Thm If E is a finite extension of F, K is a finite extension of E, then K is a finite etension of F ($F \subseteq E \subseteq K$) and

$$[K:F] = \underbrace{[K:E]}_{=m}\underbrace{[E:F]}_{=n}$$

Proof: Let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis for E as an F-vector space and $\{\beta_1, \ldots, \beta_m\}$ be a basis for K as a E vector space

$F \subseteq E \subseteq K$

Show $\{\alpha_i \beta_j\}$ forms a basis for K over F

Show spans K. Let $u \in K$ arbitrary, then

$$u = \sum_{i=1}^{m} b_i \beta_i \qquad \text{and} \qquad b_i \in E$$

Since $b_i \in E \Rightarrow b_i = \sum_{j=1}^{n} a_{ij} \alpha_j$, $a_{ij} \in F$

$$\therefore \; u = \sum_{i=1}^{m} \sum_{j=1}^{n} \underbrace{a_{ij}}_{\in F} \beta_i \alpha_j$$

$\therefore \{ \alpha_j \beta_i \mid i = 1, \ldots, m, \; j = 1, \ldots, n \}$ spans K over F.

Show $\{\alpha_i \beta_j\}$ is lin. independent

$$u = \sum_{i=1}^{n} \sum_{j=1}^{m} c_{ij} \alpha_i \beta_j = 0 \in K, \quad c_{ij} \in F$$

$$= \sum_{j=1}^{m} \underbrace{\left(\sum_{i=1}^{n} c_{ij} \alpha_i \right)}_{\in E} \beta_j = 0$$

since β_j are lin. ind. over E

$$\Rightarrow \sum_{i=1}^{n} c_{ij} \alpha_i = 0$$

$\Rightarrow c_{ij} = 0$ since α_i's are lin. ind over F

$\therefore \{\alpha_i \beta_j\}$ is a basis ∎

<u>cor</u> If F_i is a field, $i = 1, \dots, k$, $F_1 \subset \cdots \subset F_k$ and if F_{i+1} is a finite extension of F_i then F_k is a finite extension of F_1 and

$$[F_k : F_1] = [F_k : F_{k-1}][F_{k-1} : F_{k-2}] \cdots \cdots [F_2 : F_1].$$

<u>cor</u> Let E be a extension field of F. If $\alpha \in E$ is alg. over F with minimal poly. $p(x)$ and $\beta \in F(\alpha)$ with min poly $q(x)$ (associated to $F(\alpha)$ over $F(\beta)$) then

$$\deg(q(x)) \mid \deg(p(x)).$$

Proof:

$$\deg(p(x)) = [F(\alpha):F]$$

$$\deg(q(x)) = [F(\alpha):F(\beta)]$$

$$F \subset F(\beta) \subset F(\alpha) \subset E$$

$$\underbrace{[F(\alpha):F]}_{=\deg(p(x))} = \underbrace{[F(\alpha):F(\beta)]}_{=\deg(q(x))} \cdot [F(\beta):F]$$

$\therefore$ Since $[F(\beta):F] \in \mathbb{Z}_+$

$\Rightarrow \deg(q(x)) \mid \deg(p(x))$ ∎

Ex] Determine $\mathbb{Q}(\sqrt{3}+\sqrt{5})$

The min. poly of $\sqrt{3}+\sqrt{5}$ is

$$x^4 - 16x^2 + 4$$

$$[\mathbb{Q}(\sqrt{3}+\sqrt{5}):\mathbb{Q}] = 4$$

- $\{1, \sqrt{3}\}$ is a basis for $\mathbb{Q}(\sqrt{3})$ over $\mathbb{Q}$ with min poly x^2-3
- $\{1, \sqrt{5}\}$ is a basis for $\mathbb{Q}(\sqrt{5})$ over $\mathbb{Q}$, with min poly x^2-5.

