Field Automorphisms §48.

Recall A field isomorphism is a bijective map

$\varphi : E \to E'$ s.t. $\varphi(a+b) = \varphi(a) + \varphi(b)$ $\forall\, a, b \in E$.
$\varphi(ab) = \varphi(a)\varphi(b)$

A field automorphism is an iso $\varphi : E \to E$.

Today: 1) Conjugate isomorphisms $\psi_{\alpha,\beta} : F(\alpha) \to F(\beta)$

2) Fixed fields and automorphism groups

3) Frobenius automorphisms $\sigma_p : E \to E$ for finite field E $\mathrm{char}(E) = p$.

Conjugation isomorphism

Example $\varphi : \mathbb{C} \longrightarrow \mathbb{C}$ ← conju. autom. $\varphi(z) = \bar{z}$ $\quad \varphi(a+ib) = a-ib$

Notice $\varphi(zw) = \overline{zw} = \bar{z}\,\bar{w} = \varphi(z)\varphi(w)$ $\Longrightarrow$ φ is an automorphism of $\mathbb{C}$.

$\varphi(z+w) = \overline{z+w} = \bar{z} + \bar{w} = \varphi(z) + \varphi(w)$

Def 48.1 Let E be alg. ext. of F. Then $\alpha, \beta \in E$ are conjugate over F if $\operatorname{irr}(\alpha, F) = \operatorname{irr}(\beta, F)$.

Ex $F \le E$, $F = \mathbb{R}$, $E = \mathbb{C}$ $\quad \operatorname{irr}(i, \mathbb{R}) = \operatorname{irr}(-i, \mathbb{R}) = x^2+1$

Hence $i, -i$ are conjugate / $\mathbb{R}$.

Exercise Show $a+ib$ and $a-ib$ have same irred poly over $\mathbb{R}$ $\forall\, a, b \in \mathbb{R}$.

Hint: $(x-(a+ib))(x-(a-ib))$

Ex2 If $F = \overline{F}$ then $\operatorname{irr}(\alpha, F) = x - \alpha$

$\neq \operatorname{irr}(\beta, F) = x - \beta$

if $\alpha \neq \beta$

No distinct conjugate elements.

Thm 48.3 Let F be a field and α, β be alg over F with $\deg(\alpha, F) = n$. The map

$$\psi_{\alpha,\beta} : F(\alpha) \longrightarrow F(\beta)$$

$$\psi_{\alpha,\beta}(c_0 + c_1\alpha + \dots + c_{n-1}\alpha^{n-1}) = c_0 + c_1\beta + \dots + c_{n-1}\beta^{n-1}$$

is a field isom if and only if α, β are conjugate over F.

Proof Suppose $\psi_{\alpha,\beta}$ is an iso and $\operatorname{irr}(\alpha, F) = a_0 + a_1x + \dots + x^n$

$0 = \psi_{\alpha,\beta}(a_0 + a_1\alpha + \dots + \alpha^n) = a_0 + a_1\beta + \dots + \beta^n \Rightarrow \beta$ is a zero of $\operatorname{irr}(\alpha, F)$ and $\operatorname{irr}(\alpha, F)$ divides $\operatorname{irr}(\beta, F)$ over F.

Since $\psi_{\alpha,\beta}: F(\alpha) \to F(\beta)$ is a field isomorphism it is also a iso of vector spaces over F

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

$\operatorname{irr}(\alpha, F) = \operatorname{irr}(\beta, F)$ and α, β are conjugate.

Conversely, $\operatorname{Irr}(\alpha, F) = \operatorname{Irr}(\beta, F) = p(x)$ then

$$\begin{array}{ccccc} F(\alpha) & \xleftarrow[\cong]{\psi_\alpha} & F[x]/\langle p(x)\rangle & \xrightarrow[\cong]{\psi_\beta} & F(\beta). \\ \alpha & \longleftrightarrow & x + \langle p(x)\rangle & \longmapsto & \beta \end{array}$$

So $F(\alpha), F(\beta) \cong F[x]/\langle p(x)\rangle$ moreover,

$\psi_\beta \circ \psi_\alpha^{-1} = \psi_{\alpha,\beta}$ so $\psi_{\alpha,\beta}$ is an isom. $\square$

Example $f(x) = x^3 - 2$ is irreducible over $\mathbb{Q}$. $\overline{\mathbb{Q}} \leq \mathbb{C}$.

$f(x)$ has zeros $\underbrace{2^{1/3},\ e^{2\pi i/3}2^{1/3},\ e^{4\pi i/3}2^{1/3}}$.

all 3 have same irr poly over $\mathbb{Q}$ x^3-2

all conjugates.

