Extension Fields

- $F \subseteq E$ field extension
- $a \in E$ algebraic / F and look at $F[a]$, the extension of F by a.

Theorem: $F[a]$ is also a field extension of F.

Proof: Need to show $F[a] = \{f(a) \mid f(x) \in F[x]\}$ is a field.

Remember $F[a] = \operatorname{img}(\phi_a)$ for $\phi_a : F[x] \to E$

So $F[a]$ is a subring of E..

Need to show $F[a]$ has multiplicative inverses.

Given $\alpha \in F[a]$, NTS $\exists\ \beta \in F[a]$

$$\alpha\beta = \beta\alpha = 1 .$$

I know $\exists\ f(x) \in F[x]$ with $\alpha = f(a)$.

Consider the minimal polynomial $p_a(x)$ of a.

By the euclidean algorithm, find polynomials $u(x), v(x) \in F[x]$ such that

$$u(x) f(x) + v(x) p_a(x) = \gcd(f(x), p_a(x))$$

Prove this in a bit!

Super cool property of $p_a(x)$: if $g(x) \mid p_a(x)$ then either $g(x) = c\,p_a(x)$ or $g(x) = c$ for some $c \in F$.

Two cases:
(I) $\gcd(f(x), p_a(x)) = 1$
(II) $\gcd(f(x), p_a(x)) = p_a(x)$

In case (II): this means $p_a(x) \mid f(x) \Rightarrow$

$$f(x) \in \langle p_a(x) \rangle \Rightarrow f(a) = 0 \Rightarrow \alpha = 0$$

In case (I): $\gcd(f(x), p_a(x)) = 1$

$$u(x) f(x) + v(x) p_a(x) = 1$$

$$u(a) f(a) + v(a) \cancel{p_a(a)} = 1$$

$$u(a)\, \alpha = 1$$

$\beta = u(a)$ is the inverse of α! $\square$

<u>Lemma</u>: If $g(x) \in F[x]$ divides $p_a(x)$, then

$$g(x) = c \quad \text{or} \quad g(x) = c\,p_a(x).$$

<u>Proof</u>:

Since $g(x) \mid p_a(x)$, $p_a(x) = g(x)\, h(x)$ for some $h(x) \in F[x]$.

$$0 = p_a(a) = g(a)\, h(a) \Rightarrow g(a) = 0 \quad \text{or} \quad h(a) = 0$$

Now $\deg(g(x)) \leq \deg(p_a)$ so if $g(a) = 0$,

then $\cancel{g(x) = 0}$ or $g(x) = c\,p_a(x)$.

Likewise $\deg(h(x)) \leq \deg(p_a(x))$, so if $h(a) = 0$, then $h(x) = c\,p_a(x)$.

Either $g(x) = \text{const} \cdot p_a(x)$ or $h(x) = \text{const} \cdot p_a(x)$

and since $p_a(x) = g(x)h(x)$, the opposite will have to be a constant. $g_a(x) = c$.

$\square$

Key idea: $F[a]$ is a field as long as a is algebraic / F.

Picture that we are going for:

to understand this

$$\begin{tikzcd}[row sep=large] \mathbb{C} \arrow[d, no head] \arrow[dr, no head] & \\ {} & \mathbb{Q}[\sqrt{2}] \arrow[dl, no head] \\ \mathbb{Q} & \end{tikzcd}$$

explore/understand this.

$$\begin{tikzcd} & \mathbb{Q}[\sqrt{2}][i] = \mathbb{Q}[\sqrt{2}, i] \arrow[dl, no head] \arrow[dr, no head] & \\ \mathbb{Q}[i] \arrow[dr, no head] & & \mathbb{Q}[\sqrt{2}] \arrow[dl, no head] \\ & \mathbb{Q} & \end{tikzcd}$$

Luis: What does $\mathbb{Q}[\sqrt{2}][i]$ look like?

$$\begin{aligned} \mathbb{Q}[\sqrt{2}][i] &= \{ f(i) \mid f(x) \in \mathbb{Q}[\sqrt{2}][x] \} \\ &= \{ f(i, \sqrt{2}) \mid f(x,y) \in \mathbb{Q}[x,y] \} \\ &= \{ a + bi + c\sqrt{2} + di\sqrt{2} \mid a,b,c,d \in \mathbb{Q} \} \end{aligned}$$

Brian's aside: $\mathbb{Q} \times \mathbb{Q} = \{ (a,b) \mid a, b \in \mathbb{Q} \}$

$$(1,0) \cdot (0,1) = (0,0)$$

def not a field

Quest: What does $F[\alpha]$ look like really?

