E$ that contain $F$ and $\theta_1, \ldots, \theta_n$. Then $F(\theta_1, \ldots, \theta_n)$ is called the field $F$ with the elements $\theta_1, \ldots, \theta_n$ adjoined.

**Example.** $C = \mathbb{R}(i)$.

**Theorem.** Let $(F, +, ·)$ be a field, let $E$ be an extension of $F$ and let $\theta_1, \ldots, \theta_n \in E \setminus F$. Then the elements of $F(\theta_1, \ldots, \theta_n)$ are rational combinations of the $\theta_j$, where a rational combination is formed from elements of $F$ and the $\theta_1, \ldots, \theta_n$ using sums, products, additive inversions and multiplicative inversions (except divisions by zero).
**Definition.** Let \((F, +, \cdot)\) be a field, let \(E\) be an extension of \(F\) and let \(\theta_1, \ldots, \theta_n \in E \setminus F\). We define \(F(\theta_1, \ldots, \theta_n)\) to be the intersection of all subfields of \(E\) that contain \(F\) and \(\theta_1, \ldots, \theta_n\). Then \(F(\theta_1, \ldots, \theta_n)\) is called the field \(F\) with the elements \(\theta_1, \ldots, \theta_n\) adjoined.

**Example.** \(\mathbb{C} = \mathbb{R}(i)\).

**Theorem.** Let \((F, +, \cdot)\) be a field, let \(E\) be an extension of \(F\) and let \(\theta_1, \ldots, \theta_n \in E \setminus F\). Then the elements of \(F(\theta_1, \ldots, \theta_n)\) are rational combinations of the \(\theta_j\), where a rational combination is formed from elements of \(F\) and the \(\theta_1, \ldots, \theta_n\) using sums.
**Definition.** Let \((\mathbb{F}, +, \cdot)\) be a field, let \(\mathbb{E}\) be an extension of \(\mathbb{F}\) and let \(\theta_1, \ldots, \theta_n \in \mathbb{E} \setminus \mathbb{F}\). We define \(\mathbb{F}(\theta_1, \ldots, \theta_n)\) to be the intersection of all subfields of \(\mathbb{E}\) that contain \(\mathbb{F}\) and \(\theta_1, \ldots, \theta_n\). Then \(\mathbb{F}(\theta_1, \ldots, \theta_n)\) is called the field \(\mathbb{F}\) with the elements \(\theta_1, \ldots, \theta_n\) adjoined.

**Example.** \(\mathbb{C} = \mathbb{R}(i)\).

**Theorem.** Let \((\mathbb{F}, +, \cdot)\) be a field, let \(\mathbb{E}\) be an extension of \(\mathbb{F}\) and let \(\theta_1, \ldots, \theta_n \in \mathbb{E} \setminus \mathbb{F}\). Then the elements of \(\mathbb{F}(\theta_1, \ldots, \theta_n)\) are rational combinations of the \(\theta_j\), where a rational combination is formed from elements of \(\mathbb{F}\) and the \(\theta_1, \ldots, \theta_n\) using sums, products.
Definition. Let \((\mathbb{F}, +, \cdot)\) be a field, let \(\mathbb{E}\) be an extension of \(\mathbb{F}\) and let \(\theta_1, \ldots, \theta_n \in \mathbb{E} \setminus \mathbb{F}\). We define \(\mathbb{F}(\theta_1, \ldots, \theta_n)\) to be the intersection of all subfields of \(\mathbb{E}\) that contain \(\mathbb{F}\) and \(\theta_1, \ldots, \theta_n\). Then \(\mathbb{F}(\theta_1, \ldots, \theta_n)\) is called the field \(\mathbb{F}\) with the elements \(\theta_1, \ldots, \theta_n\) adjoined.

Example. \(\mathbb{C} = \mathbb{R}(i)\).

Theorem. Let \((\mathbb{F}, +, \cdot)\) be a field, let \(\mathbb{E}\) be an extension of \(\mathbb{F}\) and let \(\theta_1, \ldots, \theta_n \in \mathbb{E} \setminus \mathbb{F}\). Then the elements of \(\mathbb{F}(\theta_1, \ldots, \theta_n)\) are rational combinations of the \(\theta_j\), where a rational combination is formed from elements of \(\mathbb{F}\) and the \(\theta_1, \ldots, \theta_n\) using sums, products, additive inversions and multiplicative inversions (except divisions by zero).
**Definition.** Let \((F, +, \cdot)\) be a field, let \(E\) be an extension of \(F\) and let \(\theta_1, \ldots, \theta_n \in E \setminus F\). We define \(F(\theta_1, \ldots, \theta_n)\) to be the intersection of all subfields of \(E\) that contain \(F\) and \(\theta_1, \ldots, \theta_n\). Then \(F(\theta_1, \ldots, \theta_n)\) is called the field \(F\) with the elements \(\theta_1, \ldots, \theta_n\) adjoined.

**Example.** \(\mathbb{C} = \mathbb{R}(i)\).

**Theorem.** Let \((F, +, \cdot)\) be a field, let \(E\) be an extension of \(F\) and let \(\theta_1, \ldots, \theta_n \in E \setminus F\). Then the elements of \(F(\theta_1, \ldots, \theta_n)\) are rational combinations of the \(\theta_j\), where a rational combination is formed from elements of \(F\) and the \(\theta_1, \ldots, \theta_n\) using sums, products, additive inversions and multiplicative inversions.
**Definition.** Let \((F, +, \cdot)\) be a field, let \(E\) be an extension of \(F\) and let \(\theta_1, \ldots, \theta_n \in E \setminus F\). We define \(F(\theta_1, \ldots, \theta_n)\) to be the intersection of all subfields of \(E\) that contain \(F\) and \(\theta_1, \ldots, \theta_n\). Then \(F(\theta_1, \ldots, \theta_n)\) is called the field \(F\) with the elements \(\theta_1, \ldots, \theta_n\) adjoined.