$\mathbb{Q}(\alpha) \leq \mathbb{C}$ for any of these zeros α.

$$\begin{tikzcd}
 & & \mathbb{C} \arrow[dll, dash] \arrow[ddr, dash] & \\
\mathbb{R} \arrow[d, dash] & & & \\
\mathbb{Q}(2^{1/3}) \arrow[drr, dash] & & & \mathbb{Q}(e^{2\pi i/3}2^{1/3}) \arrow[dl, dash] \\
 & & \mathbb{Q} &
\end{tikzcd}$$

So $\mathbb{Q}(2^{1/3}) \neq \mathbb{Q}(e^{2\pi i/3}2^{1/3})$ as subfields of $\mathbb{C}$.

But $\mathbb{Q}(2^{1/3}) \xrightarrow[\psi_{2^{1/3},\, e^{2\pi i/3}2^{1/3}}]{\cong} \mathbb{Q}(e^{2\pi i/3}2^{1/3})$

Corollary 48.5 Let α be alg. over F. Every isomorphism $\psi : F(\alpha) \to E$ where $E \leq \overline{F}$ with $\psi(a) = a \ \forall a \in F$ maps α to a conjugate β of α over F.

Proof Hint: show $\psi(\alpha) = \beta$ has the same degree of irr poly $/F$ as α.
then show β is a zero of $\operatorname{irr}(\alpha, F)$.

Conversely for every conjugate β of α there exists exactly one isomorphism $\psi_{\alpha,\beta} : F(\alpha) \to E$ which maps $\alpha \mapsto \beta$ and $a \mapsto a$ $a \in F$

Corollary 48.6 Let $f(x) \in \mathbb{R}[x]$. If $f(a+ib) = 0$ $a, b \in \mathbb{R}$ then $f(a-ib) = 0$.

Proof Use part 1 of 48.5 with $\psi : \mathbb{C} \to \mathbb{C}$ complex conj.

$\psi(a) = a$ $a \in \mathbb{R}$. Hence $\psi(a+ib) = a-ib$ is a zero of f.

$$0 = \psi_{i,-i}(f(a+ib)) = \underset{\overset{\shortparallel}{0}}{f(a-ib)}$$

$\square$.

Field automorphisms $\sigma : E \to E$ isomorphism

Def 48.8 Let $\sigma : E \to E$ be an automorphism. An elt $a \in E$ is fixed by σ if $\sigma(a) = a$

Example $\sigma : \mathbb{C} \to \mathbb{C}$ complex conjugation fixes exactly the real numbers.

Thm 48.11 Let S be a collection of automorphisms of E. Then $E_S = \{ a \in E \mid \sigma(a) = a \ \forall \sigma \in S \}$ is a subfield of E. (E_S is the subfield fixed by S)

Proof (see text).

Def 48.12 The field E_σ is the fixed field of an automorphism σ. If S is a collection of automorphisms E_S is the fixed field of S

Thm 48.14 The set of all field automorphisms of E is a group under function composition. $\mathrm{Aut}(E)$.

Proof 1) comp. is associative 2) $id: E \to E \in \mathrm{Aut}(E)$
3) $\psi \in \mathrm{Aut}(E)$ then $\psi^{-1} \in \mathrm{Aut}(E)$

Thm 48.15 If $F \leq E$ then the automorphisms of E fixing F (ie. $a \mapsto a$ $\forall a \in F$) forms a subgp $G(E/F) \leq \mathrm{Aut}(E)$ and

$$F \leq E_{G(E/F)}.$$

Proof (see text).

Example Frobenius automorphism. (finite fields)

Thm 48.19 Let E be a finite field char $F = p$

The map $\sigma_p : E \to E$ defined by

$\sigma_p(a) = a^p \quad \forall \quad a \in E$ is an automorphism

$$E_{\sigma_p} \cong \mathbb{Z}_p = \{ c \cdot 1 \mid 0 \leq c \leq p-1 \}.$$

Proof $a, b \in E$

$$\sigma_p(ab) = (ab)^p = a^p b^p = \sigma_p(a)\,\sigma_p(b)$$

$$\sigma_p(a+b) = (a+b)^p = a^p + \cancel{\binom{p}{1} a^{p-1} b} + \dots + \cancel{\binom{p}{1} a b^{p-1}} + b^p$$

$\mathrm{char}(F) = p.$

$$= a^p + b^p$$

$$= \sigma_p(a) + \sigma_p(b).$$

Hence σ_p is a homomorphism.

claim σ_p is a bijection

if $\sigma_p(a) = 0 \Rightarrow a^p = 0 \Rightarrow a = 0$ hence injective.

Since E is finite $\sigma_p : E \to E$ is a bijection hence automorphism.

If $c \in \mathbb{Z}_p \leq E$ by Fermat's little theorem $c^p = c$. Hence $\sigma_p(c) = c$

$c \in E_{\sigma_p}$

Notice E_{σ_p} has size at most p since it consists of zeros of $X^p - X$. Hence $E_{\sigma_p} = \mathbb{Z}_p$.

$\square$