Part 3: Fields

19 Extension Fields

19.1 The Fundamental Theorem of Field Theorey

Definition Extension Field

> A field $\mathbb{E}$ is an **extension field** of a field $\mathbb{F}$ if $\mathbb{F} \subseteq \mathbb{E}$ and the operations of $\mathbb{F}$ are those of $\mathbb{E}$ restricted to $\mathbb{F}$.

- $\mathbb{F}(a, b) = \mathbb{F}(a)\mathbb{F}(b) = \mathbb{F}(b)\mathbb{F}(a)$.
- $\mathbb{F}(c) = \mathbb{F}(ac + b)$, $a, b \in \mathbb{F}$.
- $\mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(\sqrt{a} + \sqrt{b})$.

Theorem 19.1 Fundamental Theorem of Field Theory (Kronecker's Theorem)

> Let $\mathbb{F}$ be a field and let $f(x)$ be a nonconstant polynomial in $\mathbb{F}[x]$. Then there is an extension field $\mathbb{E}$ of $\mathbb{F}$ in which $f(x)$ has a zero.

Proof Let $f(x) = p(x)g(x)$ where $p(x)$ is irreducible. Then

$\phi : \mathbb{F} \to \mathbb{E}$, $a \mapsto a + \langle p(x) \rangle$ is one-to-one and preserves operations.

Write $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, then, in $\mathbb{E}$, $x + \langle p(x) \rangle$ is a zero of $p(x)$, because

$$\begin{aligned} p(x + \langle p(x) \rangle) &= a_n(x + \langle p(x) \rangle)^n + a_{n-1}(x + \langle p(x) \rangle)^{n-1} + \cdots + a_0 \\ &= a_n(x^n + \langle p(x) \rangle) + a_{n-1}(x^{n-1} + \langle p(x) \rangle) + \cdots + a_0 \\ &= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 + \langle p(x) \rangle \\ &= p(x) + \langle p(x) \rangle = 0 + \langle p(x) \rangle. \end{aligned}$$

- Let $f(x) = (x^2+1)(x^3+2x+2) \in \mathbb{Z}_3[x]$, then $E = \mathbb{Z}_3[x]/\left\langle x^2+1 \right\rangle$ with 9 elements, or $E = \mathbb{Z}_3/\left\langle x^3+2x+2 \right\rangle$ with 27 elements.
- Every integral domain is contained in its field of quotients,

  but it's not true for commutative rings in general,

  such as $f(x) = 2x+1 \in \mathbb{Z}_4[x]$ has no zero in any ring containing $\mathbb{Z}_4$ as a subring. Otherwise $0 = 2\beta + 1 = 4\beta + 2 = 2$, which is not true.

19.2 Splitting Fields

Definition Splitting Field

> Let $\mathbb{E}$ be an extension field of $\mathbb{F}$ and let $f(x) \in \mathbb{F}[x]$ with degree at least 1. We say that $f(x)$ **splits** in $\mathbb{E}$ if there are elements $a \in \mathbb{F}$ and $a_1, a_2, \cdots, a_n \in \mathbb{E}$ such that
>
> $$f(x) = a(x-a_1)(x-a_2)\cdots(x-a_n).$$
>
> We call $\mathbb{E}$ a **splitting field** for $f(x)$ over $\mathbb{F}$ if $\mathbb{E} = \mathbb{F}(a_1, a_2, \cdots, a_n)$.

- A splitting field of x^2+1 over $\mathbb{Q}$ is $\mathbb{Q}(\mathrm{i})$, and over $\mathbb{R}$ is $\mathbb{C}$.

Theorem 19.2 Existence of Splitting Fields

> Let $\mathbb{F}$ be a field and let $f(x)$ be a nonconstant element of $\mathbb{F}[x]$. Then there exists a splitting field $\mathbb{E}$ for $f(x)$ over $\mathbb{F}$.

- A splitting field for $f(x) = (x^2-2)(x^2+1)$ over $\mathbb{Q}$ is $Q(\sqrt{2}, \mathrm{i}) = \mathbb{Q}(\sqrt{2})(\mathrm{i}) = \left\{(a+b\sqrt{2}) + (c+d\sqrt{2})\mathrm{i} \mid a,b,c,d \in \mathbb{Q}\right\}$.
- Both $\mathbb{Z}_3(\mathrm{i})$ and $\mathbb{Z}_3[x]/\left\langle x^2+x+2 \right\rangle$ are splitting fields for x^2+x+2 over $\mathbb{Z}_3$.

