Algebraic Extensions

E extension field of F

$\alpha \in E$ algebraic

$\operatorname{irr}(\alpha, F)$ = minimal poly of α / F

Theorem: $F[x]$ is a PID, a principal ideal domain, ie an integral domain where every ideal is principal

Proof: Division algorithm.

Theorem: Let $\alpha \in E$ be algebraic over F. Then $\operatorname{irr}(\alpha, F)$ divides all polynomials $f(x)$ satisfying $f(\alpha) = 0$.

Proof: $F[x]$ is a PID so

$$\{f(x) \mid f(\alpha) = 0\} = \langle p(x) \rangle \quad \text{for some } p(x) \in F[x]$$

with $\deg p(x) \geq 1$. WLOG, $p(x)$ monic. Then

$$\operatorname{irred}(\alpha, F) = g(x)p(x)$$

and since $\operatorname{irr}(\alpha, F)$ has minimal degree, $\deg g = 0$ and $p(x) = \operatorname{irr}(\alpha, F)$. Thus if $f(\alpha) = 0$, then $\exists\, h(x) \in F[x]$ with

$$f(x) = h(x)p(x) = h(x) \cdot \operatorname{irr}(\alpha, F).$$

Thus $\operatorname{irr}(\alpha, F)$ divides $F[x]$ ☐

Corollary: $\operatorname{irr}(\alpha, F)$ is irreducible.

Theorem: If R is a PID and $r \in R$ is irreducible, then $\langle r \rangle$ is maximal

Proof:

S'pose r is irreducible. Then if $\langle r \rangle \subseteq J$ is an ideal we have that $J = \langle s \rangle$ and since $r \in J$

$r = xs$ for some $x \in R$

Since r is irreducible, x or s is a unit. If x is a unit, $\langle r \rangle = \langle s \rangle$.

If s is a unit, $J = R$

$\square$

Def: Let $\alpha_1, \ldots, \alpha_n \in E$. The smallest subfield of E containing F and $\alpha_1, \ldots, \alpha_n$ is the field obtained by <u>adjoining $\alpha_1, \ldots, \alpha_n$ to F</u>.

Notation: $F(\alpha_1, \ldots, \alpha_n)$

If $E = F(\alpha)$ for some $\alpha \in E$, then E is called a <u>simple extension</u>.

Ex: $E = \mathbb{Q}(\sqrt{2})$ is a simple extension

$E = \mathbb{Q}(\sqrt{2}, \pi)$ is <u>not</u> a simple ext.

Ex: $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ <u>is</u> a simple extension because

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$

Two kinds of simple extensions

- when α is algebraic
- when α is transcendental $\left(F(\alpha) \cong F(x) \right)$

<u>Theorem</u>: If α is algebraic, then

$$F(\alpha) = F[\alpha] := \operatorname{img}(\phi_\alpha) = \{ f(\alpha) \mid f(x) \in F[x] \}$$

where here

$$\phi_\alpha : F[x] \to E$$

is the evaluation homomorphism.

<u>Proof</u>:

$$\operatorname{img}(\phi_\alpha) \cong F[x]/\ker(\phi_\alpha)$$

and $\ker(\phi_\alpha) = \langle \operatorname{irr}(\alpha, F) \rangle$ is maximal so $\operatorname{img}(\phi_\alpha)$ is a field.

If $F \subseteq K \subseteq E$ and $\alpha \in E$, then $f(\alpha) \in E$ $\forall$ polynomials $f(x) \in F[x]$. Thus $\operatorname{img}(\phi_\alpha) \subseteq K$ and this shows $\operatorname{img}(\phi_\alpha)$ is the minimal subfield of E containing F and α.

$\square$

<u>Theorem</u>: Let $\alpha \in E$ and $\operatorname{irr}(\alpha, F)$ have degree d.

Then

$$F[\alpha] = \{ a_0 + a_1\alpha + a_2\alpha^2 + a_{d-1}\alpha^{d-1} \mid a_0, \dots, a_d \in F \}$$

and $F[\alpha]$ is d-dimensional $/F$ with basis $1, \alpha, \alpha^2, \dots, \alpha^{d-1}$.

Ex: $\mathbb{Q}[\sqrt{2}] = \{a_0 + a_1\sqrt{2} \mid a_0, a_1 \in \mathbb{Q}\}$

Ex: $\mathbb{Q}[e^{i\pi/3}] = \{a_0 + a_1 e^{i\pi/3} + a_2 e^{2i\pi/3} \mid a_0, a_1, a_2 \in \mathbb{Q}\}$

Ex: $\mathbb{Q}\left[\sqrt{1+\sqrt{3}}\right] = ?$

$$\operatorname{irr}\left(\sqrt{1+\sqrt{3}}, \mathbb{Q}\right) = (x^2-1)^2 - 3 \quad \deg 4$$

$$\mathbb{Q}\left[\sqrt{1+\sqrt{3}}\right] = \left\{a_0 + a_1\sqrt{1+\sqrt{3}} + a_2\left(\sqrt{1+\sqrt{3}}\right)^2 + a_3\left(\sqrt{1+\sqrt{3}}\right)^3 \,\middle|\, a_0, \dots, a_3 \in \mathbb{Q}\right\}$$

Def: An extension E is algebraic if every element of E is algebraic over F.

Theorem: If E is an algebraic extension of F and $\dim_F(E) = d < \infty$, then E is algebraic

Proof:

Let $\beta \in F(\alpha)$. Then consider the F-linear map $T: F(\alpha) \to F(\alpha)$, $T(r) = \alpha r \ \forall r$.

$$T(\alpha^j) = \sum_{k=0}^{d-1} a_{jk}\alpha^k, \quad a_{jk} \in F$$

So if we let $A \in M_d(F)$, $A_{jk} = a_{jk}$

then we have that

the characteristic poly $p(x) = \det(xI - A) \in F[x]$ satisfies $p(A) = 0$ by Cayley–Hamilton. Thus $p(\alpha) = 0$.

$\blacksquare$

Def: The *degree* $[E:F]$ of an extension E of F is the dimension of E as an F-vector space. If $[E:F]<\infty$, E is a *finite extension*.

Corollary: If $\alpha \in E$ is algebraic over F, then $F[\alpha]$ is a finite extension of degree
$$[E:F] = \deg \operatorname{irr}(F,\alpha)$$
In particular, E is an algebraic extension.

Theorem: If E is a finite extension of F and K is a finite extension of E then $[K:F]=[K:E][E:F]$.

Def: The *algebraic closure* of F in E is
$$\overline{F}_E = \{\alpha \in E \mid \alpha \text{ is algebraic over } F\}$$
A field F is *algebraically closed* if every polynomial $f(x)\in F[x]$ has a root in F.
A field extension $\overline{F}$ of F which is algebraic and algebraically closed is called an *algebraic closure* of F.

Lemma: $\overline{F}_E$ is a field

Ex: $\overline{\mathbb{Q}}_{\mathbb{C}} = \overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$.

Note: $\overline{\mathbb{Q}}$ is countable, so $\overline{\mathbb{Q}} \neq \mathbb{C}$!