**Example.** \(\mathbb{C} = \mathbb{R}(i)\).

**Theorem.** Let \((F, +, \cdot)\) be a field, let \(E\) be an extension of \(F\) and let \(\theta_1, \ldots, \theta_n \in E \setminus F\). Then the elements of \(F(\theta_1, \ldots, \theta_n)\) are rational combinations of the \(\theta_j\), where a rational combination is formed from elements of \(F\) and the \(\theta_1, \ldots, \theta_n\) using sums, products, additive inversions and multiplicative inversions (except divisions by zero).
Proof.

A polynomial combination is formed from the elements of \( F \) and \( \theta_1, \ldots, \theta_n \) using sums, products and additive inversions.

We first prove by induction on the total number of operations (sums, products, additive and multiplicative inversions) needed to form a rational combination \( r \) that

\[
    r = \frac{p}{q},
\]

where \( p \) and \( q \) are polynomial combinations.

For \( k = 0 \): Trivial:

\[
    r \in F \cup \{ \theta_1, \ldots, \theta_n \}
\]

and

\[
    r = r_1.
\]

Induction step, \( k > 0 \): Let \( r \) be a rational combination.

First case: \( r = r_1 + r_2 \), where \( r_1 \) and \( r_2 \) are rational combinations.

Both \( r_1 \) and \( r_2 \) were formed using fewer than \( k \) operations.

By induction hypothesis, for \( j = 1, 2 \) we have

\[
    r_j = \frac{p_j}{q_j},
\]

where \( p_j \) and \( q_j \) are polynomial combinations.

Now

\[
    r = r_1 + r_2 = \frac{p_1}{q_1} + \frac{p_2}{q_2} = \frac{p_1 q_2 + p_2 q_1}{q_1 q_2}.
\]
**Proof.** A polynomial combination is formed from the elements of $\mathbb{F}$ and $\theta_1, \ldots, \theta_n$ using sums, products and additive inversions.
Proof. A polynomial combination is formed from the elements of $\mathbb{F}$ and $\theta_1, \ldots, \theta_n$ using sums, products and additive inversions. We first prove by induction on the total number $k$ of operations (sums, products, additive and multiplicative inversions) needed to form a rational combination $r$ that $r = \frac{p}{q}$, where $p$ and $q$ are polynomial combinations.
Proof. A polynomial combination is formed from the elements of $\mathbb{F}$ and $\theta_1, \ldots, \theta_n$ using sums, products and additive inversions. We first prove by induction on the total number $k$ of operations (sums, products, additive and multiplicative inversions) needed to form a rational combination $r$ that $r = \frac{p}{q}$, where $p$ and $q$ are polynomial combinations.

$k = 0$
**Proof.** A polynomial combination is formed from the elements of $\mathbb{F}$ and $\theta_1, \ldots, \theta_n$ using sums, products and additive inversions. We first prove by induction on the total number $k$ of operations (sums, products, additive and multiplicative inversions) needed to form a rational combination $r$ that $r = \frac{p}{q}$, where $p$ and $q$ are polynomial combinations.

$k = 0$: Trivial
**Proof.** A polynomial combination is formed from the elements of $\mathbb{F}$ and $\theta_1, \ldots, \theta_n$ using sums, products and additive inversions. We first prove by induction on the total number $k$ of operations (sums, products, additive and multiplicative inversions) needed to form a rational combination $r$ that $r = \frac{p}{q}$, where $p$ and $q$ are polynomial combinations.

$k = 0$: Trivial: $r \in \mathbb{F} \cup \{\theta_1, \ldots, \theta_n\}$ and $r = \frac{r}{1}$. 
**Proof.** A polynomial combination is formed from the elements of $\mathbb{F}$ and $\theta_1, \ldots, \theta_n$ using sums, products and additive inversions. We first prove by induction on the total number $k$ of operations (sums, products, additive and multiplicative inversions) needed to form a rational combination $r$ that $r = \frac{p}{q}$, where $p$ and $q$ are polynomial combinations.

$k = 0$: Trivial: $r \in \mathbb{F} \cup \{\theta_1, \ldots, \theta_n\}$ and $r = \frac{r}{1}$.

*Induction step, $k > 0$:*
Proof. A polynomial combination is formed from the elements of $\mathbb{F}$ and $\theta_1, \ldots, \theta_n$ using sums, products and additive inversions. We first prove by induction on the total number $k$ of operations (sums, products, additive and multiplicative inversions) needed to form a rational combination $r$ that $r = \frac{p}{q}$, where $p$ and $q$ are polynomial combinations.

$k = 0$: Trivial: $r \in \mathbb{F} \cup \{\theta_1, \ldots, \theta_n\}$ and $r = \frac{r}{1}$.

Induction step, $k > 0$: Let $r$ be a rational combination.
Proof. A polynomial combination is formed from the elements of $\mathbb{F}$ and $\theta_1, \ldots, \theta_n$ using sums, products and additive inversions. We first prove by induction on the total number $k$ of operations (sums, products, additive and multiplicative inversions) needed to form a rational combination $r$ that $r = \frac{p}{q}$, where $p$ and $q$ are polynomial combinations.

$k = 0$: Trivial: $r \in \mathbb{F} \cup \{\theta_1, \ldots, \theta_n\}$ and $r = \frac{r}{1}$.

Induction step, $k > 0$: Let $r$ be a rational combination. First case: $r = r_1 + r_2$, where $r_1$ and $r_2$ are rational combinations.
**Proof.** A polynomial combination is formed from the elements of $\mathbb{F}$ and $\theta_1, \ldots, \theta_n$ using sums, products and additive inversions. We first prove by induction on the total number $k$ of operations (sums, products, additive and multiplicative inversions) needed to form a rational combination $r$ that $r = \frac{p}{q}$, where $p$ and $q$ are polynomial combinations.

$k = 0$: Trivial: $r \in \mathbb{F} \cup \{\theta_1, \ldots, \theta_n\}$ and $r = \frac{r}{1}$.

