Section 29 – Introduction to extension fields

Instructor: Yifan Yang

Spring 2007

Definition of an extension field

Definition

A field E is an extension field of a field if $F \leq E$.

Example

We have

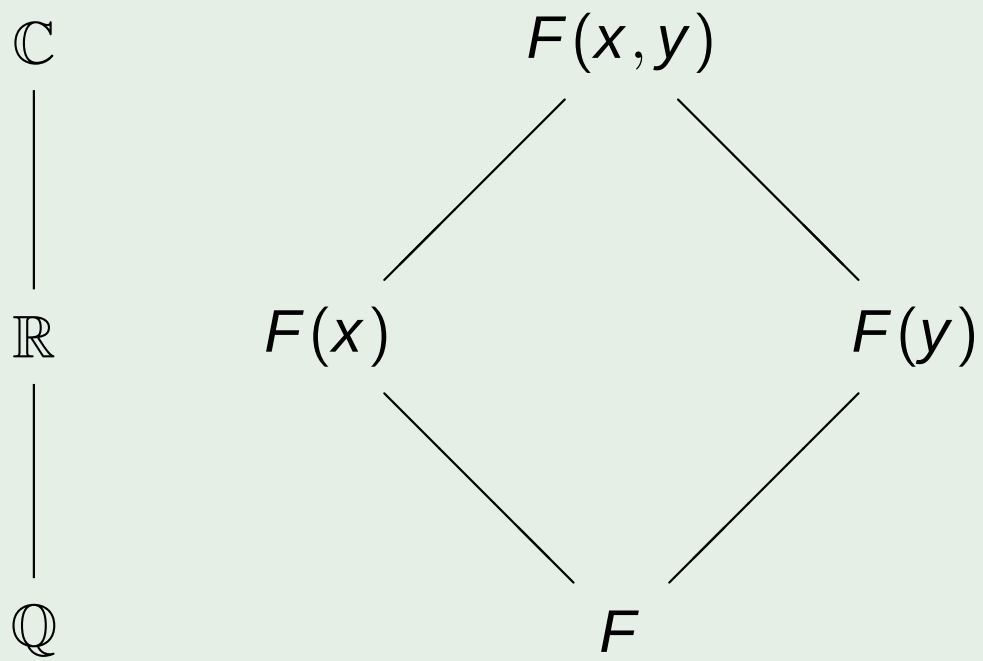
Definition of an extension field

Definition

A field E is an extension field of a field if $F \leq E$.

Example

We have



Every polynomial has a zero in some extension field

Remark

Theorem 27.19 can be rephrased as follows. If a field is of characteristic p, then it can be regarded as an extension field of $\mathbb{Z}_p$. If a field is of characteristic 0, then it can be regarded as an extension field of $\mathbb{Q}$.

Theorem (29.3, Kronecker)

Let F be a field, and $f(x)$ be a nonconstant polynomial in $F[x]$. Then there exists an extension field E of F and an $\alpha \in E$ such that $f(\alpha) = 0$.

Every polynomial has a zero in some extension field

Remark

Theorem 27.19 can be rephrased as follows. If a field is of characteristic p, then it can be regarded as an extension field of $\mathbb{Z}_p$. If a field is of characteristic 0, then it can be regarded as an extension field of $\mathbb{Q}$.

Theorem (29.3, Kronecker)

Let F be a field, and $f(x)$ be a nonconstant polynomial in $F[x]$. Then there exists an extension field E of F and an $\alpha \in E$ such that $f(\alpha) = 0$.

Proof of Theorem 29.3

Proof.

- Let $p(x)$ be an irreducible factor of $f(x)$ over F, say $f(x) = p(x)g(x)$ for some $g(x) \in F[x]$.
- By Theorems 27.9 and 27.25, $F[x]/\langle p(x)\rangle$ is a field.
- The field F is naturally embedded in $F[x]/\langle p(x)\rangle$ by $a \mapsto a + \langle p(x)\rangle$ for $a \in F$. Thus, we may consider $F[x]/\langle p(x)\rangle$ as an extension field of F.
- Now let $\alpha = x + \langle p(x)\rangle \in F[x]/\langle p(x)\rangle$.
- Then we have $f(\alpha) = f(x) + \langle p(x)\rangle = p(x)g(x) + \langle p(x)\rangle = \langle p(x)\rangle$. That is, α is a zero of $f(x)$ in $F[x]/\langle f(x)\rangle$. □

Proof of Theorem 29.3

Proof.

- Let $p(x)$ be an irreducible factor of $f(x)$ over F, say $f(x) = p(x)g(x)$ for some $g(x) \in F[x]$.
- By Theorems 27.9 and 27.25, $F[x]/\langle p(x)\rangle$ is a field.
- The field F is naturally embedded in $F[x]/\langle p(x)\rangle$ by $a \mapsto a + \langle p(x)\rangle$ for $a \in F$. Thus, we may consider $F[x]/\langle p(x)\rangle$ as an extension field of F.
- Now let $\alpha = x + \langle p(x)\rangle \in F[x]/\langle p(x)\rangle$.
- Then we have $f(\alpha) = f(x) + \langle p(x)\rangle = p(x)g(x) + \langle p(x)\rangle = \langle p(x)\rangle$. That is, α is a zero of $f(x)$ in $F[x]/\langle f(x)\rangle$. □

Proof of Theorem 29.3

Proof.

- Let $p(x)$ be an irreducible factor of $f(x)$ over F, say $f(x) = p(x)g(x)$ for some $g(x) \in F[x]$.
- By Theorems 27.9 and 27.25, $F[x]/\langle p(x)\rangle$ is a field.
- The field F is naturally embedded in $F[x]/\langle p(x)\rangle$ by $a \mapsto a + \langle p(x)\rangle$ for $a \in F$. Thus, we may consider $F[x]/\langle p(x)\rangle$ as an extension field of F.
- Now let $\alpha = x + \langle p(x)\rangle \in F[x]/\langle p(x)\rangle$.
- Then we have $f(\alpha) = f(x) + \langle p(x)\rangle = p(x)g(x) + \langle p(x)\rangle = \langle p(x)\rangle$. That is, α is a zero of $f(x)$ in $F[x]/\langle f(x)\rangle$. □

Proof of Theorem 29.3

Proof.

- Let $p(x)$ be an irreducible factor of $f(x)$ over F, say $f(x) = p(x)g(x)$ for some $g(x) \in F[x]$.
- By Theorems 27.9 and 27.25, $F[x]/\langle p(x)\rangle$ is a field.
- The field F is naturally embedded in $F[x]/\langle p(x)\rangle$ by $a \mapsto a + \langle p(x)\rangle$ for $a \in F$. Thus, we may consider $F[x]/\langle p(x)\rangle$ as an extension field of F.
- Now let $\alpha = x + \langle p(x)\rangle \in F[x]/\langle p(x)\rangle$.
- Then we have $f(\alpha) = f(x) + \langle p(x)\rangle = p(x)g(x) + \langle p(x)\rangle = \langle p(x)\rangle$. That is, α is a zero of $f(x)$ in $F[x]/\langle f(x)\rangle$. □

Proof of Theorem 29.3

Proof.

- Let $p(x)$ be an irreducible factor of $f(x)$ over F, say $f(x) = p(x)g(x)$ for some $g(x) \in F[x]$.
- By Theorems 27.9 and 27.25, $F[x]/\langle p(x)\rangle$ is a field.
- The field F is naturally embedded in $F[x]/\langle p(x)\rangle$ by $a \mapsto a + \langle p(x)\rangle$ for $a \in F$. Thus, we may consider $F[x]/\langle p(x)\rangle$ as an extension field of F.
- Now let $\alpha = x + \langle p(x)\rangle \in F[x]/\langle p(x)\rangle$.
- Then we have $f(\alpha) = f(x) + \langle p(x)\rangle = p(x)g(x) + \langle p(x)\rangle = \langle p(x)\rangle$. That is, α is a zero of $f(x)$ in $F[x]/\langle f(x)\rangle$. □

Algebraic and transcendental elements

Definition

An element α of an extension field E of a field F is algebraic over F if $f(\alpha) = 0$ for some nonzero polynomial $f(x) \in F[x]$. If such a polynomial does not exist, then α is transcendental over F.