Theorem 19.3 $\mathbb{F}(a) \approx \mathbb{F}[x]/\langle p(x) \rangle$

> Let $\mathbb{F}$ be a field and let $p(x) \in \mathbb{F}[x]$ be irreducible over $\mathbb{F}$. If a is a zero of $p(x)$ in some extension $\mathbb{E}$ of $\mathbb{F}$, then $\mathbb{F}(a) \approx \mathbb{F}[x]/\langle p(x) \rangle$. Futhermore, if $\deg p(x) = n$, then every member of $\mathbb{F}(a)$ can be uniquely expressed in the form
>
> $$c_{n-1}a^{n-1} + c_{n-2}a^{n-2} + \cdots + c_1 a + c_0,$$
>
> where $c_0, c_1, \cdots, c_{n-1} \in \mathbb{F}$.

- The set $\left\{1, a, \cdots, a^{n-1}\right\}$ is a basis for $\mathbb{F}(a)$ over $\mathbb{F}$.
- If $p(x)$ is reducible, then the splitting field for $p(x)$ has at most $n!$ basis elements over $\mathbb{F}$.

Corollary $\mathbb{F}(a) \approx \mathbb{F}(b)$

> Let $\mathbb{F}$ be a field and let $p(x) \in \mathbb{F}[x]$ be irreducible over $\mathbb{F}$. If a is a zero of $p(x)$ in some extension $\mathbb{E}$ of $\mathbb{F}$ and b is a zero of $p(x)$ in some extension $\mathbb{E}'$ of $\mathbb{F}$, then $\mathbb{F}(a) \approx \mathbb{F}(b)$.

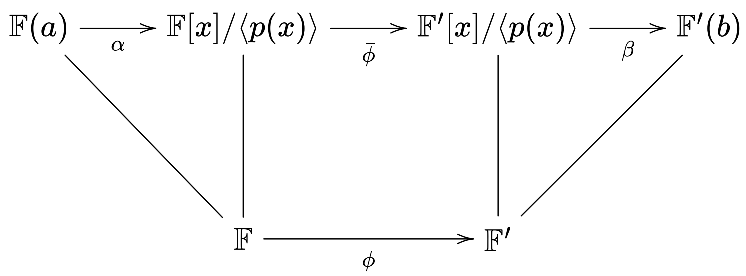
Lemma

Let $\mathbb{F}$ be a field, let $p(x) \in \mathbb{F}[x]$ be irreducible over $\mathbb{F}$, and let a be a zero of $p(x)$ in some extension of $\mathbb{F}$. If ϕ is a field isomorphism from $\mathbb{F}$ to $\mathbb{F}'$ and b is a zero of $\phi(p(x))$ in some extension of $\mathbb{F}'$, then there is an isomorphism from $\mathbb{F}(a)$ to $\mathbb{F}'(b)$ that agrees with ϕ on $\mathbb{F}$ and carries a to b.

Proof Define

$$\begin{array}{ll|ll} \phi: & \mathbb{F} \to \mathbb{F}' & \alpha: & \mathbb{F}(a) \to \mathbb{F}[x]/\langle p(x)\rangle \\ & & & f(a) \mapsto f(x) + \langle p(x)\rangle \\ \bar{\phi}: & \mathbb{F}[x]/\langle p(x)\rangle \to \mathbb{F}'[x]/\langle p(x)\rangle & \beta: & \mathbb{F}'[x]/\langle \phi(p(x))\rangle \to \mathbb{F}'(b) \\ & f(x) + \langle p(x)\rangle \mapsto \phi(f(x)) + \langle \phi(p(x))\rangle & & f(x) + \langle \phi(p(x))\rangle \mapsto f(b) \end{array}$$

Then $\beta\bar{\phi}\alpha : \mathbb{F}(a) \to \mathbb{F}'(b)$.



Theorem 19.4 Extending $\phi : \mathbb{F} \to \mathbb{F}'$

Let ϕ be an isomorphism from a field $\mathbb{F}$ to a field $\mathbb{F}'$ and let $f(x) \in \mathbb{F}[x]$. If $\mathbb{E}$ is a splitting field for $f(x)$ over $\mathbb{F}$ and $\mathbb{E}'$ is a splitting field for $\phi(f(x))$ over $\mathbb{F}'$, then there is an isomorphism from $\mathbb{E}$ to $\mathbb{E}'$ that agrees with ϕ on $\mathbb{F}$.