$\{1, \sqrt{3}, \sqrt{5}, \sqrt{3}\cdot\sqrt{5}\}$ is a basis for $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ over $\mathbb{Q}$

and $\quad \dim_{\mathbb{Q}}(\mathbb{Q}(\sqrt{3}, \sqrt{5})) = 4 \quad$, i.e $[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 4$

$\sqrt{3} + \sqrt{5} \in \mathbb{Q}(\sqrt{3}, \sqrt{5})$

$\therefore \quad \mathbb{Q}(\sqrt{3} + \sqrt{5}) = \mathbb{Q}(\sqrt{3}, \sqrt{5})$

and $\quad$ this is actually a simple extension of degree 4

Can have $\quad F(\alpha_1, \dots, \alpha_n) = F(\alpha) \cong F[x]/\langle p(x) \rangle$

Note $\quad [\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}(\sqrt{3})] = 2$

and min. poly of $\sqrt{5}$ over $\mathbb{Q}(\sqrt{3})$ is still $x^2 - 5$.

Thm Let E be a field extension of F. The following are equivalent

1) E is a finite extension of F

2) $\exists$ a finite number of algebraic elements $\alpha_1, \dots, \alpha_n \in E$ s.t. $E = F(\alpha_1, \dots, \alpha_n)$

3) There exists a sequence of fields

$$E = F(\alpha_1, \dots, \alpha_n) \supseteq F(\alpha_1, \dots, \alpha_{n-1}) \supseteq \cdots \supseteq F(\alpha_1) \supseteq F$$

Thm Let E be a field extension of F. The set A_F of elements in E that are algebraic over F form a field.

Proof: Let $\alpha, \beta \in A_F$ i.e. α, β are alg. over F

$\Rightarrow$ $F(\alpha, \beta)$ is a finite extension

and all elements of $F(\alpha, \beta)$ are alg. over F

$$\therefore \underbrace{\alpha \pm \beta,\ \alpha\beta,\ \frac{\alpha}{\beta},\ \frac{1}{\beta},\ \frac{1}{\alpha}}_{\in A_F} \quad (\beta \neq 0,\ \alpha \neq 0 \text{ respectively})$$

are algebraic over F

$\therefore$ A_F is a field. ■

- set of all numbers in $\mathbb{C}$ which are the roots of some polynomial $P(x) \in \mathbb{Q}[x]$

Cor) The set of all algebraic numbers = algebraic elements of $\mathbb{C}$ over $\mathbb{Q}$

is a field.

Def) Let E be a field extension of F.

$\overline{F}$ = algebraic closure of F in E is the field consisting of all $\alpha \in E$ s.t. α is alg. over F.

- F is algebraically closed ($F = \overline{F}$) if every non-constant polynomial in $F[x]$ has a root in F

Ex) $\overline{\mathbb{Q}}$ = set (field) of algebraic numbers

$\mathbb{C}$ is algebraically closed

Thm | A field F is algebraically closed iff every non-constant poly. factors into linear factors in $F[x]$.

Proof (sketch) Assume alg. closed:

$\forall\, p(x) \in F[x]$, $\deg(p(x)) = n$, have a zero in F

Suppose $\alpha \in F$ is this zero, $p(\alpha) = 0$

$$p(x) = (x-\alpha)\,q_1(x) \qquad \deg(q_1(x)) = \deg(p) - 1$$

now repeat for $q_1(x) \in F[x]$

this gives a linear factorization.

Converseley, if we have a linear factorization for any poly, then the roots must be in F. ∎

Cor | An algebraically closed field F has no proper algebraic extension E.

Thm | Every field F has a unique algebraic closure (upto isomorphism).

Thm | (Fundamental thm. of Alg) $\mathbb{C}$ is algebraically closed.

Splitting Fields

Q: Over what (smallest) extension field may we factor $p(x) \in F[x]$ into linear factors?

Def:
Let F be a field, $p(x) \in F[x]$, $\deg(p) = n \geq 1$

An extension field E of F is a splitting field of $p(x)$ if $\exists$ $\alpha_1, \dots, \alpha_n \in E$ s.t. $E = F(\alpha_1, \dots, \alpha_n)$ and

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

- $p(x) \in F[x]$ splits in E if it is the product of linear factors in $E[x]$.

Ex

$$p(x) = x^4 + 2x^2 - 8 \in \mathbb{Q}[x]$$
$$= (x^2-2)(x^2+4)$$

splitting field of $p(x) = \mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(-\sqrt{2}, \sqrt{2}, -2i, 2i)$

$$p(x) = (x-\sqrt{2})(x+\sqrt{2})(x-2i)(x+2i)$$

Q: Are splitting fields unique?