Example

- $\sqrt{2}, \sqrt{3}$ are algebraic over $\mathbb{Q}$ since they are zeros of $x^2 - 2, x^2 - 1$, and $x^2 - 3$, respectively.
- $\alpha = \sqrt{1 + \sqrt{2}}$ is algebraic over $\mathbb{Q}$ since it satisfies $(\alpha^2 - 1)^2 = 2$.
- π and e are transcendental over $\mathbb{Q}$, although the proof is not easy.
- π is algebraic over $\mathbb{R}$, as it is a zero of $x - \pi \in \mathbb{R}[x]$.

Algebraic and transcendental elements

Definition

An element α of an extension field E of a field F is algebraic over F if $f(\alpha) = 0$ for some nonzero polynomial $f(x) \in F[x]$. If such a polynomial does not exist, then α is transcendental over F.

Example

- $\sqrt{2}$, i, $\sqrt[3]{3}$ are algebraic over $\mathbb{Q}$ since they are zeros of $x^2 - 2$, $x^2 + 1$, and $x^3 - 3$, respectively.
- $\alpha = \sqrt{1 + \sqrt{2}}$ is algebraic over $\mathbb{Q}$ since it satisfies $(\alpha^2 - 1)^2 = 2$.
- π and e are transcendental over $\mathbb{Q}$, although the proof is not easy.
- π is algebraic over $\mathbb{R}$, as it is a zero of $x - \pi \in \mathbb{R}[x]$.

Algebraic and transcendental elements

Definition

An element α of an extension field E of a field F is algebraic over F if $f(\alpha) = 0$ for some nonzero polynomial $f(x) \in F[x]$. If such a polynomial does not exist, then α is transcendental over F.

Example

- $\sqrt{2}$, i, $\sqrt[3]{3}$ are algebraic over $\mathbb{Q}$ since they are zeros of $x^2 - 2$, $x^2 + 1$, and $x^3 - 3$, respectively.
- $\alpha = \sqrt{1 + \sqrt{2}}$ is algebraic over $\mathbb{Q}$ since it satisfies $(\alpha^2 - 1)^2 = 2$.
- π and e are transcendental over $\mathbb{Q}$, although the proof is not easy.
- π is algebraic over $\mathbb{R}$, as it is a zero of $x - \pi \in \mathbb{R}[x]$.

Algebraic and transcendental elements

Definition

An element α of an extension field E of a field F is algebraic over F if $f(\alpha) = 0$ for some nonzero polynomial $f(x) \in F[x]$. If such a polynomial does not exist, then α is transcendental over F.

Example

- $\sqrt{2}$, i, $\sqrt[3]{3}$ are algebraic over $\mathbb{Q}$ since they are zeros of $x^2 - 2$, $x^2 + 1$, and $x^3 - 3$, respectively.
- $\alpha = \sqrt{1 + \sqrt{2}}$ is algebraic over $\mathbb{Q}$ since it satisfies $(\alpha^2 - 1)^2 = 2$.
- π and e are transcendental over $\mathbb{Q}$, although the proof is not easy.
- π is algebraic over $\mathbb{R}$, as it is a zero of $x - \pi \in \mathbb{R}[x]$.

Algebraic and transcendental elements

Definition

An element α of an extension field E of a field F is algebraic over F if $f(\alpha) = 0$ for some nonzero polynomial $f(x) \in F[x]$. If such a polynomial does not exist, then α is transcendental over F.

Example

- $\sqrt{2}$, i, $\sqrt[3]{3}$ are algebraic over $\mathbb{Q}$ since they are zeros of $x^2 - 2$, $x^2 + 1$, and $x^3 - 3$, respectively.
- $\alpha = \sqrt{1 + \sqrt{2}}$ is algebraic over $\mathbb{Q}$ since it satisfies $(\alpha^2 - 1)^2 = 2$.
- π and e are transcendental over $\mathbb{Q}$, although the proof is not easy.
- π is algebraic over $\mathbb{R}$, as it is a zero of $x - \pi \in \mathbb{R}[x]$.

Algebraic and transcendental numbers

Remark

The last example shows that algebraicity and transcendence depend on the ground field. So whenever we talk about algebraicity and transcendence, we should specify which field we are talking about.

Definition (29.11)

An element $\alpha \in \mathbb{C}$ is an algebraic number if α is algebraic over $\mathbb{Q}$. A transcendental number is an element of $\mathbb{C}$ that is transendental over $\mathbb{Q}$.

Example

1, $\sqrt{2}$, $\sqrt{1+\sqrt{2}}$ are algebraic numbers, while π and e are transcendental numbers.

Algebraic and transcendental numbers

Remark

The last example shows that algebraicity and transcendence depend on the ground field. So whenever we talk about algebraicity and transcendence, we should specify which field we are talking about.

Definition (29.11)

An element $\alpha \in \mathbb{C}$ is an algebraic number if α is algebraic over $\mathbb{Q}$. A transcendental number is an element of $\mathbb{C}$ that is transendental over $\mathbb{Q}$.

Example

1, $\sqrt{2}$, $\sqrt{1+\sqrt{2}}$ are algebraic numbers, while π and e are transcendental numbers.

Algebraic and transcendental numbers

Remark

The last example shows that algebraicity and transcendence depend on the ground field. So whenever we talk about algebraicity and transcendence, we should specify which field we are talking about.

Definition (29.11)

An element $\alpha \in \mathbb{C}$ is an algebraic number if α is algebraic over $\mathbb{Q}$. A transcendental number is an element of $\mathbb{C}$ that is transendental over $\mathbb{Q}$.

Example

1, $\sqrt{2}$, $\sqrt{1+\sqrt{2}}$ are algebraic numbers, while π and e are transcendental numbers.

Algebraic and transcendental elements

Theorem (29.12)

Let E be an extension field of a field F. Let $\alpha \in E$. Then α is transcendental over F if and only if the evaluation homomorphism $\phi_\alpha : F[x] \to E$ is an isomorphism of $F[x]$ with a subdomain of E.

Proof.

It suffices to show that $\alpha \in E$ is transcendental over F if and only if ϕ_α is one-to-one, which is obvious. □

Remark

The theorem says that if $\alpha \in E$ is transcendental over F, then $F[\alpha]$ looks just like $F[x]$.

Algebraic and transcendental elements

Theorem (29.12)

Let E be an extension field of a field F. Let $\alpha \in E$. Then α is transcendental over F if and only if the evaluation homomorphism $\phi_\alpha : F[x] \to E$ is an isomorphism of $F[x]$ with a subdomain of E.

Proof.

It suffices to show that $\alpha \in E$ is transcendental over F if and only if ϕ_α is one-to-one, which is obvious. □

Remark

The theorem says that if $\alpha \in E$ is transcendental over F, then $F[\alpha]$ looks just like $F[x]$.

Algebraic and transcendental elements

Theorem (29.12)

Let E be an extension field of a field F. Let $\alpha \in E$. Then α is transcendental over F if and only if the evaluation homomorphism $\phi_\alpha : F[x] \to E$ is an isomorphism of $F[x]$ with a subdomain of E.

Proof.

It suffices to show that $\alpha \in E$ is transcendental over F if and only if ϕ_α is one-to-one, which is obvious. □

Remark

The theorem says that if $\alpha \in E$ is transcendental over F, then $F[\alpha]$ looks just like $F[x]$.