Corollary Splitting Fields Are Unique

Let $\mathbb{F}$ be a field and let $f(x) \in \mathbb{F}[x]$, then any two splitting fields of $f(x)$ over $\mathbb{F}$ are isomorphic.

Proof Letting ϕ be the identity from $\mathbb{F}$ to $\mathbb{F}$.

- The splitting field of $x^n - a$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[n]{a}, \omega)$, where $\omega = \mathrm{e}^{2\pi\mathrm{i}/n}$.

19.3 Zeros of an Irreducible Polynomial

Definition Derivative

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ belong to $\mathbb{F}[x]$. The derivative of $f(x)$, denoted by $f'(x)$, is the polynomial $na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1$ in $\mathbb{F}[x]$.

Lemma Properties of the Derivative

Let $f(x), g(x) \in \mathbb{F}[x]$, $a \in \mathbb{F}$, then

1. $(f(x) + g(x))' = f'(x) + g'(x)$.
2. $(af(x))' = af'(x)$.
3. $(f(x)g(x))' = f(x)g'(x) + g(x)f'(x)$.

Theorem 19.5 Criterion for Multiple Zeros

A polynomial $f(x)$ over a field $\mathbb{F}$ has a multiple zero in some extension $\mathbb{E}$ if and only if $f(x)$ and $f'(x)$ have a common factor of positive degree in $\mathbb{F}[x]$.

Theorem 19.6 Zeros of an Irreducible

> Let $f(x)$ be an irreducible polynomial over a field $\mathbb{F}$. If $\mathbb{F}$ has characteristic 0, then $f(x)$ has no multiple zeros. If $\mathbb{F}$ has characteristic $p \neq 0$, then $f(x)$ has a multiple zero only if it is of the form $f(x) = g(x^p)$ for some $g(x)$ in $\mathbb{F}[x]$.

Definition Perfect Field

> A field $\mathbb{F}$ is called **perfect** if $\mathbb{F}$ has characteristic 0 or if $\mathbb{F}$ has characteristic p and $\mathbb{F}^p = \{a^p \mid a \in \mathbb{F}\} = \mathbb{F}$.

Theorem 19.7 Finite Fields Are Perfect

> Every finite field is perfect.

Proof $\phi(x) = x^p$ preserves operations, and is one-to-one and onto.

Theorem 19.8 Criterion for No Multiple Zeros

> If $f(x)$ is an irreducible polynomial over a perfect field $\mathbb{F}$, then $f(x)$ has no multiple zeros.

Proof Let $\mathbb{F}$ has characteteristic p, and that $f(x) = g(x^p)$, since $\mathbb{F}^p = \mathbb{F}$, we have

$$\begin{aligned} f(x) = g(x^p) &= a_n x^{pn} + a_{n-1} x^{p(n-1)} + \cdots + a_1 x^p + a_0 \\ &= b_n^p x^{pn} + b_{n-1}^p x^{p(n-1)} + \cdots + b_1^p x^p + b_0^p \\ &= (b_n x^n + b_{n-1} x^{n-1} + \cdots + b_0)^p = (h(x))^p, \end{aligned}$$

but then $f(x)$ is reducible.

Theorem 19.9 Zeros of an Irreducible over a Splitting Field

> Let $f(x)$ be an irreducible polynomial over a field $\mathbb{F}$ and let $\mathbb{E}$ be a splitting field of $f(x)$ over $\mathbb{F}$. Then all the zeros of $f(x)$ in $\mathbb{E}$ have the same multiplicity.

Proof If a has multiplicity m, then in $\mathbb{E}[x]$ we may write
$f(x) = (x-a)^m g(x) = \phi(f(x)) = (x-b)^m \phi(g(x))$, thus the multiplicity of a is less than b. Likewise, the multiplicity of b is less than a.

- Let $f(x)$ be an irreducible polynomial over a field $\mathbb{F}$, then the number of distinct zeros of $f(x)$ in a splitting field divides $\deg f(x)$.

Corollary Factorization of an Irreducible over a Splitting Field

> Let $f(x)$ be an irreducible polynomial over a fied $\mathbb{F}$ and let $\mathbb{E}$ be a splitting field of $f(x)$. Then $f(x)$ has the form
>
> $$f(x) = a(x-a_1)^n (x-a_2)^n \cdots (x-a_t)^n,$$
>
> where $a_1, a_2, \cdots, a_t$ are distinct elements of $\mathbb{E}$ and $a \in \mathbb{F}$.