*Induction step, $k > 0$: Let $r$ be a rational combination. First case: $r = r_1 + r_2$, where $r_1$ and $r_2$ are rational combinations. Both $r_1$ and $r_2$ were formed using fewer than $k$ operations.
Proof. A polynomial combination is formed from the elements of $\mathbb{F}$ and $\theta_1, \ldots, \theta_n$ using sums, products and additive inversions. We first prove by induction on the total number $k$ of operations (sums, products, additive and multiplicative inversions) needed to form a rational combination $r$ that $r = \frac{p}{q}$, where $p$ and $q$ are polynomial combinations.

$k = 0$: Trivial: $r \in \mathbb{F} \cup \{\theta_1, \ldots, \theta_n\}$ and $r = \frac{r}{1}$.

Induction step, $k > 0$: Let $r$ be a rational combination. First case: $r = r_1 + r_2$, where $r_1$ and $r_2$ are rational combinations. Both $r_1$ and $r_2$ were formed using fewer than $k$ operations. By induction hypothesis, for $j = 1, 2$ we have $r_j = \frac{p_j}{q_j}$, where $p_j$ and $q_j$ are polynomial combinations.
**Proof.** A polynomial combination is formed from the elements of \( \mathbb{F} \) and \( \theta_1, \ldots, \theta_n \) using sums, products and additive inversions. We first prove by induction on the total number \( k \) of operations (sums, products, additive and multiplicative inversions) needed to form a rational combination \( r \) that \( r = \frac{p}{q} \), where \( p \) and \( q \) are polynomial combinations.

\( k = 0 \): Trivial: \( r \in \mathbb{F} \cup \{ \theta_1, \ldots, \theta_n \} \) and \( r = \frac{r}{1} \).

**Induction step, \( k > 0 \):** Let \( r \) be a rational combination. First case: \( r = r_1 + r_2 \), where \( r_1 \) and \( r_2 \) are rational combinations. Both \( r_1 \) and \( r_2 \) were formed using fewer than \( k \) operations. By induction hypothesis, for \( j = 1, 2 \) we have \( r_j = \frac{p_j}{q_j} \), where \( p_j \) and \( q_j \) are polynomial combinations. Now

\( r \)
**Proof.** A polynomial combination is formed from the elements of $\mathbb{F}$ and $\theta_1, \ldots, \theta_n$ using sums, products and additive inversions. We first prove by induction on the total number $k$ of operations (sums, products, additive and multiplicative inversions) needed to form a rational combination $r$ that $r = \frac{p}{q}$, where $p$ and $q$ are polynomial combinations.

$k = 0$: Trivial: $r \in \mathbb{F} \cup \{\theta_1, \ldots, \theta_n\}$ and $r = \frac{r}{1}$.

**Induction step, $k > 0$:** Let $r$ be a rational combination. First case: $r = r_1 + r_2$, where $r_1$ and $r_2$ are rational combinations. Both $r_1$ and $r_2$ were formed using fewer than $k$ operations. By induction hypothesis, for $j = 1, 2$ we have $r_j = \frac{p_j}{q_j}$, where $p_j$ and $q_j$ are polynomial combinations. Now

$$r = r_1 + r_2$$
Proof. A polynomial combination is formed from the elements of \( \mathbb{F} \) and \( \theta_1, \ldots, \theta_n \) using sums, products and additive inversions. We first prove by induction on the total number \( k \) of operations (sums, products, additive and multiplicative inversions) needed to form a rational combination \( r \) that \( r = \frac{p}{q} \), where \( p \) and \( q \) are polynomial combinations.

\( k = 0 \): Trivial: \( r \in \mathbb{F} \cup \{ \theta_1, \ldots, \theta_n \} \) and \( r = \frac{r}{1} \).

Induction step, \( k > 0 \): Let \( r \) be a rational combination. First case: \( r = r_1 + r_2 \), where \( r_1 \) and \( r_2 \) are rational combinations. Both \( r_1 \) and \( r_2 \) were formed using fewer than \( k \) operations. By induction hypothesis, for \( j = 1, 2 \) we have \( r_j = \frac{p_j}{q_j} \), where \( p_j \) and \( q_j \) are polynomial combinations. Now

\[
r = r_1 + r_2 = \frac{p_1}{q_1} + \frac{p_2}{q_2}.
\]
**Proof.** A polynomial combination is formed from the elements of $\mathbb{F}$ and $\theta_1, \ldots, \theta_n$ using sums, products and additive inversions. We first prove by induction on the total number $k$ of operations (sums, products, additive and multiplicative inversions) needed to form a rational combination $r$ that $r = \frac{p}{q}$, where $p$ and $q$ are polynomial combinations.

$k = 0$: Trivial: $r \in \mathbb{F} \cup \{\theta_1, \ldots, \theta_n\}$ and $r = \frac{r}{1}$.

*Induction step, $k > 0$: * Let $r$ be a rational combination. First case: $r = r_1 + r_2$, where $r_1$ and $r_2$ are rational combinations. Both $r_1$ and $r_2$ were formed using fewer than $k$ operations. By induction hypothesis, for $j = 1, 2$ we have $r_j = \frac{p_j}{q_j}$, where $p_j$ and $q_j$ are polynomial combinations. Now

$$r = r_1 + r_2 = \frac{p_1}{q_1} + \frac{p_2}{q_2} = \frac{p_1q_2 + p_2q_1}{q_1q_2}.$$
Proof (concl.).
Proof (concl.). The arguments for $r = r_1 \cdot r_2$, $r = -r_1$ and $r = (r_1)^{-1}$ (for $r_1 \neq 0$) are similar.
Proof (concl.). The arguments for $r = r_1 \cdot r_2$, $r = -r_1$ and $r = (r_1)^{-1}$ (for $r_1 \neq 0$) are similar.
It is now easy to verify that the rational combinations are a field
**Proof (concl.).** The arguments for \( r = r_1 \cdot r_2, r = -r_1 \) and \( r = (r_1)^{-1} \) (for \( r_1 \neq 0 \)) are similar.