The irreducible polynomial for α over F

- Assume that $F \leq E$, and $\alpha \in E$ is algebraic over F.
- It is easy to check that the set $I_\alpha = \{f(x) \in F[x] : f(\alpha) = 0\}$ is an ideal of $F[x]$.
- Since $F[x]$ is a PID, $I_\alpha = \langle p_\alpha(x) \rangle$ for some $p_\alpha(x) \in F[x]$.

Lemma

The polynomial $p_\alpha(x)$ is irreducible.

Proof.

- If $p_\alpha(x) = r(x)s(x)$, then we have $r(\alpha)s(\alpha) = 0$ and thus $r(\alpha) = 0$ or $s(\alpha) = 0$.
- That is, $r(x) \in \langle p_\alpha(x) \rangle$ or $s(x) \in \langle p_\alpha(x) \rangle$.
- Since $p_\alpha(x)$ is a nonzero polynomial of minimal degree in I_α, we must have $\deg s(x) = 0$ or $\deg r(x) = 0$. That is, one of $r(x)$ and $s(x)$ is a unit. □

The irreducible polynomial for α over F

- Assume that $F \leq E$, and $\alpha \in E$ is algebraic over F.
- It is easy to check that the set $I_\alpha = \{f(x) \in F[x] : f(\alpha) = 0\}$ is an ideal of $F[x]$.
- Since $F[x]$ is a PID, $I_\alpha = \langle p_\alpha(x) \rangle$ for some $p_\alpha(x) \in F[x]$.

Lemma

The polynomial $p_\alpha(x)$ is irreducible.

Proof.

- If $p_\alpha(x) = r(x)s(x)$, then we have $r(\alpha)s(\alpha) = 0$ and thus $r(\alpha) = 0$ or $s(\alpha) = 0$.
- That is, $r(x) \in \langle p_\alpha(x) \rangle$ or $s(x) \in \langle p_\alpha(x) \rangle$.
- Since $p_\alpha(x)$ is a nonzero polynomial of minimal degree in I_α, we must have $\deg s(x) = 0$ or $\deg r(x) = 0$. That is, one of $r(x)$ and $s(x)$ is a unit. □

The irreducible polynomial for α over F

- Assume that $F \leq E$, and $\alpha \in E$ is algebraic over F.
- It is easy to check that the set $I_\alpha = \{f(x) \in F[x] : f(\alpha) = 0\}$ is an ideal of $F[x]$.
- Since $F[x]$ is a PID, $I_\alpha = \langle p_\alpha(x) \rangle$ for some $p_\alpha(x) \in F[x]$.

Lemma

The polynomial $p_\alpha(x)$ is irreducible.

Proof.

- If $p_\alpha(x) = r(x)s(x)$, then we have $r(\alpha)s(\alpha) = 0$ and thus $r(\alpha) = 0$ or $s(\alpha) = 0$.
- That is, $r(x) \in \langle p_\alpha(x) \rangle$ or $s(x) \in \langle p_\alpha(x) \rangle$.
- Since $p_\alpha(x)$ is a nonzero polynomial of minimal degree in I_α, we must have $\deg s(x) = 0$ or $\deg r(x) = 0$. That is, one of $r(x)$ and $s(x)$ is a unit.

□

The irreducible polynomial for α over F

- Assume that $F \leq E$, and $\alpha \in E$ is algebraic over F.
- It is easy to check that the set $I_\alpha = \{f(x) \in F[x] : f(\alpha) = 0\}$ is an ideal of $F[x]$.
- Since $F[x]$ is a PID, $I_\alpha = \langle p_\alpha(x) \rangle$ for some $p_\alpha(x) \in F[x]$.

Lemma

The polynomial $p_\alpha(x)$ is irreducible.

Proof.

- If $p_\alpha(x) = r(x)s(x)$, then we have $r(\alpha)s(\alpha) = 0$ and thus $r(\alpha) = 0$ or $s(\alpha) = 0$.
- That is, $r(x) \in \langle p_\alpha(x) \rangle$ or $s(x) \in \langle p_\alpha(x) \rangle$.
- Since $p_\alpha(x)$ is a nonzero polynomial of minimal degree in I_α, we must have $\deg s(x) = 0$ or $\deg r(x) = 0$. That is, one of $r(x)$ and $s(x)$ is a unit. □

The irreducible polynomial for α over F

- Assume that $F \leq E$, and $\alpha \in E$ is algebraic over F.
- It is easy to check that the set $I_\alpha = \{f(x) \in F[x] : f(\alpha) = 0\}$ is an ideal of $F[x]$.
- Since $F[x]$ is a PID, $I_\alpha = \langle p_\alpha(x) \rangle$ for some $p_\alpha(x) \in F[x]$.

Lemma

The polynomial $p_\alpha(x)$ is irreducible.

Proof.

- If $p_\alpha(x) = r(x)s(x)$, then we have $r(\alpha)s(\alpha) = 0$ and thus $r(\alpha) = 0$ or $s(\alpha) = 0$.
- That is, $r(x) \in \langle p_\alpha(x) \rangle$ or $s(x) \in \langle p_\alpha(x) \rangle$.
- Since $p_\alpha(x)$ is a nonzero polynomial of minimal degree in I_α, we must have $\deg s(x) = 0$ or $\deg r(x) = 0$. That is, one of $r(x)$ and $s(x)$ is a unit. □

The irreducible polynomial for α over F

- Assume that $F \leq E$, and $\alpha \in E$ is algebraic over F.
- It is easy to check that the set $I_\alpha = \{f(x) \in F[x] : f(\alpha) = 0\}$ is an ideal of $F[x]$.
- Since $F[x]$ is a PID, $I_\alpha = \langle p_\alpha(x) \rangle$ for some $p_\alpha(x) \in F[x]$.

Lemma

The polynomial $p_\alpha(x)$ is irreducible.

Proof.

- If $p_\alpha(x) = r(x)s(x)$, then we have $r(\alpha)s(\alpha) = 0$ and thus $r(\alpha) = 0$ or $s(\alpha) = 0$.
- That is, $r(x) \in \langle p_\alpha(x) \rangle$ or $s(x) \in \langle p_\alpha(x) \rangle$.
- Since $p_\alpha(x)$ is a nonzero polynomial of minimal degree in I_α, we must have $\deg s(x) = 0$ or $\deg r(x) = 0$. That is, one of $r(x)$ and $s(x)$ is a unit. □

The irreducible polynomial for α over F

- Assume that $F \leq E$, and $\alpha \in E$ is algebraic over F.
- It is easy to check that the set $I_\alpha = \{f(x) \in F[x] : f(\alpha) = 0\}$ is an ideal of $F[x]$.
- Since $F[x]$ is a PID, $I_\alpha = \langle p_\alpha(x) \rangle$ for some $p_\alpha(x) \in F[x]$.

Lemma

The polynomial $p_\alpha(x)$ is irreducible.

Proof.

- If $p_\alpha(x) = r(x)s(x)$, then we have $r(\alpha)s(\alpha) = 0$ and thus $r(\alpha) = 0$ or $s(\alpha) = 0$.
- That is, $r(x) \in \langle p_\alpha(x) \rangle$ or $s(x) \in \langle p_\alpha(x) \rangle$.
- Since $p_\alpha(x)$ is a nonzero polynomial of minimal degree in I_α, we must have $\deg s(x) = 0$ or $\deg r(x) = 0$. That is, one of $r(x)$ and $s(x)$ is a unit. □

The irreducible polynomial for α over F

- Assume that $F \leq E$, and $\alpha \in E$ is algebraic over F.
- It is easy to check that the set $I_\alpha = \{f(x) \in F[x] : f(\alpha) = 0\}$ is an ideal of $F[x]$.
- Since $F[x]$ is a PID, $I_\alpha = \langle p_\alpha(x) \rangle$ for some $p_\alpha(x) \in F[x]$.