A: Yes, upto isomorphisms of F

Lemma: Let $\phi : E \xrightarrow{\sim} F$ (isomorphism, fields), ϕ is a isomorphism, $E \subseteq K$, K an extension field of E, $\alpha \in K$ alg. over F with min. poly $p(x)$, $F \subseteq L$, β is a root of $\phi(p(x))$. Then ϕ Extends to a unique isomorphism $\overline{\phi} : E(\alpha) \to F(\beta)$ s.t. $\overline{\phi}(\alpha) = \beta$

and $\overline{\phi}(E) = \phi(E)$

↑ Same as ϕ on E.

Proof sketch

Idea: $\phi : E \xrightarrow{\sim} F$ ← isomorphism

gives an isomorphism

$$\phi : E[x] \to F[x]$$

$$a_0 + a_1 x + \cdots + a_n x^n \longmapsto \phi(a_0) + \phi(a_1)x + \cdots + \phi(a_n)x^n$$

induces an isomorphism $E(\alpha) \to F(\beta)$ — min. poly. of α over E.

where min. poly of β over $F = q(x) = \phi(p(x))$

$$\begin{tikzcd}
E[x]/\langle p(x)\rangle \arrow[rr, leftrightarrow, "\psi", "\sim"', "\phi(\langle p(x)\rangle) = \langle q(x)\rangle"' yshift=-12pt] \arrow[d, leftrightarrow, "\sigma"', "\wr"] & & F[x]/\langle q(x)\rangle \arrow[d, leftrightarrow, "\wr"', "\tau"] \\
E(\alpha) \arrow[rr, leftrightarrow, "\overline{\phi}", "\sim"'] \arrow[d] & & F(\beta) \arrow[d] \\
E \arrow[rr, leftrightarrow, "\phi", "\sim"'] & & F
\end{tikzcd}$$

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} \longmapsto \phi(a_0) + \cdots + \phi(a_{n-1})\beta^{n-1}$$

∎

Thm $\phi : E \to F$ is an isomorphism of fields, $p(x) \in E[x]$ non-constant, $q(x) = \phi(p(x))$. If K is a splitting field of $p(x)$ and L is a splitting field of $q(x)$

then ϕ extends to an isomorphism $\psi: K \to L$.

Cor| Let $p(x) \in F[x]$. Then there exists a unique (upto isomorphism) splitting field of $p(x)$.

Ex| $x^2 - 4 = (x+2)(x-2) \Rightarrow$ splitting field is $\mathbb{Q}$

$x^2 + 4 \Rightarrow$ Splitting field $\mathbb{Q}(i) = \mathbb{Q}(2i, -2i)$

$\| $

$(x+2i)(x-2i)$

$x^2 + 2 \Rightarrow$ Splitting field is $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(-i\sqrt{2}, i\sqrt{2})$

$\|$

$(x - i\sqrt{2})(x + i\sqrt{2})$

Structure of a finite field

Prop| If F is a finite field $\Rightarrow$ char$(F) = p$, p prime

Proof: If Char$(F) = n$, n composite

then $n = ij$

$\alpha = \underbrace{1 + \cdots + 1}_{i \text{ times}}$ and $\beta = \underbrace{1 + \cdots + 1}_{j \text{ times}}$ are in F

Check $\alpha \cdot \beta = 0$

※

running assumption p = prime.

• $\mathbb{Z}/p\mathbb{Z}$ is a finite field of charcteristic p

what about $|F| = n$ where $p \mid n$

i.e $|F| = p^m$?

Prop | If F is a finite field ($\text{char}(F) = p$), then $|F| = p^n$ for some $n \in \mathbb{N}$

Proof: Define a ring hom by

$$\phi : \mathbb{Z} \longrightarrow F$$
$$n \longmapsto n \cdot 1 = \underbrace{1 + 1 + \cdots + 1}_{n \text{ times}}$$

$\text{Char}(F) = p \quad \therefore \quad \ker(\phi) = p\mathbb{Z}$

$\therefore$ by 1st iso. theorem

$$\phi(\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z}$$

this is a sub field of F

Let $K = \phi(\mathbb{Z})$, Since F is a finite field

$\Rightarrow$ finite extension of K.