19.4 Exercises

1. If $f(x)$ and $g(x)$ are relatively prime in $\mathbb{F}[x]$, they are also relatively prime in $\mathbb{E}[x]$, where $\mathbb{E}$ is any extension field of $\mathbb{F}$.

Question: 42.

19.5 Bibliography of Leopold Kronecker

20 Algebraic Extensions

20.1 Characterization of Extensions

Definition Types of Extensions

> Let $\mathbb{E}$ be an extension field of a field $\mathbb{F}$ and let $a \in \mathbb{E}$. We call a **algebraic** over $\mathbb{F}$ if a is the zero of some nonzero polynomial in $\mathbb{F}[x]$. Otherwise, it is called **transcendental** over $\mathbb{F}$. An extension $\mathbb{E}$ of $\mathbb{F}$ is called an **algebraic extension** of $\mathbb{F}$ if every element of $\mathbb{E}$ is algebraic over $\mathbb{F}$. Otherwise, it is called a **transcendental** extension of $\mathbb{F}$. An extension of $\mathbb{F}$ of the form $\mathbb{F}(a)$ is called a **simple extension** of $\mathbb{F}$.

Theorem 20.1 Characterization of Extensions

> Let $\mathbb{E}$ be an extension field of the field $\mathbb{F}$ and let $a \in \mathbb{E}$. If a is transcendental over $\mathbb{F}$, then $\mathbb{F}(a) \approx \mathbb{F}(x)$.
>
> If a is algebraic over $\mathbb{F}$, then $\mathbb{F}(a) \approx \mathbb{F}[x]/\left\langle p(x)\right\rangle$, where $p(x)$ is a polynomial in $\mathbb{F}[x]$ of minimum degree such that $p(a) = 0$. Moreover, $p(x)$ is irreducible over $\mathbb{F}$.

Theorem 20.2 Uniqueness Property

> If a is algebraic over a field $\mathbb{F}$, then there is a unique monic irreducible polynomial $p(x)$ in $\mathbb{F}[x]$ such that $p(a) = 0$, which is called the **minimal polynomial** for a over $\mathbb{F}$.

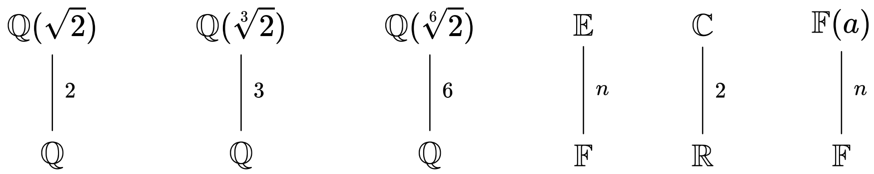
Theorem 20.3 Divisibility Property

> Let a be algeraic over $\mathbb{F}$, and let $p(x)$ be the minimal polynomial for a over $\mathbb{F}$. If $f(x) \in \mathbb{F}[x]$ and $f(a) = 0$, then $p(x) \mid f(x)$ in $\mathbb{F}[x]$.

20.2 Finite Extensions

Definition Degree of an Extension

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



Theorem 20.4 Finite Implies Algebraic

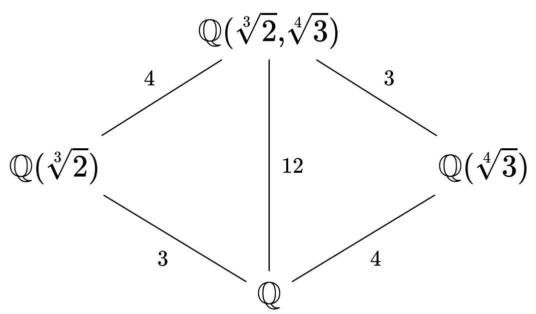
> If $\mathbb{E}$ is a finite extension of $\mathbb{F}$, then $\mathbb{E}$ is an algebraic extension of $\mathbb{F}$.