Lemma

The polynomial $p_\alpha(x)$ is irreducible.

Proof.

- If $p_\alpha(x) = r(x)s(x)$, then we have $r(\alpha)s(\alpha) = 0$ and thus $r(\alpha) = 0$ or $s(\alpha) = 0$.
- That is, $r(x) \in \langle p_\alpha(x) \rangle$ or $s(x) \in \langle p_\alpha(x) \rangle$.
- Since $p_\alpha(x)$ is a nonzero polynomial of minimal degree in I_α, we must have $\deg s(x) = 0$ or $\deg r(x) = 0$. That is, one of $r(x)$ and $s(x)$ is a unit. □

The irreducible polynomial for α over F

Definition

A polynomial in $F[x]$ with leading coefficient 1 is called a monic polynomial.

Definition

The unique monic irreducible polynomial $p(x)$ in I_α is called the irreducible polynomial for α over F, and will be denoted by $\mathrm{irr}(\alpha, F)$. The degree of $\mathrm{irr}(\alpha, F)$ is the degree of α over F, and is denoted by $\deg(\alpha, F)$.

Remark

- The irreducible polynomial $\mathrm{irr}(\alpha, F)$ can also be defined as the monic polynomial of smallest degree in $F[x]$ having α as a zero.
- Again, when we speak of the irreducible polynomial of an element, we need to specify which field we are talking

The irreducible polynomial for α over F

Definition

A polynomial in $F[x]$ with leading coefficient 1 is called a monic polynomial.

Definition

The unique monic irreducible polynomial $p(x)$ in I_α is called the irreducible polynomial for α over F, and will be denoted by $\mathrm{irr}(\alpha, F)$. The degree of $\mathrm{irr}(\alpha, F)$ is the degree of α over F, and is denoted by $\deg(\alpha, F)$.

Remark

- The irreducible polynomial $\mathrm{irr}(\alpha, F)$ can also be defined as the monic polynomial of smallest degree in $F[x]$ having α as a zero.
- Again, when we speak of the irreducible polynomial of an element, we need to specify which field we are talking

The irreducible polynomial for α over F

Definition

A polynomial in $F[x]$ with leading coefficient 1 is called a monic polynomial.

Definition

The unique monic irreducible polynomial $p(x)$ in I_α is called the irreducible polynomial for α over F, and will be denoted by $\mathrm{irr}(\alpha, F)$. The degree of $\mathrm{irr}(\alpha, F)$ is the degree of α over F, and is denoted by $\deg(\alpha, F)$.

Remark

- The irreducible polynomial $\mathrm{irr}(\alpha, F)$ can also be defined as the monic polynomial of smallest degree in $F[x]$ having α as a zero.
- Again, when we speak of the irreducible polynomial of an element, we need to specify which field we are talking about.

The irreducible polynomial for α over F

Definition

A polynomial in $F[x]$ with leading coefficient 1 is called a monic polynomial.

Definition

The unique monic irreducible polynomial $p(x)$ in I_α is called the irreducible polynomial for α over F, and will be denoted by $\mathrm{irr}(\alpha, F)$. The degree of $\mathrm{irr}(\alpha, F)$ is the degree of α over F, and is denoted by $\deg(\alpha, F)$.

Remark

- The irreducible polynomial $\mathrm{irr}(\alpha, F)$ can also be defined as the monic polynomial of smallest degree in $F[x]$ having α as a zero.
- Again, when we speak of the irreducible polynomial of an element, we need to specify which field we are talking about.

Examples

1. $\mathrm{irr}(1/\sqrt{2}, \mathbb{Q}) = x^2 - 1/2$.
2. $\mathrm{irr}(\sqrt[4]{2}, \mathbb{Q}[\sqrt{2}]) = x^2 - \sqrt{2}$.
3. The number $\alpha = \sqrt{1+\sqrt{2}}$ satisfies $(\alpha^2 - 1)^2 = 2$. We then check that $x^4 - 2x^2 - 1$ is irreducible. Thus, $\mathrm{irr}(\alpha, \mathbb{Q}) = x^4 - 2x^2 - 1$.
4. $\mathrm{irr}(\sqrt{\pi}, \mathbb{Q}(\pi)) = x^2 - \pi$.
5. Let $F = \mathbb{Z}_3$ and $E = \mathbb{Z}[i]/\langle 3 \rangle$. Then the irreducible polynomial for $(1+i) + \langle 3 \rangle$ over $\mathbb{Z}_3$ is $x^2 + x + 2 \in \mathbb{Z}_3[x]$. (We have $(1+i)^2 + (1+i) + 2 = 3 + 3i \in \langle 3 \rangle$.)

Examples

1. $\mathrm{irr}(1/\sqrt{2}, \mathbb{Q}) = x^2 - 1/2$.
2. $\mathrm{irr}(\sqrt[4]{2}, \mathbb{Q}[\sqrt{2}]) = x^2 - \sqrt{2}$.
3. The number $\alpha = \sqrt{1+\sqrt{2}}$ satisfies $(\alpha^2 - 1)^2 = 2$. We then check that $x^4 - 2x^2 - 1$ is irreducible. Thus, $\mathrm{irr}(\alpha, \mathbb{Q}) = x^4 - 2x^2 - 1$.
4. $\mathrm{irr}(\sqrt{\pi}, \mathbb{Q}(\pi)) = x^2 - \pi$.
5. Let $F = \mathbb{Z}_3$ and $E = \mathbb{Z}[i]/\langle 3 \rangle$. Then the irreducible polynomial for $(1+i) + \langle 3 \rangle$ over $\mathbb{Z}_3$ is $x^2 + x + 2 \in \mathbb{Z}_3[x]$. (We have $(1+i)^2 + (1+i) + 2 = 3 + 3i \in \langle 3 \rangle$.)

Examples

1. $\mathrm{irr}(1/\sqrt{2}, \mathbb{Q}) = x^2 - 1/2$.
2. $\mathrm{irr}(\sqrt[4]{2}, \mathbb{Q}[\sqrt{2}]) = x^2 - \sqrt{2}$.
3. The number $\alpha = \sqrt{1+\sqrt{2}}$ satisfies $(\alpha^2 - 1)^2 = 2$. We then check that $x^4 - 2x^2 - 1$ is irreducible. Thus, $\mathrm{irr}(\alpha, \mathbb{Q}) = x^4 - 2x^2 - 1$.
4. $\mathrm{irr}(\sqrt{\pi}, \mathbb{Q}(\pi)) = x^2 - \pi$.
5. Let $F = \mathbb{Z}_3$ and $E = \mathbb{Z}[i]/\langle 3 \rangle$. Then the irreducible polynomial for $(1+i) + \langle 3 \rangle$ over $\mathbb{Z}_3$ is $x^2 + x + 2 \in \mathbb{Z}_3[x]$. (We have $(1+i)^2 + (1+i) + 2 = 3 + 3i \in \langle 3 \rangle$.)

Examples

1. $\mathrm{irr}(1/\sqrt{2}, \mathbb{Q}) = x^2 - 1/2$.
2. $\mathrm{irr}(\sqrt[4]{2}, \mathbb{Q}[\sqrt{2}]) = x^2 - \sqrt{2}$.
3. The number $\alpha = \sqrt{1+\sqrt{2}}$ satisfies $(\alpha^2 - 1)^2 = 2$. We then check that $x^4 - 2x^2 - 1$ is irreducible. Thus, $\mathrm{irr}(\alpha, \mathbb{Q}) = x^4 - 2x^2 - 1$.
4. $\mathrm{irr}(\sqrt{\pi}, \mathbb{Q}(\pi)) = x^2 - \pi$.
5. Let $F = \mathbb{Z}_3$ and $E = \mathbb{Z}[i]/\langle 3 \rangle$. Then the irreducible polynomial for $(1+i) + \langle 3 \rangle$ over $\mathbb{Z}_3$ is $x^2 + x + 2 \in \mathbb{Z}_3[x]$. (We have $(1+i)^2 + (1+i) + 2 = 3 + 3i \in \langle 3 \rangle$.)

