Algebraic Closures

p. 559 #7
p. 556 #8, 10-12

Def $F \subset \bar{F}$, say $\bar{F}$ is an <u>algebraic closure</u> of F if $\bar{F}/F$ is algebraic and every $f(x) \in F[x]$ splits in $\bar{F}$.

Def A field is <u>algebraically closed</u> if every polynomial w/ coefs in that field splits in that field

<u>Question</u> Is $\bar{F}$ algebraically closed?

<u>Thm</u> $\bar{F}$ is alg closed

<u>Proof</u>

<u>Thm</u> Let F be a field. Then $\exists$ an algebraic closure $\bar{F}$ which is unique up to $\cong$.

<u>Proofs</u> Various proofs, all use Zorn's Lemma. For example take all alg extensions partially ordered under inclusion.

<u>Fundamental Theorem of algebra</u> $\mathbb{C}$ is alg closed $(= \bar{\mathbb{R}})$

<u>Rmk</u> $\bar{\mathbb{Q}} \subsetneq \mathbb{C}$

SEPARABLE & INSEPARABLE EXTENSIONS

Def. $f(x) \in F[x]$ is <u>separable</u> of deg n if $f(x)$ has n-distinct roots in a splitting field
Otherwise inseparable.

Examples

1. x^3-2 is separable

2. Let $F = \mathbb{F}_2(t)$ Let $f(x) = x^2 - t$ irreducible.

   SF is $F(\sqrt{t})$ and $x^2-t = (x-\sqrt{t})^2$ so inseparable.

Def. Let K/F and $\alpha \in K$ algebraic $/F$. Say α is <u>separable over F</u> if its minimal polynomial is.
Say K/F is a <u>separable Extension</u> if all elements of K are algebraic and separable.

Thm $f(x)$ is separable $\longleftrightarrow$ $\gcd(f(x), f'(x)) = 1$.

Rmk $f'(x)$ is purely formal

Proof.

COR Every irreducible poly is separable in a field of characteristic zero.

Proof degree $f'(x) = n-1$

<u>Example</u>

1. $f(x)=x^2+t$ in $\mathbb{F}_2(t)$, $f'(x)=0$ so inseparable

2. $f(x)=x^n-1$ is separable over any field of char $\nmid n$.

<u>Prop</u> Suppose char $F=p$. Then $\forall\, \alpha,\beta\in F$ $(\alpha+\beta)^p=\alpha^p+\beta^p$
$(\alpha\beta)^p=\alpha^p\beta^p$

Thus $\varphi(x)=x^p$ gives a field homomorphism from $F\to F$ (which of course is 1-1). Called Frobenius endomorphism.

<u>Cor</u> In a finite field of char p every element is a p^{th} power.

<u>Thm</u> Every irreducible polynomial over a finite field is separable. More generally, a polynomial is separable $\leftrightarrow$ product of distinct irreducible.

<u>Proof</u> Suppose $p(x)$ is irreducible and inseparable. We must have $p'(x)=0$ so $p(x)=a_0+a_1x^p+a_2x^{p^2}+\dots+a_nx^{p^n}$

~~Let $q(x)=a_0+a_1x+\dots+a_nx^n$ so $p(x)=q(x^p)$~~

Let $a_i=b_i^p$ by Cor above. Then

$$p(x)=b_0^p+(b_1x)^p+\dots+(b_nx^n)^p$$
$$=(b_0+b_1x+\dots+b_nx^n)^p \quad ⨳$$

Def A field is <u>perfect</u> if it has char 0 or if it has char p and the Frobenius map is onto.

Thm F is perfect $\leftrightarrow$ Every irreducible poly is separable

Classification of Finite Fields

Let $\mathbb{F}_p$ = field of p elts. Let $f(x) = x^{p^n} - x$. Then $f'(x) = -1$ so $f(x)$ is separable. Thus $f(x)$ has p^n distinct roots in a splitting field.

<u>Lemma</u> α, β roots, so are $\alpha\beta$, $\alpha+\beta$, α^{-1}.

<u>COR</u> Splitting field has exactly p^n elements

<u>Rmk</u> Any field on p^n elts is all roots

<u>Thm</u> For each p^n there is a unique field with p^n elements up to $\cong$. Namely, the splitting field of $x^{p^n} - x$.

<u>Rmk</u> All lie in $\overline{\mathbb{F}_p}$.

Inseparable Irreducibles

Rmk Assume $p(x)$ irred, insep. Then char $F=p$ and $p'(x)=0$. Thus $p(x)=p_1(x^p)$. Is p_1 sep? If not, then $p_1=p_2(x^p)$ so $p=p_2(x^{p^2})$ etc..

Def Let $p(x)$ be irred poly / F of char p. Then $\exists!\ k\geq 0$ and unique separable polynomial $p_{sep}(x)$ such that

$$p(x)=p_{sep}(x^{p^k}).$$

Degree of $p_{sep}(x)$ is the separable degree $\deg_s p(x)$. Integer p^k is inseparable degree $\deg_i p(x)$.

Rmk $\deg p(x)=\deg_s p(x)\deg_i p(x)$.

Ex $p(x)=x^2-t$ / $\mathbb{F}_2(t)$.

$p_{sep}(x)=x-t$, insep degree is 2.

Thm (later) Let E/F alg. Then $\exists!\ E_{sep}$ with

$$F\subseteq E_{sep}\subseteq E \quad \text{so } E_{sep}/F \text{ separable},$$

E/E_{sep} purely inseparable