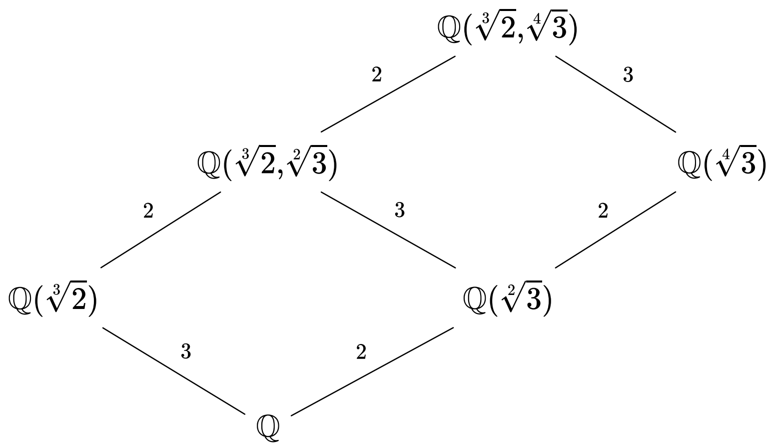
- The converse is not true, since $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \cdots)$ is an algebraic extension of $\mathbb{Q}$.

Theorem 20.5 $[\mathbb{K} : \mathbb{F}] = [\mathbb{K} : \mathbb{E}][\mathbb{E} : \mathbb{F}]$

> Let $\mathbb{K}$ be a finite extension field of the field $\mathbb{E}$ and let $\mathbb{E}$ be a finite extension field of the field $\mathbb{F}$.

- $[\mathbb{L} : \mathbb{J}] = n$ if and only if $\mathbb{L} \approx \mathbb{J}^n$.
- The subfield lattice of $\mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{3})$ is the same as the subgroup lattice of $\mathbb{Z}_{12}$.





Theorem 20.6 Primitive Element Theorem

> If $\mathbb{F}$ is a field of characteristic 0, and a and b are algebraic over F, then there is an element c in $\mathbb{F}(a, b)$ such that $\mathbb{F}(a, b) = \mathbb{F}(c)$.

- Any finite extension of a field of characteristic 0 is a simple extension.
- An element a with the property that $\mathbb{E} = \mathbb{F}(a)$ is called a **primitive element** of $\mathbb{E}$.

20.3 Properties of Alebraic Extensions

Theorem 20.7 Algbraic over Algebraic Is Algebraic

> If $\mathbb{K}$ is an algebraic extension of $\mathbb{E}$ and $\mathbb{E}$ is an algebraic extension of $\mathbb{F}$, then $\mathbb{K}$ is an algebraic extension of $\mathbb{F}$.

Corollary Subfield of Algebraic Elements

> Let $\mathbb{E}$ be an extension field of the field $\mathbb{F}$. Then the set of all elements of $\mathbb{E}$ that are algebraic over $\mathbb{F}$ is a subfield of $\mathbb{E}$.

Proof Suppose that $a, b \in \mathbb{E}$ are algebraic over $\mathbb{F}$ and $b \neq 0$, to show that $a + b$, $a - b$, ab, a/b are algebraic, it suffices to show that $[\mathbb{F}(a, b) : \mathbb{F}] = [\mathbb{F}(a, b) : \mathbb{F}(b)][\mathbb{F}(b) : \mathbb{F}]$ is finite.

- This subfield is called the **algebraic closure** of $\mathbb{F}$ in $\mathbb{E}$.
- A field with no proper algebraic extension is called **algebraically closed**.
- Every field $\mathbb{F}$ has a unique (up to isomorphism) algebraic extension that is algebraically closed, which is called the **algebraic closure** of $\mathbb{F}$.

20.4 Exercises

Degree

1. If $\mathbb{E}$ is an extension of $\mathbb{F}$ of prime degree, then $\forall a \in \mathbb{E}, \mathbb{F}(a) = \mathbb{F}$ or $\mathbb{F}(a) = \mathbb{E}$.
2. $[\mathbb{E} : \mathbb{F}] = 1 \Leftrightarrow \mathbb{E} = \mathbb{F}$.
3. If $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{L}$ and $\mathbb{L}$ is a finite extension, then $[\mathbb{L} : \mathbb{F}] = [\mathbb{L} : \mathbb{K}] \Leftrightarrow \mathbb{F} = \mathbb{K}$.
4. Let $\mathbb{F} \subseteq \mathbb{E}_1, \mathbb{E}_2 \subseteq \mathbb{K}$, if $[\mathbb{E}_1 : \mathbb{F}]$ and $[\mathbb{E}_2 : \mathbb{F}]$ are both prime, then $\mathbb{E}_1 = \mathbb{E}_2$ or $\mathbb{E}_1 \cap \mathbb{E}_2 = \mathbb{F}$.
5. If $f(x)$ and $g(x)$ are irreducible over $\mathbb{F}$ and $\deg f(x)$ and $\deg g(x)$ are relatively prime. If a is a zero of $f(x)$ in some extension $\mathbb{F}$, then $g(x)$ is irreducible over $\mathbb{F}(a)$.
6. Let $\mathbb{E}$ be an algebraic extension of a field $\mathbb{D}$. If $\mathbb{R}$ is a ring and $\mathbb{E} \supseteq \mathbb{R} \supseteq \mathbb{F}$, show that $\mathbb{R}$ must be a field.