Examples

1. $\mathrm{irr}(1/\sqrt{2}, \mathbb{Q}) = x^2 - 1/2$.
2. $\mathrm{irr}(\sqrt[4]{2}, \mathbb{Q}[\sqrt{2}]) = x^2 - \sqrt{2}$.
3. The number $\alpha = \sqrt{1+\sqrt{2}}$ satisfies $(\alpha^2 - 1)^2 = 2$. We then check that $x^4 - 2x^2 - 1$ is irreducible. Thus, $\mathrm{irr}(\alpha, \mathbb{Q}) = x^4 - 2x^2 - 1$.
4. $\mathrm{irr}(\sqrt{\pi}, \mathbb{Q}(\pi)) = x^2 - \pi$.
5. Let $F = \mathbb{Z}_3$ and $E = \mathbb{Z}[i]/\langle 3 \rangle$. Then the irreducible polynomial for $(1+i) + \langle 3 \rangle$ over $\mathbb{Z}_3$ is $x^2 + x + 2 \in \mathbb{Z}_3[x]$. (We have $(1+i)^2 + (1+i) + 2 = 3 + 3i \in \langle 3 \rangle$.)

α algebraic over $F \Rightarrow F(\alpha) = F[\alpha]$

Notation

Let F be a field. The notation $F[\alpha]$ denotes the set $\{f(\alpha) : f(x) \in F[x]\}$, while $F(\alpha)$ is the set $\{f(\alpha)/g(\alpha) : f(x), g(x) \in F[x],\ g(\alpha) \neq 0\}$.

Theorem

Let $F \leq E$, and $\alpha \in E$ be a nonzero element algebraic over F. Then $F(\alpha) = F[\alpha]$ and is isomorphic to $F[x]/\langle \text{irr}(\alpha, F)\rangle$.

Theorem (29.18)

Let $E = F(\alpha)$ be a simple extension of F. Assume that α is algebraic over F. Then any $\beta \in E = F(\alpha)$ can be uniquely expressed in the form $\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$, where $n = \deg \text{irr}(\alpha, F)$.

α algebraic over $F \Rightarrow F(\alpha) = F[\alpha]$

Notation

Let F be a field. The notation $F[\alpha]$ denotes the set $\{f(\alpha) : \ f(x) \in F[x]\}$, while $F(\alpha)$ is the set $\{f(\alpha)/g(\alpha) : \ f(x), g(x) \in F[x], \ g(\alpha) \neq 0\}$.

Theorem

Let $F \leq E$, and $\alpha \in E$ be a nonzero element algebraic over F. Then $F(\alpha) = F[\alpha]$ and is isomorphic to $F[x]/\langle \text{irr}(\alpha, F)\rangle$.

Theorem (29.18)

Let $E = F(\alpha)$ be a simple extension of F. Assume that α is algebraic over F. Then any $\beta \in E = F(\alpha)$ can be uniquely expressed in the form $\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$, where $n = \deg \text{irr}(\alpha, F)$.

α algebraic over $F \Rightarrow F(\alpha) = F[\alpha]$

Notation

Let F be a field. The notation $F[\alpha]$ denotes the set $\{f(\alpha) : \ f(x) \in F[x]\}$, while $F(\alpha)$ is the set $\{f(\alpha)/g(\alpha) : \ f(x), g(x) \in F[x], \ g(\alpha) \neq 0\}$.

Theorem

Let $F \leq E$, and $\alpha \in E$ be a nonzero element algebraic over F. Then $F(\alpha) = F[\alpha]$ and is isomorphic to $F[x]/\langle \text{irr}(\alpha, F)\rangle$.

Theorem (29.18)

Let $E = F(\alpha)$ be a simple extension of F. Assume that α is algebraic over F. Then any $\beta \in E = F(\alpha)$ can be uniquely expressed in the form $\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$, where $n = \deg \text{irr}(\alpha, F)$.

Proof of $F(\alpha) = F[\alpha]$

- It is clear that $F[\alpha] \subset F(\alpha)$. We now show that every element $f(\alpha)/g(\alpha) \in F(\alpha)$ with $g(\alpha) \neq 0$ can be expressed as $h(\alpha)$ for some $h(x) \in F[x]$.
- Since $g(\alpha) \neq 0$, $g(x)$ is not divisible by $\mathrm{irr}(\alpha, F)$. This in turn implies that $\gcd(g(x), \mathrm{irr}(\alpha, F)) = 1$ because $\mathrm{irr}(\alpha, F)$ is irreducible.
- Using the Euclidean algorithm, we can find $p(x)$ and $q(x)$ such that $p(x)g(x) + q(x)\,\mathrm{irr}(\alpha, F) = 1$. Then we have $p(\alpha)g(\alpha) = 1$.
- Then we have

$$\frac{f(\alpha)}{g(\alpha)} = \frac{f(\alpha)p(\alpha)}{g(\alpha)p(\alpha)} = f(\alpha)p(\alpha) \in F[\alpha].$$

Proof of $F(\alpha) = F[\alpha]$

- It is clear that $F[\alpha] \subset F(\alpha)$. We now show that every element $f(\alpha)/g(\alpha) \in F(\alpha)$ with $g(\alpha) \neq 0$ can be expressed as $h(\alpha)$ for some $h(x) \in F[x]$.
- Since $g(\alpha) \neq 0$, $g(x)$ is not divisible by $\mathrm{irr}(\alpha, F)$. This in turn implies that $\gcd(g(x), \mathrm{irr}(\alpha, F)) = 1$ because $\mathrm{irr}(\alpha, F)$ is irreducible.
- Using the Euclidean algorithm, we can find $p(x)$ and $q(x)$ such that $p(x)g(x) + q(x)\,\mathrm{irr}(\alpha, F) = 1$. Then we have $p(\alpha)g(\alpha) = 1$.
- Then we have

$$\frac{f(\alpha)}{g(\alpha)} = \frac{f(\alpha)p(\alpha)}{g(\alpha)p(\alpha)} = f(\alpha)p(\alpha) \in F[\alpha].$$

Proof of $F(\alpha) = F[\alpha]$

- It is clear that $F[\alpha] \subset F(\alpha)$. We now show that every element $f(\alpha)/g(\alpha) \in F(\alpha)$ with $g(\alpha) \neq 0$ can be expressed as $h(\alpha)$ for some $h(x) \in F[x]$.
- Since $g(\alpha) \neq 0$, $g(x)$ is not divisible by $\mathrm{irr}(\alpha, F)$. This in turn implies that $\gcd(g(x), \mathrm{irr}(\alpha, F)) = 1$ because $\mathrm{irr}(\alpha, F)$ is irreducible.
- Using the Euclidean algorithm, we can find $p(x)$ and $q(x)$ such that $p(x)g(x) + q(x)\,\mathrm{irr}(\alpha, F) = 1$. Then we have $p(\alpha)g(\alpha) = 1$.
- Then we have

$$\frac{f(\alpha)}{g(\alpha)} = \frac{f(\alpha)p(\alpha)}{g(\alpha)p(\alpha)} = f(\alpha)p(\alpha) \in F[\alpha].$$