It is now easy to verify that the rational combinations are a field and that every subfield of \( \mathbb{E} \) that contains \( \mathbb{F} \cup \{ \theta_1, \ldots, \theta_n \} \) contains all rational combinations of the \( \theta_j \).
Proof (concl.). The arguments for $r = r_1 \cdot r_2$, $r = -r_1$ and $r = (r_1)^{-1}$ (for $r_1 \neq 0$) are similar.

It is now easy to verify that the rational combinations are a field and that every subfield of $\mathbb{E}$ that contains $\mathbb{F} \cup \{\theta_1, \ldots, \theta_n\}$ contains all rational combinations of the $\theta_j$. (Good exercise.)
**Proof (concl.).** The arguments for $r = r_1 \cdot r_2$, $r = -r_1$ and $r = (r_1)^{-1}$ (for $r_1 \neq 0$) are similar.

It is now easy to verify that the rational combinations are a field and that every subfield of $\mathbb{E}$ that contains $\mathbb{F} \cup \{\theta_1, \ldots, \theta_n\}$ contains all rational combinations of the $\theta_j$. (Good exercise.) ■
**Proposition.**
**Proposition.** Let \((\mathbb{F}, +, \cdot)\) be a field, let \(p \in \mathbb{F}[x]\) be a polynomial over \(\mathbb{F}\), let \(\mathbb{E}\) be an extension of \(\mathbb{F}\) that splits \(p\) and let \(\theta_1, \ldots, \theta_n \in \mathbb{E} \setminus \mathbb{F}\) be the zeros of \(p\) that are not in \(\mathbb{F}\). Then \(\mathbb{F}(\theta_1, \ldots, \theta_n)\) is the splitting field for \(p\) over \(\mathbb{F}\).
Proposition. Let \((\mathbb{F}, +, \cdot)\) be a field, let \(p \in \mathbb{F}[x]\) be a polynomial over \(\mathbb{F}\), let \(\mathbb{E}\) be an extension of \(\mathbb{F}\) that splits \(p\) and let \(\theta_1, \ldots, \theta_n \in \mathbb{E} \setminus \mathbb{F}\) be the zeros of \(p\) that are not in \(\mathbb{F}\). Then \(\mathbb{F}(\theta_1, \ldots, \theta_n)\) is the splitting field for \(p\) over \(\mathbb{F}\).
**Proposition.** Let $(\mathbb{F}, +, \cdot)$ be a field, let $p \in \mathbb{F}[x]$ be a polynomial over $\mathbb{F}$, let $\mathbb{E}$ be an extension of $\mathbb{F}$ that splits $p$ and let $\theta_1, \ldots, \theta_n \in \mathbb{E} \setminus \mathbb{F}$ be the zeros of $p$ that are not in $\mathbb{F}$. Then $\mathbb{F}(\theta_1, \ldots, \theta_n)$ is the splitting field for $p$ over $\mathbb{F}$.

**Proof.**
**Proposition.** Let $(\mathbb{F}, +, \cdot)$ be a field, let $p \in \mathbb{F}[x]$ be a polynomial over $\mathbb{F}$, let $\mathbb{E}$ be an extension of $\mathbb{F}$ that splits $p$ and let $\theta_1, \ldots, \theta_n \in \mathbb{E} \setminus \mathbb{F}$ be the zeros of $p$ that are not in $\mathbb{F}$. Then $\mathbb{F}(\theta_1, \ldots, \theta_n)$ is the splitting field for $p$ over $\mathbb{F}$.

**Proof.** Let $a_d \in \mathbb{F}$ be the leading coefficient of $p$
**Proposition.** Let $(\mathbb{F}, +, \cdot)$ be a field, let $p \in \mathbb{F}[x]$ be a polynomial over $\mathbb{F}$, let $\mathbb{E}$ be an extension of $\mathbb{F}$ that splits $p$ and let $\theta_1, \ldots, \theta_n \in \mathbb{E} \setminus \mathbb{F}$ be the zeros of $p$ that are not in $\mathbb{F}$. Then $\mathbb{F}(\theta_1, \ldots, \theta_n)$ is the splitting field for $p$ over $\mathbb{F}$.

**Proof.** Let $a_d \in \mathbb{F}$ be the leading coefficient of $p$, let $\theta_1, \ldots, \theta_n$ be the zeros of $p$ in $\mathbb{E} \setminus \mathbb{F}$.
**Proposition.** Let \((F, +, \cdot)\) be a field, let \(p \in F[x]\) be a polynomial over \(F\), let \(E\) be an extension of \(F\) that splits \(p\) and let \(\theta_1, \ldots, \theta_n \in E \setminus F\) be the zeros of \(p\) that are not in \(F\). Then \(F(\theta_1, \ldots, \theta_n)\) is the splitting field for \(p\) over \(F\).

**Proof.** Let \(a_d \in \mathbb{F}\) be the leading coefficient of \(p\), let \(\theta_1, \ldots, \theta_n\) be the zeros of \(p\) in \(E \setminus F\), let \(m_j\) be the multiplicity of \(\theta_j\).
**Proposition.** Let \((\mathbb{F}, +, \cdot)\) be a field, let \(p \in \mathbb{F}[x]\) be a polynomial over \(\mathbb{F}\), let \(\mathbb{E}\) be an extension of \(\mathbb{F}\) that splits \(p\) and let \(\theta_1, \ldots, \theta_n \in \mathbb{E} \setminus \mathbb{F}\) be the zeros of \(p\) that are not in \(\mathbb{F}\). Then \(\mathbb{F}(\theta_1, \ldots, \theta_n)\) is the splitting field for \(p\) over \(\mathbb{F}\).