$\therefore$ F is a finite dimensional vector space over K, say $\dim_K(F) = n$

i.e. $[F : K] = n$

$\therefore \exists$ a basis of F, say $\alpha_1, \ldots, \alpha_n \in F$

$\therefore$ for any $\alpha \in F$

$$\alpha = a_1 \alpha_1 + \cdots + a_n \alpha_n \quad , a_i \in K$$

But $|K| = p$ $\therefore$ are exactly p choices for each a_i

$\therefore \exists$ p^n linear combinations of α_i's

$\therefore |F| = p^n$ ■

Lemma Let p be prime, D an integral domain char$(D) = p$. Then

$$(a+b)^{p^n} = a^{p^n} + b^{p^n} \qquad \forall n \in \mathbb{N}, a, b \in D$$

Proof: induction, Binomial formula. ■

Def Let F be a field, $f(x) \in F[x]$, $\deg(f) = n$ is **seprable** if it has n distinct roots in the splitting field of $f(x)$

- An extension E of F is a seprable extension of F if every element in E is a root of a seperable polynomial in $F[x]$.

Ex $x^2 - 2$ is seprable over $\mathbb{Q}$

$$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$$

$\mathbb{Q}(\sqrt{2})$ is in fact a seperable extension:

all $\alpha \in \mathbb{Q}(\sqrt{2})$ are of the form

$$\alpha = a + b\sqrt{2} \quad , a, b \in \mathbb{Q}$$

- $b = 0 \Rightarrow \alpha$ is a root of $x - a$, which is seprable
- $b \neq 0 \Rightarrow \alpha$ is a root of

$$x^2 - 2ax + a^2 - 2b^2 = (x - (a + b\sqrt{2}))(x - (a - b\sqrt{2}))$$

Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in F[x]$

Def/ The derivative of $f(x)$ is

$$f'(x) = a_1 + 2a_2 + \cdots + n a_n x^{n-1}$$

Lemma/ $f(x)$ is seprable iff

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

Proof: write $f(x)$ in facted form in splitting field, take the derivative, check gcd. $\blacksquare$

Thm/ For every prime p, every $n \in \mathbb{N}$ $\exists$ a finite field F with p^n elements; and any such F is isomorphic to the splitting field of $f(x) = x^{p^n} - x$ over $\mathbb{Z}_p$.

Proof: Let F = splitting field of $f(x) = x^{p^n} - x$

$$f'(x) = p^n x^{p^n - 1} - 1 = -1$$

$\therefore \gcd(f(x), f'(x)) = 1 \quad \therefore f$ is a seperable polynomial

$\therefore$ f has p^n distinct roots,

show that F = roots of $f(x)$

first show roots of $f(x) = x^{p^n} - x$ form a subfield of F.

Check that $0, 1, \alpha+\beta, -\alpha, \alpha\beta, \alpha^{-1}$ are roots of $f(x)$ for any roots α, β of $f(x)$.

$$(\alpha+\beta)^{p^n} - (\alpha+\beta) = \alpha^{p^n} + \beta^{p^n} - \alpha - \beta$$
$$= 0 \quad \therefore \alpha+\beta \text{ is a root.}$$

$\therefore$ the set of roots of $f(x)$ form a subfield of F and $f(x)$ splits in this subfield $\therefore$ the set of roots is the splitting field of $x^{p^n} - x$.

$\therefore$ Always exists a finite field with p^n elements

uniqness (upto iso)

multiplicitive group of non-zero elements of E.

Suppose E is a field, $|E| = p^n$, $\Rightarrow |E^*| = p^n - 1$

$$\therefore \forall \alpha \neq 0 \in E \qquad \alpha^{p^n - 1} = 1$$

$$\therefore \forall \alpha \neq 0 \in E \qquad \alpha^{p^n} - \alpha = 0$$

$\therefore$ E has all roots of $f(x)$

$\therefore$ Since splitting fields are unique

$\Rightarrow E \simeq$ splitting field of $f(x)$.