Proof of $F(\alpha) = F[\alpha]$

- It is clear that $F[\alpha] \subset F(\alpha)$. We now show that every element $f(\alpha)/g(\alpha) \in F(\alpha)$ with $g(\alpha) \neq 0$ can be expressed as $h(\alpha)$ for some $h(x) \in F[x]$.
- Since $g(\alpha) \neq 0$, $g(x)$ is not divisible by $\mathrm{irr}(\alpha, F)$. This in turn implies that $\gcd(g(x), \mathrm{irr}(\alpha, F)) = 1$ because $\mathrm{irr}(\alpha, F)$ is irreducible.
- Using the Euclidean algorithm, we can find $p(x)$ and $q(x)$ such that $p(x)g(x) + q(x)\,\mathrm{irr}(\alpha, F) = 1$. Then we have $p(\alpha)g(\alpha) = 1$.
- Then we have

$$\frac{f(\alpha)}{g(\alpha)} = \frac{f(\alpha)p(\alpha)}{g(\alpha)p(\alpha)} = f(\alpha)p(\alpha) \in F[\alpha].$$

Proof of $F(\alpha) = F[\alpha]$

- It is clear that $F[\alpha] \subset F(\alpha)$. We now show that every element $f(\alpha)/g(\alpha) \in F(\alpha)$ with $g(\alpha) \neq 0$ can be expressed as $h(\alpha)$ for some $h(x) \in F[x]$.
- Since $g(\alpha) \neq 0$, $g(x)$ is not divisible by $\mathrm{irr}(\alpha, F)$. This in turn implies that $\gcd(g(x), \mathrm{irr}(\alpha, F)) = 1$ because $\mathrm{irr}(\alpha, F)$ is irreducible.
- Using the Euclidean algorithm, we can find $p(x)$ and $q(x)$ such that $p(x)g(x) + q(x)\,\mathrm{irr}(\alpha, F) = 1$. Then we have $p(\alpha)g(\alpha) = 1$.
- Then we have

$$\frac{f(\alpha)}{g(\alpha)} = \frac{f(\alpha)p(\alpha)}{g(\alpha)p(\alpha)} = f(\alpha)p(\alpha) \in F[\alpha].$$

Proof of $F(\alpha) = F[\alpha]$

- It is clear that $F[\alpha] \subset F(\alpha)$. We now show that every element $f(\alpha)/g(\alpha) \in F(\alpha)$ with $g(\alpha) \neq 0$ can be expressed as $h(\alpha)$ for some $h(x) \in F[x]$.
- Since $g(\alpha) \neq 0$, $g(x)$ is not divisible by $\mathrm{irr}(\alpha, F)$. This in turn implies that $\gcd(g(x), \mathrm{irr}(\alpha, F)) = 1$ because $\mathrm{irr}(\alpha, F)$ is irreducible.
- Using the Euclidean algorithm, we can find $p(x)$ and $q(x)$ such that $p(x)g(x) + q(x)\,\mathrm{irr}(\alpha, F) = 1$. Then we have $p(\alpha)g(\alpha) = 1$.
- Then we have

$$\frac{f(\alpha)}{g(\alpha)} = \frac{f(\alpha)p(\alpha)}{g(\alpha)p(\alpha)} = f(\alpha)p(\alpha) \in F[\alpha].$$

Proof of $F[\alpha] \simeq F[x]/\langle \text{irr}(\alpha, F)\rangle$

- Consider the evaluation homomorphism $\phi_\alpha : F[x] \to F[\alpha]$ given by $\phi_\alpha(f(x)) = f(\alpha)$. By the isomorphism theorem (Theorem 34.2 in case of groups), $F[x]/\text{Ker}(\phi_\alpha) \simeq \text{Im}(\phi_\alpha)$.
- The kernel consists of polynomials f over F satisfying $f(\alpha) = 0$. Thus, $\text{Ker}(\phi_\alpha) = \langle \text{irr}(\alpha, F)\rangle$.
- The homomorphism ϕ_α is clear onto.
- Then the isomorphism theorem says $F[x]/\langle \text{irr}(\alpha, F)\rangle \simeq F[\alpha]$. $\square$.

Proof of $F[\alpha] \simeq F[x]/\langle \text{irr}(\alpha, F)\rangle$

- Consider the evaluation homomorphism $\phi_\alpha : F[x] \to F[\alpha]$ given by $\phi_\alpha(f(x)) = f(\alpha)$. By the isomorphism theorem (Theorem 34.2 in case of groups), $F[x]/\text{Ker}(\phi_\alpha) \simeq \text{Im}(\phi_\alpha)$.
- The kernel consists of polynomials f over F satisfying $f(\alpha) = 0$. Thus, $\text{Ker}(\phi_\alpha) = \langle \text{irr}(\alpha, F)\rangle$.
- The homomorphism ϕ_α is clear onto.
- Then the isomorphism theorem says $F[x]/\langle \text{irr}(\alpha, F)\rangle \simeq F[\alpha]$. $\square$.

Proof of $F[\alpha] \simeq F[x]/\langle \text{irr}(\alpha, F)\rangle$

- Consider the evaluation homomorphism $\phi_\alpha : F[x] \to F[\alpha]$ given by $\phi_\alpha(f(x)) = f(\alpha)$. By the isomorphism theorem (Theorem 34.2 in case of groups), $F[x]/\text{Ker}(\phi_\alpha) \simeq \text{Im}(\phi_\alpha)$.
- The kernel consists of polynomials f over F satisfying $f(\alpha) = 0$. Thus, $\text{Ker}(\phi_\alpha) = \langle \text{irr}(\alpha, F)\rangle$.
- The homomorphism ϕ_α is clear onto.
- Then the isomorphism theorem says $F[x]/\langle \text{irr}(\alpha, F)\rangle \simeq F[\alpha]$. $\square$.

Proof of $F[\alpha] \simeq F[x]/\langle \text{irr}(\alpha, F)\rangle$

- Consider the evaluation homomorphism $\phi_\alpha : F[x] \to F[\alpha]$ given by $\phi_\alpha(f(x)) = f(\alpha)$. By the isomorphism theorem (Theorem 34.2 in case of groups), $F[x]/\text{Ker}(\phi_\alpha) \simeq \text{Im}(\phi_\alpha)$.
- The kernel consists of polynomials f over F satisfying $f(\alpha) = 0$. Thus, $\text{Ker}(\phi_\alpha) = \langle \text{irr}(\alpha, F)\rangle$.
- The homomorphism ϕ_α is clear onto.
- Then the isomorphism theorem says $F[x]/\langle \text{irr}(\alpha, F)\rangle \simeq F[\alpha]$. $\square$.

Proof of $F[\alpha] \simeq F[x]/\langle \text{irr}(\alpha, F)\rangle$

- Consider the evaluation homomorphism $\phi_\alpha : F[x] \to F[\alpha]$ given by $\phi_\alpha(f(x)) = f(\alpha)$. By the isomorphism theorem (Theorem 34.2 in case of groups), $F[x]/\text{Ker}(\phi_\alpha) \simeq \text{Im}(\phi_\alpha)$.
- The kernel consists of polynomials f over F satisfying $f(\alpha) = 0$. Thus, $\text{Ker}(\phi_\alpha) = \langle \text{irr}(\alpha, F)\rangle$.
- The homomorphism ϕ_α is clear onto.
- Then the isomorphism theorem says $F[x]/\langle \text{irr}(\alpha, F)\rangle \simeq F[\alpha]$. $\square$.

Proof of $F[\alpha] \simeq F[x]/\langle \text{irr}(\alpha, F)\rangle$

- Consider the evaluation homomorphism $\phi_\alpha : F[x] \to F[\alpha]$ given by $\phi_\alpha(f(x)) = f(\alpha)$. By the isomorphism theorem (Theorem 34.2 in case of groups), $F[x]/\text{Ker}(\phi_\alpha) \simeq \text{Im}(\phi_\alpha)$.
- The kernel consists of polynomials f over F satisfying $f(\alpha) = 0$. Thus, $\text{Ker}(\phi_\alpha) = \langle \text{irr}(\alpha, F)\rangle$.
- The homomorphism ϕ_α is clear onto.
- Then the isomorphism theorem says $F[x]/\langle \text{irr}(\alpha, F)\rangle \simeq F[\alpha]$. $\square$.