**Proof.** Let \(a_d \in \mathbb{F}\) be the leading coefficient of \(p\), let \(\theta_1, \ldots, \theta_n\) be the zeros of \(p\) in \(\mathbb{E} \setminus \mathbb{F}\), let \(m_j\) be the multiplicity of \(\theta_j\), let \(\nu_1, \ldots, \nu_l\) be the zeros of \(p\) in \(\mathbb{F}\).
Proposition. Let $(\mathbb{F}, +, \cdot)$ be a field, let $p \in \mathbb{F}[x]$ be a polynomial over $\mathbb{F}$, let $\mathbb{E}$ be an extension of $\mathbb{F}$ that splits $p$ and let $\theta_1, \ldots, \theta_n \in \mathbb{E} \setminus \mathbb{F}$ be the zeros of $p$ that are not in $\mathbb{F}$. Then $\mathbb{F}(\theta_1, \ldots, \theta_n)$ is the splitting field for $p$ over $\mathbb{F}$.

Proof. Let $a_d \in \mathbb{F}$ be the leading coefficient of $p$, let $\theta_1, \ldots, \theta_n$ be the zeros of $p$ in $\mathbb{E} \setminus \mathbb{F}$, let $m_j$ be the multiplicity of $\theta_j$, let $\nu_1, \ldots, \nu_l$ be the zeros of $p$ in $\mathbb{F}$ and let $M_k$ be the multiplicity of $\nu_k$. 
**Proposition.** Let \((\mathbb{F}, +, \cdot)\) be a field, let \(p \in \mathbb{F}[x]\) be a polynomial over \(\mathbb{F}\), let \(\mathbb{E}\) be an extension of \(\mathbb{F}\) that splits \(p\) and let \(\theta_1, \ldots, \theta_n \in \mathbb{E} \setminus \mathbb{F}\) be the zeros of \(p\) that are not in \(\mathbb{F}\). Then \(\mathbb{F}(\theta_1, \ldots, \theta_n)\) is the splitting field for \(p\) over \(\mathbb{F}\).

**Proof.** Let \(a_d \in \mathbb{F}\) be the leading coefficient of \(p\), let \(\theta_1, \ldots, \theta_n\) be the zeros of \(p\) in \(\mathbb{E} \setminus \mathbb{F}\), let \(m_j\) be the multiplicity of \(\theta_j\), let \(\nu_1, \ldots, \nu_l\) be the zeros of \(p\) in \(\mathbb{F}\) and let \(M_k\) be the multiplicity of \(\nu_k\). Then \(p(x) = a_d \prod_{j=1}^{n} (x - \theta_j)^{m_j} \prod_{k=1}^{l} (x - \nu_k)^{M_k}\).
**Proposition.** Let $(\mathbb{F}, +, \cdot)$ be a field, let $p \in \mathbb{F}[x]$ be a polynomial over $\mathbb{F}$, let $\mathbb{E}$ be an extension of $\mathbb{F}$ that splits $p$ and let $\theta_1, \ldots, \theta_n \in \mathbb{E} \setminus \mathbb{F}$ be the zeros of $p$ that are not in $\mathbb{F}$. Then $\mathbb{F}(\theta_1, \ldots, \theta_n)$ is the splitting field for $p$ over $\mathbb{F}$.

**Proof.** Let $a_d \in \mathbb{F}$ be the leading coefficient of $p$, let $\theta_1, \ldots, \theta_n$ be the zeros of $p$ in $\mathbb{E} \setminus \mathbb{F}$, let $m_j$ be the multiplicity of $\theta_j$, let $\nu_1, \ldots, \nu_l$ be the zeros of $p$ in $\mathbb{F}$ and let $M_k$ be the multiplicity of $\nu_k$. Then $p(x) = a_d \prod_{j=1}^{n}(x - \theta_j)^{m_j} \prod_{k=1}^{l}(x - \nu_k)^{M_k}$. Because $a_d, \theta_1, \ldots, \theta_n, \nu_1, \ldots, \nu_l \in \mathbb{F}(\theta_1, \ldots, \theta_n)$, the polynomial $p$ splits in $\mathbb{F}(\theta_1, \ldots, \theta_n)$. 
**Proposition.** Let \((\mathbb{F}, +, \cdot)\) be a field, let \(p \in \mathbb{F}[x]\) be a polynomial over \(\mathbb{F}\), let \(\mathbb{E}\) be an extension of \(\mathbb{F}\) that splits \(p\) and let \(\theta_1, \ldots, \theta_n \in \mathbb{E} \setminus \mathbb{F}\) be the zeros of \(p\) that are not in \(\mathbb{F}\). Then \(\mathbb{F}(\theta_1, \ldots, \theta_n)\) is the splitting field for \(p\) over \(\mathbb{F}\).

**Proof.** Let \(a_d \in \mathbb{F}\) be the leading coefficient of \(p\), let \(\theta_1, \ldots, \theta_n\) be the zeros of \(p\) in \(\mathbb{E} \setminus \mathbb{F}\), let \(m_j\) be the multiplicity of \(\theta_j\), let \(\nu_1, \ldots, \nu_l\) be the zeros of \(p\) in \(\mathbb{F}\) and let \(M_k\) be the multiplicity of \(\nu_k\). Then \(p(x) = a_d \prod_{j=1}^{n} (x - \theta_j)^{m_j} \prod_{k=1}^{l} (x - \nu_k)^{M_k}\). Because \(a_d, \theta_1, \ldots, \theta_n, \nu_1, \ldots, \nu_l \in \mathbb{F}(\theta_1, \ldots, \theta_n)\), the polynomial \(p\) splits in \(\mathbb{F}(\theta_1, \ldots, \theta_n)\). Moreover, every field \(\mathbb{G}\) with \(\mathbb{F} \subseteq \mathbb{G} \subseteq \mathbb{E}\) in which \(p\) splits must contain \(\theta_1, \ldots, \theta_n\).
Proposition. Let \((\mathbb{F}, +, \cdot)\) be a field, let \(p \in \mathbb{F}[x]\) be a polynomial over \(\mathbb{F}\), let \(\mathbb{E}\) be an extension of \(\mathbb{F}\) that splits \(p\) and let \(\theta_1, \ldots, \theta_n \in \mathbb{E} \setminus \mathbb{F}\) be the zeros of \(p\) that are not in \(\mathbb{F}\). Then \(\mathbb{F}(\theta_1, \ldots, \theta_n)\) is the splitting field for \(p\) over \(\mathbb{F}\).