Defl Galois field of order p^n = unique finite field with p^n

$\shortparallel$

$GF(p^n)$ = splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$

Thm/ Every subfield of $GF(p^n)$ has p^m elements where $m \mid n$. Conversely if $m \mid n$ $\exists$ a unique subfield of $GF(p^n)$ isomorphic to $GF(p^m)$

Proof:

F a subfield of $E = GF(p^n)$

$\Rightarrow$ F is an extension of $K \cong \mathbb{Z}_p$

$\Rightarrow$ F contains p^m elements for some $m \leq n$

$K \subseteq F \subseteq E$

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

$n = [E:F]\, m$

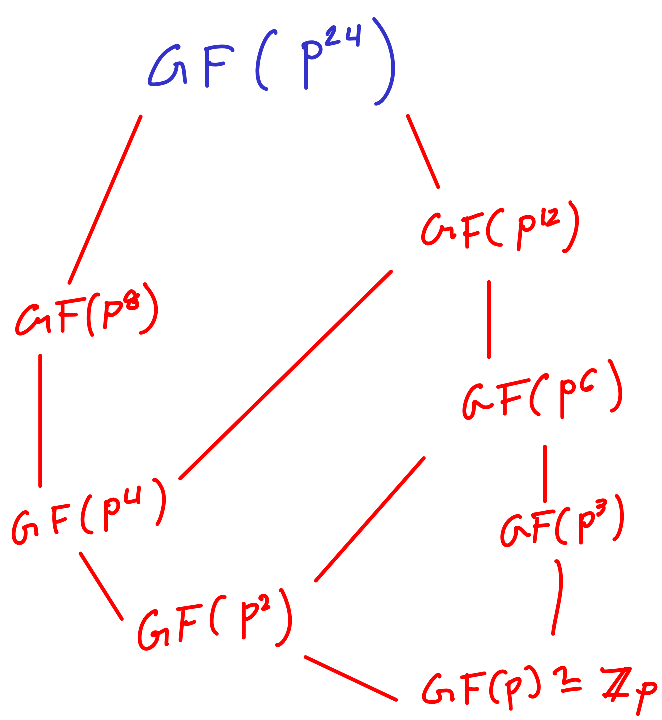
There was a typo here in the notes. (Fixed now).

point: [E:K]=n since we know that E is a dimension n K-vector space from our earlier proof that constructed E as an extension field of Z/pZ.

$\Rightarrow$ $m \mid n$ since $[E:F]$ is an integer

Converse exercise ∎

Ex|



For each field F we have a multiplicative group of non-zero elements F^*.

Thm If G is a finite subgroup of F^* (for any F) then G is cyclic.

Cor F^* is cyclic whenever F is a finite field.

Cor Every finite extension E of a finite field F is a simple extension

proof: Let α generate E^* $\Rightarrow$ $E = F(\alpha)$ ⊠

End of material for final

Field Automorphisms

- want to establish a link between field theory and group theory
- use automorphisms of fields = isomorphisms $F \to F$.

proposition The set of all automorphisms of a field F is a group under composition of functions.

proof: τ, σ auto. of F $\Rightarrow$ $\sigma\tau$, σ^{-1} are automorphisms as well, and id-map is an automorphism ⊠

Prop/ Let E be a field extension of F. Then the set of all automorphisms of E that fix all elements of F, i.e. the set $\sigma : E \to E$ s.t

$\sigma(\alpha) = \alpha \quad \forall \alpha \in F$

are a subgroup, denoted $G(E/F)$, of $Aut(E)$ = group of Automorphisms of E.

Proof: need only show $G(E/F)$ is a subgroup of $Aut(E)$

If $\sigma, \tau \in G(E/F)$

$$\Rightarrow \sigma\tau(\alpha) = \sigma(\alpha) = \alpha \quad \forall \alpha \in F$$

and $\sigma^{-1}(\alpha) = \alpha$, $id \in G(E/F)$ $\blacksquare$

Def: The Galois group of E over F is

$$G(E/F) = \{ \sigma \in Aut(E) \mid \sigma(\alpha) = \alpha \quad \forall \alpha \in F \}$$