Proof of Theorem 29.18.

By the previous theorem, we have $F(\alpha) = F[\alpha]$ since α is algebraic over F. Thus, $\beta = f(\alpha)$ for some $f(x) \in f[x]$. By the division algorithm, there exists $q(x)$ and $r(x)$ such that $f(x) = q(x)\,\mathrm{irr}(\alpha, F) + r(x)$ with $r(x) = 0$ or $\deg r(x) < n$. Then $r(\alpha) = f(\alpha) = \beta$. The uniqueness is guaranteed by Theorem 23.1 (division algorithm). □

Definition

Let $F \leq E$. If there exists $\alpha \in E$ such that $E = F(a)$, then $E = F(\alpha)$ is a simple extension of F.

Proof of Theorem 29.18.

By the previous theorem, we have $F(\alpha) = F[\alpha]$ since α is algebraic over F. Thus, $\beta = f(\alpha)$ for some $f(x) \in f[x]$. By the division algorithm, there exists $q(x)$ and $r(x)$ such that $f(x) = q(x)\,\mathrm{irr}(\alpha, F) + r(x)$ with $r(x) = 0$ or $\deg r(x) < n$. Then $r(\alpha) = f(\alpha) = \beta$. The uniqueness is guaranteed by Theorem 23.1 (division algorithm). □

Definition

Let $F \leq E$. If there exists $\alpha \in E$ such that $E = F(a)$, then $E = F(\alpha)$ is a simple extension of F.

Proof of Theorem 29.18.

By the previous theorem, we have $F(\alpha) = F[\alpha]$ since α is algebraic over F. Thus, $\beta = f(\alpha)$ for some $f(x) \in f[x]$. By the division algorithm, there exists $q(x)$ and $r(x)$ such that $f(x) = q(x)\,\mathrm{irr}(\alpha, F) + r(x)$ with $r(x) = 0$ or $\deg r(x) < n$. Then $r(\alpha) = f(\alpha) = \beta$. The uniqueness is guaranteed by Theorem 23.1 (division algorithm). □

Definition

Let $F \leq E$. If there exists $\alpha \in E$ such that $E = F(a)$, then $E = F(\alpha)$ is a simple extension of F.

Proof of Theorem 29.18.

By the previous theorem, we have $F(\alpha) = F[\alpha]$ since α is algebraic over F. Thus, $\beta = f(\alpha)$ for some $f(x) \in f[x]$. By the division algorithm, there exists $q(x)$ and $r(x)$ such that $f(x) = q(x)\,\mathrm{irr}(\alpha, F) + r(x)$ with $r(x) = 0$ or $\deg r(x) < n$. Then $r(\alpha) = f(\alpha) = \beta$. The uniqueness is guaranteed by Theorem 23.1 (division algorithm). □

Definition

Let $F \leq E$. If there exists $\alpha \in E$ such that $E = F(a)$, then $E = F(\alpha)$ is a simple extension of F.

Proof of Theorem 29.18.

By the previous theorem, we have $F(\alpha) = F[\alpha]$ since α is algebraic over F. Thus, $\beta = f(\alpha)$ for some $f(x) \in f[x]$. By the division algorithm, there exists $q(x)$ and $r(x)$ such that $f(x) = q(x)\,\mathrm{irr}(\alpha, F) + r(x)$ with $r(x) = 0$ or $\deg r(x) < n$. Then $r(\alpha) = f(\alpha) = \beta$. The uniqueness is guaranteed by Theorem 23.1 (division algorithm). □

Definition

Let $F \leq E$. If there exists $\alpha \in E$ such that $E = F(a)$, then $E = F(\alpha)$ is a simple extension of F.

Proof of Theorem 29.18.

By the previous theorem, we have $F(\alpha) = F[\alpha]$ since α is algebraic over F. Thus, $\beta = f(\alpha)$ for some $f(x) \in f[x]$. By the division algorithm, there exists $q(x)$ and $r(x)$ such that $f(x) = q(x)\,\mathrm{irr}(\alpha, F) + r(x)$ with $r(x) = 0$ or $\deg r(x) < n$. Then $r(\alpha) = f(\alpha) = \beta$. The uniqueness is guaranteed by Theorem 23.1 (division algorithm). □

Definition

Let $F \leq E$. If there exists $\alpha \in E$ such that $E = F(a)$, then $E = F(\alpha)$ is a simple extension of F.

Example

Problem. Let α be a zero of x^3+x+1 in $\mathbb{Q}[x]$. Write $\beta=(2\alpha^2+3\alpha-1)/(\alpha^2-\alpha+1)$ in the form $a_0+a_1\alpha+a_2\alpha^2$.

Solution. We first use the Euclidean algorithm to find polynomials $g(x)$ and $h(x)$ such that $(x^3+x+1)g(x)+(x^2-x+1)h(x)=1$. We have

$$x^3+x+1=(x+1)(x^2-x+1)+x$$
$$x^2-x+1=(x-1)x+1$$

Then

$$1=(x^2-x+1)-(x-1)x=x^2(x^2-x+1)-(x-1)(x^3+x+1).$$

It follows that

$$\frac{2\alpha^2+3\alpha-1}{\alpha^2-\alpha+1}=\frac{(2\alpha^2+3\alpha-1)\alpha^2}{(\alpha^2-\alpha+1)\alpha^2}=2\alpha^4+3\alpha^3-\alpha^2$$
$$=(2\alpha+3)(\alpha^3+\alpha+1)-(3\alpha^2+5\alpha+3)$$
$$=-3\alpha^2-5\alpha-3.$$

Example

Problem. Let α be a zero of x^3+x+1 in $\mathbb{Q}[x]$. Write $\beta=(2\alpha^2+3\alpha-1)/(\alpha^2-\alpha+1)$ in the form $a_0+a_1\alpha+a_2\alpha^2$.

Solution. We first use the Euclidean algorithm to find polynomials $g(x)$ and $h(x)$ such that $(x^3+x+1)g(x)+(x^2-x+1)h(x)=1$. We have

$$x^3+x+1=(x+1)(x^2-x+1)+x$$
$$x^2-x+1=(x-1)x+1$$

Then

$$1=(x^2-x+1)-(x-1)x=x^2(x^2-x+1)-(x-1)(x^3+x+1).$$

It follows that

$$\frac{2\alpha^2+3\alpha-1}{\alpha^2-\alpha+1}=\frac{(2\alpha^2+3\alpha-1)\alpha^2}{(\alpha^2-\alpha+1)\alpha^2}=2\alpha^4+3\alpha^3-\alpha^2$$
$$=(2\alpha+3)(\alpha^3+\alpha+1)-(3\alpha^2+5\alpha+3)$$
$$=-3\alpha^2-5\alpha-3.$$

Example

Problem. Let α be a zero of x^3+x+1 in $\mathbb{Q}[x]$. Write $\beta=(2\alpha^2+3\alpha-1)/(\alpha^2-\alpha+1)$ in the form $a_0+a_1\alpha+a_2\alpha^2$.

Solution. We first use the Euclidean algorithm to find polynomials $g(x)$ and $h(x)$ such that $(x^3+x+1)g(x)+(x^2-x+1)h(x)=1$. We have

$$x^3+x+1=(x+1)(x^2-x+1)+x$$
$$x^2-x+1=(x-1)x+1$$

Then

$$1=(x^2-x+1)-(x-1)x=x^2(x^2-x+1)-(x-1)(x^3+x+1).$$

It follows that

$$\frac{2\alpha^2+3\alpha-1}{\alpha^2-\alpha+1}=\frac{(2\alpha^2+3\alpha-1)\alpha^2}{(\alpha^2-\alpha+1)\alpha^2}=2\alpha^4+3\alpha^3-\alpha^2$$
$$=(2\alpha+3)(\alpha^3+\alpha+1)-(3\alpha^2+5\alpha+3)$$
$$=-3\alpha^2-5\alpha-3.$$

Example

Problem. Let α be a zero of x^3+x+1 in $\mathbb{Q}[x]$. Write $\beta=(2\alpha^2+3\alpha-1)/(\alpha^2-\alpha+1)$ in the form $a_0+a_1\alpha+a_2\alpha^2$.