Proof. Let \(a_d \in \mathbb{F}\) be the leading coefficient of \(p\), let \(\theta_1, \ldots, \theta_n\) be the zeros of \(p\) in \(\mathbb{E} \setminus \mathbb{F}\), let \(m_j\) be the multiplicity of \(\theta_j\), let \(\nu_1, \ldots, \nu_l\) be the zeros of \(p\) in \(\mathbb{F}\) and let \(M_k\) be the multiplicity of \(\nu_k\). Then

\[
p(x) = a_d \prod_{j=1}^{n}(x - \theta_j)^{m_j} \prod_{k=1}^{l}(x - \nu_k)^{M_k}.
\]

Because \(a_d, \theta_1, \ldots, \theta_n, \nu_1, \ldots, \nu_l \in \mathbb{F}(\theta_1, \ldots, \theta_n)\), the polynomial \(p\) splits in \(\mathbb{F}(\theta_1, \ldots, \theta_n)\). Moreover, every field \(\mathbb{G}\) with \(\mathbb{F} \subseteq \mathbb{G} \subseteq \mathbb{E}\) in which \(p\) splits must contain \(\theta_1, \ldots, \theta_n\). Hence it must contain \(\mathbb{F}(\theta_1, \ldots, \theta_n)\).
Proposition. Let \((\mathbb{F}, +, \cdot)\) be a field, let \(p \in \mathbb{F}[x]\) be a polynomial over \(\mathbb{F}\), let \(\mathbb{E}\) be an extension of \(\mathbb{F}\) that splits \(p\) and let \(\theta_1, \ldots, \theta_n \in \mathbb{E} \setminus \mathbb{F}\) be the zeros of \(p\) that are not in \(\mathbb{F}\). Then \(\mathbb{F}(\theta_1, \ldots, \theta_n)\) is the splitting field for \(p\) over \(\mathbb{F}\).

Proof. Let \(a_d \in \mathbb{F}\) be the leading coefficient of \(p\), let \(\theta_1, \ldots, \theta_n\) be the zeros of \(p\) in \(\mathbb{E} \setminus \mathbb{F}\), let \(m_j\) be the multiplicity of \(\theta_j\), let \(\nu_1, \ldots, \nu_l\) be the zeros of \(p\) in \(\mathbb{F}\) and let \(M_k\) be the multiplicity of \(\nu_k\). Then \(p(x) = a_d \prod_{j=1}^{n} (x - \theta_j)^{m_j} \prod_{k=1}^{l} (x - \nu_k)^{M_k}\). Because \(a_d, \theta_1, \ldots, \theta_n, \nu_1, \ldots, \nu_l \in \mathbb{F}((\theta_1, \ldots, \theta_n)\), the polynomial \(p\) splits in \(\mathbb{F}((\theta_1, \ldots, \theta_n)\). Moreover, every field \(\mathbb{G}\) with \(\mathbb{F} \subseteq \mathbb{G} \subseteq \mathbb{E}\) in which \(p\) splits must contain \(\theta_1, \ldots, \theta_n\). Hence it must contain \(\mathbb{F}(\theta_1, \ldots, \theta_n)\). Thus \(\mathbb{F}(\theta_1, \ldots, \theta_n)\) is the splitting field for \(p\) over \(\mathbb{F}\).
Proposition. Let \((\mathbb{F}, +, \cdot)\) be a field, let \(p \in \mathbb{F}[x]\) be a polynomial over \(\mathbb{F}\), let \(\mathbb{E}\) be an extension of \(\mathbb{F}\) that splits \(p\) and let \(\theta_1, \ldots, \theta_n \in \mathbb{E} \setminus \mathbb{F}\) be the zeros of \(p\) that are not in \(\mathbb{F}\). Then \(\mathbb{F}(\theta_1, \ldots, \theta_n)\) is the splitting field for \(p\) over \(\mathbb{F}\).

Proof. Let \(a_d \in \mathbb{F}\) be the leading coefficient of \(p\), let \(\theta_1, \ldots, \theta_n\) be the zeros of \(p\) in \(\mathbb{E} \setminus \mathbb{F}\), let \(m_j\) be the multiplicity of \(\theta_j\), let \(\nu_1, \ldots, \nu_l\) be the zeros of \(p\) in \(\mathbb{F}\) and let \(M_k\) be the multiplicity of \(\nu_k\). Then \(p(x) = a_d \prod_{j=1}^{n} (x - \theta_j)^{m_j} \prod_{k=1}^{l} (x - \nu_k)^{M_k}\). Because \(a_d, \theta_1, \ldots, \theta_n, \nu_1, \ldots, \nu_l \in \mathbb{F}(\theta_1, \ldots, \theta_n)\), the polynomial \(p\) splits in \(\mathbb{F}(\theta_1, \ldots, \theta_n)\). Moreover, every field \(\mathbb{G}\) with \(\mathbb{F} \subseteq \mathbb{G} \subseteq \mathbb{E}\) in which \(p\) splits must contain \(\theta_1, \ldots, \theta_n\). Hence it must contain \(\mathbb{F}(\theta_1, \ldots, \theta_n)\). Thus \(\mathbb{F}(\theta_1, \ldots, \theta_n)\) is the splitting field for \(p\) over \(\mathbb{F}\).
Example.