Ex: $$\boxed{\mathbb{Q}[\sqrt{2}] = \{f(\sqrt{2}) \mid f(x) \in \mathbb{Q}[x]\}} \quad \star$$

$f(x) = a_0 + a_1 x + \dots + a_n x^n$

$$= \{a_0 + a_1\sqrt{2} + a_2(\sqrt{2})^2 + \dots + a_n(\sqrt{2})^n \mid n \geq 0 \text{ integer}, \ a_0, \dots, a_n \in \mathbb{Q}\}$$

redundant

$$= \{a_0 + a_1\sqrt{2} \mid a_0, a_1 \in \mathbb{Q}\}$$

$$= \operatorname{span}_{\mathbb{Q}}\{1, \sqrt{2}\}$$

Ex: $$\mathbb{Q}[\sqrt{2}+\sqrt{3}] = \{f(\sqrt{2}+\sqrt{3}) \mid f(x) \in \mathbb{Q}[x]\}$$

$$= \{a_0 + a_1(\sqrt{2}+\sqrt{3}) + a_2(\sqrt{2}+\sqrt{3})^2 + a_3(\sqrt{2}+\sqrt{3})^3 + a_4(\sqrt{2}+\sqrt{3})^4 + \dots + a_n(\sqrt{2}+\sqrt{3})^n \mid n \geq 0, \ a_0, \dots, a_n \in \mathbb{Q}\}$$

$$= \operatorname{span}_{\mathbb{Q}}\{1, \sqrt{2}+\sqrt{3}, (\sqrt{2}+\sqrt{3})^2, (\sqrt{2}+\sqrt{3})^3, (\sqrt{2}+\sqrt{3})^4, \dots\}$$

$(11\sqrt{2}+9\sqrt{3})(\sqrt{2}+\sqrt{3}) = 22+27+20\sqrt{6}$

$$= \operatorname{span}_{\mathbb{Q}}\{1, \sqrt{2}+\sqrt{3}, \cancel{5}+2\sqrt{6}, 11\sqrt{2}+9\sqrt{3}, \cancel{49}+20\sqrt{6}, \dots\}$$

$$= \operatorname{span}_{\mathbb{Q}}\{1, \sqrt{2}+\sqrt{3}, 2\sqrt{6}, 11\sqrt{2}+9\sqrt{3}, \cancel{20\sqrt{6}}, \dots\}$$

$$= \operatorname{span}_{\mathbb{Q}}\{1, \sqrt{2}+\sqrt{3}, 2\sqrt{6}, 11\sqrt{2}+9\sqrt{3}, \dots\}$$

$$= \operatorname{span}_{\mathbb{Q}}\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\} \longleftarrow$$

$$\therefore \mathbb{Q}[\sqrt{2}+\sqrt{3}] = \{a_0 + a_1\sqrt{2} + a_2\sqrt{3} + a_3\sqrt{6} \mid a_0, a_1, a_2, a_3 \in \mathbb{Q}\}$$

Theorem: If $a \in E$ is algebraic / F,

then $F[a]$ will be a vector space / F

with basis $\{1, a, a^2, \dots, a^{d-1}\}$ where $d = \deg(p_a(x))$.

Thus $\dim(F[a]) = d = \deg(p_a(x))$

Def: The degree of an extension $F[a]$ is the degree of $p_a(x)$.

Ex: $(\sqrt{2} + \sqrt{3})$ is a root of $x^4 - 10x^2 + 1$

Expect $\mathbb{Q}[\sqrt{2}+\sqrt{3}]$ has dimension 4

$$\mathbb{Q}[\sqrt{2}+\sqrt{3}] = \operatorname{span}_{\mathbb{Q}}\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$$

so this makes sense!

Ex: $a = e^{\pi i/3}$, $\quad \mathbb{Q}[a] = ???$

$a^3 = e^{\pi i} = -1 \qquad a^3 + 1 = 0$

a is a root of $x^3 + 1 \longleftarrow$ minimal poly.

$$\mathbb{Q}[a] = \operatorname{span}_{\mathbb{Q}}\{1, a, a^2\}$$

$$= \{c_0 + c_1 a + c_2 a^2 \mid c_0, c_1, c_2 \in \mathbb{Q}\}$$

$$= \boxed{\{c_0 + c_1 e^{\pi i/3} + c_2 e^{2\pi i/3} \mid c_0, c_1, c_2 \in \mathbb{Q}\}}$$