Solution. We first use the Euclidean algorithm to find polynomials $g(x)$ and $h(x)$ such that $(x^3+x+1)g(x)+(x^2-x+1)h(x)=1$. We have

$$x^3+x+1=(x+1)(x^2-x+1)+x$$
$$x^2-x+1=(x-1)x+1$$

Then

$$1=(x^2-x+1)-(x-1)x=x^2(x^2-x+1)-(x-1)(x^3+x+1).$$

It follows that

$$\frac{2\alpha^2+3\alpha-1}{\alpha^2-\alpha+1}=\frac{(2\alpha^2+3\alpha-1)\alpha^2}{(\alpha^2-\alpha+1)\alpha^2}=2\alpha^4+3\alpha^3-\alpha^2$$
$$=(2\alpha+3)(\alpha^3+\alpha+1)-(3\alpha^2+5\alpha+3)$$
$$=-3\alpha^2-5\alpha-3.$$

Example

Problem. Let α be a zero of x^3+x+1 in $\mathbb{Q}[x]$. Write $\beta=(2\alpha^2+3\alpha-1)/(\alpha^2-\alpha+1)$ in the form $a_0+a_1\alpha+a_2\alpha^2$.

Solution. We first use the Euclidean algorithm to find polynomials $g(x)$ and $h(x)$ such that $(x^3+x+1)g(x)+(x^2-x+1)h(x)=1$. We have

$$x^3+x+1=(x+1)(x^2-x+1)+x$$
$$x^2-x+1=(x-1)x+1$$

Then

$$1=(x^2-x+1)-(x-1)x=x^2(x^2-x+1)-(x-1)(x^3+x+1).$$

It follows that

$$\frac{2\alpha^2+3\alpha-1}{\alpha^2-\alpha+1}=\frac{(2\alpha^2+3\alpha-1)\alpha^2}{(\alpha^2-\alpha+1)\alpha^2}=2\alpha^4+3\alpha^3-\alpha^2$$
$$=(2\alpha+3)(\alpha^3+\alpha+1)-(3\alpha^2+5\alpha+3)$$
$$=-3\alpha^2-5\alpha-3.$$

Example

Problem. Let α be a zero of $x^2 + x + 1 \in \mathbb{Z}_2[x]$ in some extension field. Write $\beta = \alpha/(\alpha + 1)$ in the form $a_0 + a_1\alpha$, where $a_0, a_1 \in \mathbb{Z}_2[x]$.

Solution.

- We have $x^2 + x + 1 = x(x + 1) + 1$. Thus, $(\alpha + 1)^{-1} = \alpha$.
- Then, $\beta = \alpha^2 = \alpha + 1$.

Example

Problem. Let α be a zero of $x^2+x+1 \in \mathbb{Z}_2[x]$ in some extension field. Write $\beta = \alpha/(\alpha+1)$ in the form $a_0 + a_1\alpha$, where $a_0, a_1 \in \mathbb{Z}_2[x]$.

Solution.

- We have $x^2+x+1 = x(x+1)+1$. Thus, $(\alpha+1)^{-1} = \alpha$.
- Then, $\beta = \alpha^2 = \alpha + 1$.

Example

Problem. Let α be a zero of $x^2+x+1 \in \mathbb{Z}_2[x]$ in some extension field. Write $\beta = \alpha/(\alpha+1)$ in the form $a_0 + a_1\alpha$, where $a_0, a_1 \in \mathbb{Z}_2[x]$.

Solution.

- We have $x^2+x+1 = x(x+1)+1$. Thus, $(\alpha+1)^{-1} = \alpha$.
- Then, $\beta = \alpha^2 = \alpha + 1$.

Example, continued

- Note that, by Theorem 29.18, every element in $\mathbb{Z}_2[\alpha]$ can be uniquely written as $a_0 + a_1\alpha$ with $a_0, a_1 \in \mathbb{Z}_2$.
- Thus, $\mathbb{Z}_2[\alpha]$ is a field of 4 elements. (Each a_i has two possible values.)
- The characteristic of $\mathbb{Z}_2[\alpha]$ is clear 2.
- The addition and multiplication tables are

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

Example, continued

- Note that, by Theorem 29.18, every element in $\mathbb{Z}_2[\alpha]$ can be uniquely written as $a_0 + a_1\alpha$ with $a_0, a_1 \in \mathbb{Z}_2$.
- Thus, $\mathbb{Z}_2[\alpha]$ is a field of 4 elements. (Each a_i has two possible values.)
- The characteristic of $\mathbb{Z}_2[\alpha]$ is clear 2.
- The addition and multiplication tables are

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

Example, continued

- Note that, by Theorem 29.18, every element in $\mathbb{Z}_2[\alpha]$ can be uniquely written as $a_0 + a_1\alpha$ with $a_0, a_1 \in \mathbb{Z}_2$.
- Thus, $\mathbb{Z}_2[\alpha]$ is a field of 4 elements. (Each a_i has two possible values.)
- The characteristic of $\mathbb{Z}_2[\alpha]$ is clear 2.
- The addition and multiplication tables are

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

Example, continued

- Note that, by Theorem 29.18, every element in $\mathbb{Z}_2[\alpha]$ can be uniquely written as $a_0 + a_1\alpha$ with $a_0, a_1 \in \mathbb{Z}_2$.
- Thus, $\mathbb{Z}_2[\alpha]$ is a field of 4 elements. (Each a_i has two possible values.)
- The characteristic of $\mathbb{Z}_2[\alpha]$ is clear 2.
- The addition and multiplication tables are

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

Example, continued

$\times$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

Again this field is not isomorphic to $\mathbb{Z}_4$, which is not even an integral domain.

Warning: In exams, if you are asked to construct a field of p^n elements and your answer is $\mathbb{Z}_{p^n}$, you will receive double penalty!!

Example, continued

$\times$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

Again this field is not isomorphic to $\mathbb{Z}_4$, which is not even an integral domain.

Warning: In exams, if you are asked to construct a field of p^n elements and your answer is $\mathbb{Z}_{p^n}$, you will receive double penalty!!

Example, continued

$\times$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

Again this field is not isomorphic to $\mathbb{Z}_4$, which is not even an integral domain.

Warning: In exams, if you are asked to construct a field of p^n elements and your answer is $\mathbb{Z}_{p^n}$, you will receive double penalty!!

In-class exercise

Let α be a zero of $x^3 + x + 1 \in \mathbb{Q}[x]$. Express the following elements of $\mathbb{Q}[\alpha]$ in the form $a_0 + a_1\alpha + a_2\alpha^2$, $a_i \in \mathbb{Q}$.

1. $(\alpha^2 + 2)/(\alpha + 2)$.
2. $(2\alpha^2 + \alpha)/(\alpha^2 + \alpha + 1)$.

Let α be a zero of $x^3 + x + 1 \in \mathbb{Z}_2[x]$ in some extension field of $\mathbb{Z}_2$. Express the following elements of $\mathbb{Z}_2[\alpha]$ in the form $a_0 + a_1\alpha + a_2\alpha^2$, $a_i \in \mathbb{Z}_2$.

1. $(\alpha^2 + 1)/(\alpha^2 + \alpha)$.
2. $(\alpha^2 + \alpha + 1)/(\alpha + 1)$.
3. Give the addition table of $\mathbb{Z}_2[\alpha]$.
4. Give the multiplication table of $\mathbb{Z}_2[\alpha]$.

Homework

Problems 6, 8, 12, 16, 18, 25, 26, 29, 30 of Section 29.