0.0.1 Splitting Fields

Definition 0.1 *F field, $f(x) \in F[x]$ non-zero, a splitting field of f is a field extension E/F such that $f(x) = \alpha\Pi_i(x - \alpha_i)$, with $\alpha, \alpha_1, \alpha_2, ..., \alpha_n$ and $E = F(\alpha_1, ..., \alpha_n)$*

F field, A, B rings [e.g. $A = F[x]$, $F \to F[X]$]

$$\begin{tikzcd} A \arrow[r, "\phi"] \arrow[d, "i_A"] & B \\ F \arrow[ur, "i_B"] & \end{tikzcd}$$

$Hom_F(A, B) = \{\phi : A \to B \mid i_b = \phi i_A\}$

Proposition 0.2 *$F \to F[x], F \to B$ any ring morphism.*

$Hom_F(F[x], B) \to [\cong]B$

$\phi \mapsto \phi(x)$

Proof: *Given $b \in B$, define $\phi_b : F[x] \to B$ by $\phi(\sum_{n=0}^{m} a_n x^n) = \sum_{n=0}^{m} a_n b^n$*

Check ϕ_b is a ring morphism ■

Cor: Fix $f(x) \in F[X]$, then there is a bijection $Hom_F(\frac{F[x]}{f(x)}, B)$

TODO: Turn scratchwork into proof.

Scratchwork below [Also refer to video]

$$\begin{tikzcd} A \arrow[r, "\bar{\phi}_P"] \arrow[d, "P"] & B \\ A/I \arrow[ur, "\bar{\phi}"] & \end{tikzcd}$$

$\phi(a + I) = \phi(a)$

$a + I = a' + I \implies a - a' \in I$

So $\phi(a) = \phi(a')$

$A = F[x]$

$\downarrow$

$\frac{F[X]}{f} \to B$

Corollary 0.3 *TODO: Write up from notes*

Proof: $f(\alpha) = \frac{F[x]}{(f(x))}$, f min. poly of α ■

Cor: ANy two splitting fields $\frac{E_1}{F}$, and E_2/F of a poly $f(x) \in F[x]$ are F-isomorphic.

Proof: ETS there is an $F-$morphism $\phi : E_1 \to E_2$. Since then $[E_1 : F] \leq [E_2 : F]$ By symmetry there would be a map from E_2 to E_1, so $[E_1 : F] \geq [E_2 : F]$

So ϕ will be an isomorphism.

Let $\alpha_1, ..., \alpha_n$ be the roots in E_1 of f, so $F(\alpha_1, ..., \alpha_n)$.

Assume by induction we ahve $\phi_i : F(\alpha_1, .., \alpha_i) \to E_2$

$F(\alpha_1, ..., \alpha_{i+1}) \supseteq F(\alpha_1, ..., \alpha_i) \to E_2$

Let $g(x)$ be the min poly of α_{i+1} over $F(\alpha_1, ..., \alpha_i)$, then $g|F$. So there exists a root of $g \in E_2$, since F splits there.

User cor. to define ϕ_{i+1} ∎

0.0.2 Computing the degree of a splitting field

1. $f(x) = x^3 - 2$ over $\mathbb{Q}$.

   $E = \mathbb{Q}()$

0.0.3 Lattice of subfields in F_{p^n}

X poset $x \leq y$

1) $X set, P(X) = Y \subset X subset\ X \leq Y \iff Y \subset X$

2) V a vector space/F Subspaces˙F(V) = {W ≤ V}

3) $F \subset K$ fields

Subfields$_F$(K) = $F \subseteq E \subset K, E$ field

For all $m|n \exists! subfieldof \mathbb{F}_{p^n}$ which is isom to $\mathbb{F}_{p^m}$

Example $F_{p^1 2} \supseteq F_{p^6} F_{p^2} F_{p^4} F_{p^3} F_p$

Note:

$F \subset E_1$, $E_2 \subset K$.

$E_1 = E_2 \implies E_1 \cong E_2 \implies [E_1 : F] = [E_2 : F]$

Converse not true, E.g. $\mathbb{Q}[\sqrt{2}], \mathbb{Q}[\sqrt{3}]$

•Look at $x^3 - 2$ over $\mathbb{Q}$ $\sqrt[3]{2}$, $\sqrt[3]{2}\zeta$, $\sqrt[3]{2}\zeta^2 \in C$

$\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}(\sqrt[3]{2}\zeta)$

$\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}[x]/(x^3 - 2) \cong \mathbb{Q}(\sqrt[3]{2}\zeta)$

Fields are isom. but not equal.

$\mathbb{F}_p^m = \{a \in \mathbb{F}_{p^n} | a^{p^m} = a\}$

Roots of $x^{p^n} - x$

Fixed points of $\phi^m = \phi \circ ..\phi(ntimes)$

ϕ frobenius map $Def : E/F, \sigma : E \to E$ F-automomorphism. $(\sigma(a) = a \forall a \in F)$

$E^\sigma = \{a \in E | \sigma(a) = a\}$

Note E^σ is a subfield of E, it contains F.

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

$\sigma(a + b) = \sigma(a) + \sigma(b) = a + b$ $\sigma(ab) = \sigma(a)\sigma(b) = ab$

Def E/F field extension.

$Aut(E/F) = \{\sigma : E \to E | \sigma \text{ auto}\}$

This is a group. id_E, $\sigma, \tau \in Aut(E/F)$ so is $\sigma \circ \tau$.

Claim : $Aut(F_{p^n}) =< \phi >\cong C_n$

Pf: Let f be an irreducible polynomial of degree n.

$\mathbb{F}_p[x]/(f) \cong \mathbb{F}_{p^n}$

So all roots of f are in F_{p^n}

$\alpha \mapsto \alpha_1, ...\alpha_n$ tf at most n automomorphism.