$Q(\sqrt{2})$ is the splitting field for $p(x) = x^2 - 2$ over $Q$. Because $(\sqrt{2})^2 = 2$, the elements of $Q(\sqrt{2})$ are of the form $a + b\sqrt{2}$, with $a, b \in Q$. For each of these elements we have $c \in Q$ and $d\sqrt{2} \not\in Q$. Therefore $c \not\in \{\pm d\sqrt{2}\}$, and hence $c^2 - 2d^2 \neq 0$. Therefore $a + b\sqrt{2}c + d\sqrt{2}c^2 - 2d^2 = ac^2 - 2bd^2 + (bc - ad)c^2 - 2d^2\sqrt{2}$. Let $x : = ac^2 - 2bd^2$ and $y : = bc - ad$. The elements of $Q(\sqrt{2})$ are of the form $x + y\sqrt{2}$ with $x, y \in Q$. 
**Example.** $\mathbb{Q}(\sqrt{2})$ is the splitting field for $p(x) = x^2 - 2$ over $\mathbb{Q}$. 
**Example.** \( \mathbb{Q} \left( \sqrt{2} \right) \) is the splitting field for \( p(x) = x^2 - 2 \) over \( \mathbb{Q} \). Because \( \left( \sqrt{2} \right)^2 = 2 \), the elements of \( \mathbb{Q} \left( \sqrt{2} \right) \) are of the form \( \frac{a + b\sqrt{2}}{c + d\sqrt{2}} \), with \( a, b, c, d \in \mathbb{Q} \).
Example. \( \mathbb{Q} \left( \sqrt{2} \right) \) is the splitting field for \( p(x) = x^2 - 2 \) over \( \mathbb{Q} \). Because \( \left( \sqrt{2} \right)^2 = 2 \), the elements of \( \mathbb{Q} \left( \sqrt{2} \right) \) are of the form \( \frac{a + b\sqrt{2}}{c + d\sqrt{2}} \), with \( a, b, c, d \in \mathbb{Q} \). For each of these elements we have \( c \in \mathbb{Q} \) and \( d\sqrt{2} \not\in \mathbb{Q} \).
Example. $\mathbb{Q}\left(\sqrt{2}\right)$ is the splitting field for $p(x) = x^2 - 2$ over $\mathbb{Q}$. Because $\left(\sqrt{2}\right)^2 = 2$, the elements of $\mathbb{Q}\left(\sqrt{2}\right)$ are of the form $\frac{a + b\sqrt{2}}{c + d\sqrt{2}}$, with $a, b, c, d \in \mathbb{Q}$. For each of these elements we have $c \in \mathbb{Q}$ and $d\sqrt{2} \not\in \mathbb{Q}$. Therefore $c \not\in \left\{\pm d\sqrt{2}\right\}$.
Example. \( \mathbb{Q}(\sqrt{2}) \) is the splitting field for \( p(x) = x^2 - 2 \) over \( \mathbb{Q} \). Because \( (\sqrt{2})^2 = 2 \), the elements of \( \mathbb{Q}(\sqrt{2}) \) are of the form \( \frac{a + b\sqrt{2}}{c + d\sqrt{2}} \), with \( a, b, c, d \in \mathbb{Q} \). For each of these elements we have \( c \in \mathbb{Q} \) and \( d\sqrt{2} \notin \mathbb{Q} \). Therefore \( c \notin \{ \pm d\sqrt{2} \} \), and hence \( c^2 - 2d^2 \neq 0 \).
Example. $\mathbb{Q} \left( \sqrt{2} \right)$ is the splitting field for $p(x) = x^2 - 2$ over $\mathbb{Q}$. Because $\left( \sqrt{2} \right)^2 = 2$, the elements of $\mathbb{Q} \left( \sqrt{2} \right)$ are of the form $\frac{a + b\sqrt{2}}{c + d\sqrt{2}}$, with $a, b, c, d \in \mathbb{Q}$. For each of these elements we have $c \in \mathbb{Q}$ and $d\sqrt{2} \not\in \mathbb{Q}$. Therefore $c \not\in \left\{ \pm d\sqrt{2} \right\}$, and hence $c^2 - 2d^2 \neq 0$. Therefore

$$\frac{a + b\sqrt{2}}{c + d\sqrt{2}}$$
**Example.** $\mathbb{Q} \left( \sqrt{2} \right)$ is the splitting field for $p(x) = x^2 - 2$ over $\mathbb{Q}$. Because $\left( \sqrt{2} \right)^2 = 2$, the elements of $\mathbb{Q} \left( \sqrt{2} \right)$ are of the form $\frac{a + b\sqrt{2}}{c + d\sqrt{2}}$, with $a, b, c, d \in \mathbb{Q}$. For each of these elements we have $c \in \mathbb{Q}$ and $d\sqrt{2} \not\in \mathbb{Q}$. Therefore $c \not\in \{ \pm d\sqrt{2} \}$, and hence $c^2 - 2d^2 \neq 0$. Therefore

$$\frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{a + b\sqrt{2}}{c + d\sqrt{2}}$$
Example. $\mathbb{Q}\left(\sqrt{2}\right)$ is the splitting field for $p(x) = x^2 - 2$ over $\mathbb{Q}$. Because $\left(\sqrt{2}\right)^2 = 2$, the elements of $\mathbb{Q}\left(\sqrt{2}\right)$ are of the form $\frac{a + b\sqrt{2}}{c + d\sqrt{2}}$, with $a, b, c, d \in \mathbb{Q}$. For each of these elements we have $c \in \mathbb{Q}$ and $d\sqrt{2} \notin \mathbb{Q}$. Therefore $c \notin \{\pm d\sqrt{2}\}$, and hence $c^2 - 2d^2 \neq 0$. Therefore

$$\frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{a + b\sqrt{2}}{c + d\sqrt{2}} \cdot \frac{c - d\sqrt{2}}{c - d\sqrt{2}}$$
Example. \( \mathbb{Q} \left( \sqrt{2} \right) \) is the splitting field for \( p(x) = x^2 - 2 \) over \( \mathbb{Q} \). Because \( \left( \sqrt{2} \right)^2 = 2 \), the elements of \( \mathbb{Q} \left( \sqrt{2} \right) \) are of the form \( \frac{a + b\sqrt{2}}{c + d\sqrt{2}} \), with \( a, b, c, d \in \mathbb{Q} \). For each of these elements we have \( c \in \mathbb{Q} \) and \( d\sqrt{2} \not\in \mathbb{Q} \). Therefore \( c \not\in \left\{ \pm d\sqrt{2} \right\} \), and hence \( c^2 - 2d^2 \neq 0 \). Therefore