Algebraic and Transcendental

1. If a is algebraic over $\mathbb{Q}$, then $a^{m/n}$ is algebraic over $\mathbb{Q}$.

   If a is transcendental over $\mathbb{Q}$, then $a^{m/n}$ is transcendental over $\mathbb{Q}$.

2. If α and β are real and transcendental over $\mathbb{Q}$, then either $\alpha\beta$ or $\alpha + \beta$ is also transcendental over $\mathbb{Q}$. ⭐

3. Let $f(x)$ be a nonconstant element of $\mathbb{F}[x]$. If a belongs to some extension of $\mathbb{F}$ and $f(a)$ is algebraic over $\mathbb{F}$, then a is algebraic over $\mathbb{F}$.

Others

1. If $\mathbb{F}$ is a field and the multplicative group of nonzero elements of $\mathbb{F}$ is cyclic, then $\mathbb{F}$ is finite.
2. A splitting field $\mathbb{K}$ of $\mathbb{F}$ is a finite extension.

20.5 Bibliography of Ernst Steinitz

21 Finite Fields

21.1 Classification of Finite Fields

Theorem 21.1 Classification of Finite Fields

> For each prime p and each positive integer n, there is, up to isomorphism, a unique finite field or order p^n.

Proof The splitting field $\mathbb{E}$ of $f(x) = x^{p^n} - x$ over $\mathbb{Z}_p$ has exactly p^n elements and is unique.

- A field of order p^n is denoted by $\mathrm{GF}(p^n)$.

21.2 Structure of Finite Fields

Theorem 21.2 Structure of Finite Fields

> As a group under addition, $\mathrm{GF}(p^n) \approx \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$;
>
> As a group under multiplication, $\mathrm{GF}(p^n)^* \approx \mathbb{Z}_{p^n-1}$, which is cyclic.

- $\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$ is not a field.

It's a vector space over $\mathbb{Z}_p$ with $\{(1,0,\cdots,0),\cdots,(0,0,\cdots,1)\}$ as a basis.

Corollary 1

> $[\mathrm{GF}(p^n):\mathrm{GF}(p)]=n.$

- $[\mathrm{GF}(p^m):\mathrm{GF}(p^n)]=\dfrac{[\mathrm{GF}(p^m):\mathrm{GF}(p)]}{[\mathrm{GF}(p^n):\mathrm{GF}(p)]}=m/n.$

Corollary 2 $\mathrm{GF}(p^n)$ Contains an Element of Degree n

> Let a be a generator of the group of nonzero elements of $\mathrm{GF}(p^n)$ under multiplication, then a is algebraic over $\mathrm{GF}(p)$ of degree n.

Proof $[\mathrm{GF}(p)(a):\mathrm{GF}(p)]=[\mathrm{GF}(p^n):\mathrm{GF}(p)]=n.$

Theorem 21.3 Zeros of an Irreducible over $\mathbb{Z}_p$

> Let $f(x)\in\mathbb{Z}_p[x]$ be an irreducible polynomial over $\mathbb{Z}_p$ of degree d and let a be a zero of $f(x)$ in some extension $\mathbb{E}$ of $\mathbb{Z}_p$. Then $a,a^p,a^{p^2},\cdots,a^{p^{d-1}}$ are the zeros of $f(x)$ and they are distinct.

- To prove it, notice that $\forall i\in\mathbb{N}^+,\forall c\in\mathbb{Z}_p^*$, $c=c^p=c^{p^i}$ and the automorphism of $\mathrm{GF}(p^n)$ given by $\phi(x)=x^{p^i}$.

