Review: Feilds

Def: E is E xtension field of F if $F \subset E$

Theorem 21.5. *Let F be a field and let $p(x)$ be a nonconstant polynomial in $F[x]$. Then there exists an extension field E of F and an element $\alpha \in E$ such that $p(\alpha) = 0$.*

$\alpha \in E$ is algebraic over F if $f(\alpha) = 0$ for some $f(x) \in F[x]$

i is algebraic over $\mathbb{R}, \mathbb{Q} \Rightarrow x^2 + 1$

π is not alg. over $\mathbb{Q}$

π is alg over $\mathbb{R}$

$E = F(\alpha)$ — simple extension

algebraic number $= \alpha \in \mathbb{C}$ s.t. α is alg. over $\mathbb{Q}$.

Theorem 21.9. *Let E be an extension field of F and $\alpha \in E$. Then α is transcendental over F if and only if $F(\alpha)$ is isomorphic to $F(x)$, the field of fractions of $F[x]$.*

$\alpha \in E$ alg. over F

→ it has minimal polynomial is unique, monic, irreducible poly $p(x) \in F[x]$ of smallest degree s.t. $p(\alpha) = 0$.

$F[\alpha] \cong F[x]/\{0\}$ — If α is transcedental.

Proposition 21.12. *Let E be a field extension of F and $\alpha \in E$ be algebraic over F. Then $F(\alpha) \cong F[x]/\langle p(x) \rangle$, where $p(x)$ is the minimal polynomial of α over F.*

$a_0 + \cdots + \alpha^n = 0$

division alg. Say that given any $f(x) \in F[x]$, $\deg(f) > \deg(p)$

then $f(x) = p(x) \cdot q(x) + r(x)$

Theorem 21.10. *Let E be an extension field of a field F and $\alpha \in E$ with α algebraic over F. Then there is a unique irreducible monic polynomial $p(x) \in F[x]$ of smallest degree such that $p(\alpha) = 0$. If $f(x)$ is another polynomial in $F[x]$ such that $f(\alpha) = 0$, then $p(x)$ divides $f(x)$.*

Ex] $x^2 - 2 \Rightarrow \sqrt{2}$

$x^4 - 4x^2 + 1 \Leftrightarrow \sqrt{2+\sqrt{3}}$

Simple extensions $F(\alpha)$ with min poly. $p(x)$

$\deg(p) = n$ are a $\dim = n$ v. space over F

Every element of $F(\alpha)$ is $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$

$a_i \in F$

Theorem 21.13. *Let $E = F(\alpha)$ be a simple extension of F, where $\alpha \in E$ is algebraic over F. Suppose that the degree of α over F is n. Then every element $\beta \in E$ can be expressed uniquely in the form*

$$\beta = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$$

for $b_i \in F$.

↑ basis of $F(\alpha)$ as a F. v. space

is $\{1, \alpha, \ldots, \alpha^{n-1}\}$

If E is a finite dim. v. space over F $\dim_F(E) = n$ (↑ denotes v. space dim over F.)

write $[E:F] = n$ ↑ degree of the field extension E.

Thm: Every finite extension is algebraic

Note: alg. extensions can be infinite.

Ex) the set of all elements of $\mathbb{R}$ which are alg. over $\mathbb{Q}$.

Note: vector spaces will only appear in the context of fields for the final.

Theorem 21.17. *If E is a finite extension of F and K is a finite extension of E, then K is a finite extension of F and*

$$[K : F] = [K : E][E : F].$$

Ex $K = F(\alpha, \beta)$ not a simple extension

$\cong (F(\beta))(\alpha) \cong F(\beta)[x]/\langle p(x) \rangle$ ← p is the min. poly of α over $F(\beta)$.

$[F(\alpha,\beta) : F] = [F(\alpha,\beta) : F(\beta)][F(\beta) : F]$

$F(\beta) \cong F[y]/\langle q(y) \rangle$ where q is min poly of β over F

Theorem 21.17. *If E is a finite extension of F and K is a finite extension of E, then K is a finite extension of F and*

$$[K : F] = [K : E][E : F].$$

↳ basis of K over F is

$\{\alpha_i \beta_j\}$ ← K as an F v. space

α_i: basis of E as an F v. space

β_j: basis of K as an E v. space

$\mathbb{Q}(\sqrt{2}, \sqrt{3})$ ← $\{1, \sqrt{3}\}$ as a $\mathbb{Q}(\sqrt{2})$ v. space.

↓ has basis $\{1, \sqrt{2}\}$ as a $\mathbb{Q}$ v. space

has basis $\{1, \sqrt{2}, \sqrt{3}, \sqrt{2}\cdot\sqrt{3}\}$ ($= \sqrt{6}$) over $\mathbb{Q}$.

Theorem 21.23. *Let E be an extension field of F. The set of elements in E that are algebraic over F form a field.*

↳ $\overline{\mathbb{Q}} \neq \mathbb{C}$ — alg. closed

↑ alg.-closed ↑ all elements algebraic over $\mathbb{Q}$.

alg. closure of F in E = all elements in E that are alg. over F

alg. closed = every nonconstant poly in $F[x]$ has a root in F.

Theorem 21.25. *A field F is algebraically closed if and only if every nonconstant polynomial in $F[x]$ factors into linear factors over $F[x]$.*

Every field has a unique algebraic closure.