\[
\frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{a + b\sqrt{2}}{c + d\sqrt{2}} \cdot \frac{c - d\sqrt{2}}{c - d\sqrt{2}} = \frac{ac - 2bd + (bc - ad)\sqrt{2}}{c^2 - 2d^2}
\]
Example. $\mathbb{Q}\left(\sqrt{2}\right)$ is the splitting field for $p(x) = x^2 - 2$ over $\mathbb{Q}$. Because $\left(\sqrt{2}\right)^2 = 2$, the elements of $\mathbb{Q}\left(\sqrt{2}\right)$ are of the form $\frac{a + b\sqrt{2}}{c + d\sqrt{2}}$, with $a, b, c, d \in \mathbb{Q}$. For each of these elements we have $c \in \mathbb{Q}$ and $d\sqrt{2} \notin \mathbb{Q}$. Therefore $c \notin \{\pm d\sqrt{2}\}$, and hence $c^2 - 2d^2 \neq 0$. Therefore

$$\frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{a + b\sqrt{2}}{c + d\sqrt{2}} \cdot \frac{c - d\sqrt{2}}{c - d\sqrt{2}} = \frac{ac - 2bd + (bc - ad)\sqrt{2}}{c^2 - 2d^2} \cdot \frac{c^2 - 2d^2}{c^2 - 2d^2} \sqrt{2}. $$
Example. $\mathbb{Q}(\sqrt{2})$ is the splitting field for $p(x) = x^2 - 2$ over $\mathbb{Q}$. Because $(\sqrt{2})^2 = 2$, the elements of $\mathbb{Q}(\sqrt{2})$ are of the form $\frac{a + b\sqrt{2}}{c + d\sqrt{2}}$, with $a, b, c, d \in \mathbb{Q}$. For each of these elements we have $c \in \mathbb{Q}$ and $d\sqrt{2} \notin \mathbb{Q}$. Therefore $c \notin \{\pm d\sqrt{2}\}$, and hence $c^2 - 2d^2 \neq 0$. Therefore

$$\frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{a + b\sqrt{2}}{c + d\sqrt{2}} \cdot \frac{c - d\sqrt{2}}{c - d\sqrt{2}} = \frac{a c - 2bd + (bc - ad)\sqrt{2}}{c^2 - 2d^2}$$

$$= \frac{ac - 2bd}{c^2 - 2d^2} + \frac{bc - ad}{c^2 - 2d^2} \sqrt{2}.$$

Let $x := \frac{ac - 2bd}{c^2 - 2d^2} \in \mathbb{Q}$ and $y := \frac{bc - ad}{c^2 - 2d^2} \in \mathbb{Q}$. 
Example. $\mathbb{Q}(\sqrt{2})$ is the splitting field for $p(x) = x^2 - 2$ over $\mathbb{Q}$. Because $(\sqrt{2})^2 = 2$, the elements of $\mathbb{Q}(\sqrt{2})$ are of the form $\frac{a + b\sqrt{2}}{c + d\sqrt{2}}$, with $a, b, c, d \in \mathbb{Q}$. For each of these elements we have $c \in \mathbb{Q}$ and $d\sqrt{2} \notin \mathbb{Q}$. Therefore $c \notin \{\pm d\sqrt{2}\}$, and hence $c^2 - 2d^2 \neq 0$. Therefore

$$\frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{a + b\sqrt{2}}{c + d\sqrt{2}} \cdot \frac{c - d\sqrt{2}}{c - d\sqrt{2}} = \frac{ac - 2bd + (bc - ad)\sqrt{2}}{c^2 - 2d^2}$$

$$= \frac{ac - 2bd}{c^2 - 2d^2} + \frac{bc - ad}{c^2 - 2d^2} \sqrt{2}.$$  

Let $x := \frac{ac - 2bd}{c^2 - 2d^2} \in \mathbb{Q}$ and $y := \frac{bc - ad}{c^2 - 2d^2} \in \mathbb{Q}$. The elements of $\mathbb{Q}(\sqrt{2})$ are of the form $x + y\sqrt{2}$ with $x, y \in \mathbb{Q}$. 
Example. $\mathbb{Q} \left( \sqrt{2} \right)$ is the splitting field for $p(x) = x^2 - 2$ over $\mathbb{Q}$. Because $\left( \sqrt{2} \right)^2 = 2$, the elements of $\mathbb{Q} \left( \sqrt{2} \right)$ are of the form $\frac{a + b\sqrt{2}}{c + d\sqrt{2}}$, with $a, b, c, d \in \mathbb{Q}$. For each of these elements we have $c \in \mathbb{Q}$ and $d\sqrt{2} \notin \mathbb{Q}$. Therefore $c \notin \{ \pm d\sqrt{2} \}$, and hence $c^2 - 2d^2 \neq 0$. Therefore

$$
\frac{a + b\sqrt{2}}{c + d\sqrt{2}} = \frac{a + b\sqrt{2}}{c + d\sqrt{2}} \cdot \frac{c - d\sqrt{2}}{c - d\sqrt{2}} = \frac{ac - 2bd + (bc - ad)\sqrt{2}}{c^2 - 2d^2}
$$

$$
= \frac{ac - 2bd}{c^2 - 2d^2} + \frac{bc - ad}{c^2 - 2d^2} \sqrt{2}.
$$

Let $x := \frac{ac - 2bd}{c^2 - 2d^2} \in \mathbb{Q}$ and $y := \frac{bc - ad}{c^2 - 2d^2} \in \mathbb{Q}$. The elements of $\mathbb{Q} \left( \sqrt{2} \right)$ are of the form $x + y\sqrt{2}$ with $x, y \in \mathbb{Q}$. \[\square\]