Corollary Splitting Field of an Irreducible Polynomial Over $\mathbb{Z}_p$

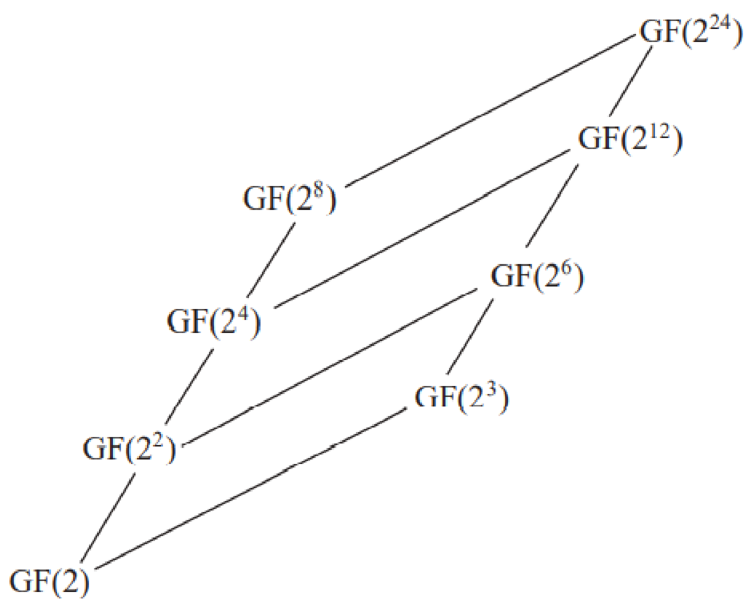
> If $f(x)$ is an irreducible polynomial over $\mathbb{Z}_p$ and a is a zero of $f(x)$ in some extension field of $\mathbb{Z}_p$, then $\mathbb{Z}_p(a)$ is the splitting field of $f(x)$ over $\mathbb{Z}_p$.

21.3 Subfields of a Finite Field

Theorem 21.4 Subfields of a Finite Field

> For each divisor m of n, $\mathrm{GF}(p^n)$ has a unique subfield of order p^m. Moreover , these are the only subfields of $\mathrm{GF}(p^n)$.

- $\mathbb{K}=\left\{x\in\mathrm{GF}(p^n)\mid x^{p^m}=x\right\}$ is a subfield of $\mathrm{GF}(p^n)$ of order p^m.
- The subfield lattice of $\mathrm{GF}(2^{24})$



Theorem 21.5 Degrees of Irreducible Factors of $x^{p^n}-x$ over $\mathbb{Z}_p$

> The degree of an irreducible factor of $x^{p^n}-x$ over $\mathbb{Z}_p$ divides n.

Proof If $g(x)$ is an irreducible factor of $x^{p^n}-x$ over $\mathbb{Z}_p$ with degee d and $a\in\mathrm{GF}(p^n)$ is a zero of $g(x)$, then $|\mathbb{Z}_p(a)|=p^d$. ⭐

21.4 Exercises

1. If $|\mathbb{F}|=2^p$, then $x=(x^n)^2$.
2. If $p(x)$ is a polynomial in $\mathbb{Z}_p$ with no multiple zeros, then $p(x)$ divides $x^{p^n}-x$ for some n. (Hint: consider $\mathbb{Z}_p(x_1,x_2,\cdots,x_m)$.)
3. If a is a nonsquare in $\mathbb{Z}_p$ where $p\neq 2$, then a is a nonsquare in $\mathrm{GF}(p^n)$ if and only if n is odd.
4. $x^{p^n}-x+1$ has no zero in $\mathrm{GF}(p^n)$, thus no finite field is algebraically closed. (Or find a prime q such that $q\nmid n$, then $\mathrm{GF}(p^{nq})$ is a proper extension.)
5. A finite extension of a finite field is a simple extension. (Hint: find a generator.)
6. If $\mathrm{GF}(5^2)=\mathbb{Z}_5(a)$, then $\mathrm{GF}(5^n)^*=\{1,1+a,1+a+a^2,\cdots,1+a+a^2+a^3+\cdots+a^{23}\}$.

   Proof: To prove that there is no zero in the set, we need only to verify that $1+a+\cdots+a^n$ is not a zero.
7.

Q50 distinct.

Confusion: 58, is a generator.

Confusion: 61, is $1+a+\cdots+a^n$ a zero?

21.5 Bibliography of L.E.Dickson

21.6 Bibliography of E.H.Moore

22 Geometric Constructions

22.1 Historical Discussion of Geometric Constructions

22.2 Constructible Numbers

22.3 Angle-Trisectors and Circle-Squares

22.4 Exercises