Splitting fields

$E = F(\alpha_1, \dots, \alpha_n)$ is a splitting field of $p(x)$ if

$p(x) = (x-\alpha_1) \cdots (x-\alpha_n)$

Thm] Exists a unique (upto isomorphism) splitting field for every $p(x) \in F[x]$.

$f(x) \in F[x]$, $\deg(f) = n$ is Separable = f has n distinct roots in its splitting field.

E seperable = $\forall \alpha \in E$ root of some sep

f seperable iff $\gcd(f(x), f'(x)) = 1$

---

unique finite field with p^n elements is called Galois field $GF(p^n)$, all finite fields are isomorphic to these

Theorem 22.6. *For every prime p and every positive integer n, there exists a finite field F with p^n elements. Furthermore, any field of order p^n is isomorphic to the splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$.*

we can draw lattice pictures

Theorem 22.7. *Every subfield of the Galois field $\mathrm{GF}(p^n)$ has p^m elements, where m divides n. Conversely, if $m \mid n$ for $m > 0$, then there exists a unique subfield of $\mathrm{GF}(p^n)$ isomorphic to $\mathrm{GF}(p^m)$.*

$GF(2^6)$

$GF(2^3)^* \cong \mathbb{Z}_{8-1} \cong \mathbb{Z}_7$

$GF(2^3)$ $GF(2^2)$

$GF(2)$

F^* = mult. group of non-zero elements $\cong \mathbb{Z}_n$ for some n

Corollary 22.11. *The multiplicative group of all nonzero elements of a finite field is cyclic.*

Corollary 22.12. *Every finite extension E of a finite field F is a simple extension of F.*

Splitting field of $x^4 + 2 = \mathbb{Q}(2^{\frac{1}{4}}, i)$ ← minimal polynomial $x^4 - 2$ ↳ $2^{\frac{1}{4}} + i$

$\mathbb{Q}(2^{\frac{1}{4}})$ has basis $\{1, 2^{\frac{1}{4}}, 2^{\frac{1}{2}}, 2^{\frac{3}{4}}\}$

roots of x^4+2 are $x = \frac{\pm 1 \pm i}{2^{\frac{1}{4}}}$

$$[\mathbb{Q}(2^{\frac{1}{4}}, i) : \mathbb{Q}] = [\mathbb{Q}(2^{\frac{1}{4}}, i) : \mathbb{Q}(i)]\,[\mathbb{Q}(i) : \mathbb{Q}]$$

(min poly x^4-2 over $\mathbb{Q}(i)$; min x^2+1 over $\mathbb{Q}$)

E is the splitting field of x^4+2

Show $\mathbb{Q}(2^{\frac{1}{4}}, i) \supseteq E$ ✓

$E \subseteq \mathbb{Q}(2^{\frac{1}{4}}, i)$ ✓ basis $\{1, 2^{\frac{1}{4}}, 2^{\frac{1}{2}}, 2^{\frac{3}{4}}, i, i2^{\frac{1}{4}}, i2^{\frac{1}{2}}, i2^{\frac{3}{4}}\}$

Find a finite field E with 27 elements.

$27 = 3^3$

we know that $E \supseteq GF(3^3)$.

we would expect a degree 3 field extension of $\mathbb{Z}/3\mathbb{Z}$.

$\{1, \alpha, \alpha^2\}$ (Since all finite extensions of a finite are finite and simple)

[Any $GF(p^n)$ is a degree n extension of $\mathbb{Z}/p\mathbb{Z}$]

Let $p(x) = x^3 - x^2 + x + 1$, $p(x)$ is irreducible over $\mathbb{Z}_3$ since $p(0) = 1$, $p(1) = 2$, $p(2) = 1$

because if p factored over $\mathbb{Z}_3$ it must have at least 1 linear factor. Let α be a root of $p(x)$

then $\mathbb{Z}_3(\alpha) \cong \mathbb{Z}_3[x]/\langle x^3 - x^2 + x + 1 \rangle$

this is our field with 27 elements.

$\mathbb{Z}_3(\alpha)^* \cong \mathbb{Z}_{26}^+ \cong \langle \alpha \rangle$ ← additive group

$\alpha^{26} = 1$

Is $E = \mathbb{Z}_2[x]/\langle x^3 + x + 1 \rangle \cong \mathbb{Z}_2[x]/\langle x^3 + x^2 + 1 \rangle = K$?

Yes. $p(x)$ $g(x)$

$p(0) = 1$ $g(0) = 1$

$p(1) = 1$ $g(1) = 1$

∴ p, g are both irr. ∴ E, K are finite fields and both are degree 3 field extensions of $\mathbb{Z}_2$

∴ have 8 elements

∴ $E \cong GF(2^3) \cong K$ ∎.

Ex)

Let K be a finite extension of F s.t. $[K:F] = p$ is prime. If $u \in K - F$ show that $K = F(u)$

Proof: $F \subseteq F(u) \subseteq K$

$u \notin F \quad \therefore \quad F \neq F(u)$

$[F(u) : F] > 1$ but

$p = [k:F] = [K:F(u)][F(u):F]$ ($[F(u):F] > 1$)

$\therefore \quad [F(u):F] = p$

$\Rightarrow \quad [k:F(u)] = 1 \quad \therefore \quad K = F(u)$. ∎

Break Down of Final

- 38% on fields
- 32% on rings
- rest on groups