Separable extensions continued   Section 51

Def 51.12 A field is <u>perfect</u> if every finite extension is a separable extension.
$[E:F] < \infty$

E separable over F if $\{E:F\} = [E:F]$

Recall For all finite ext'ns $|G(E/F)| \leq \{E:F\} \leq [E:F]$

Thm 51.13 Every field of characteristic 0 is perfect
(ie: every E finite ext'n of F has $\{E:F\} = [E:F]$ when char $F = 0$)

Thm 51.14 Every finite field is perfect.

Recall We reduced both proofs to the case of simple ext'ns $E = F(\alpha)$ for $\alpha \in \overline{F}$. Moreover $F(\alpha)$ is separable $\iff$ $\forall$ zeros of $\mathrm{irr}(\alpha, F)$ have multiplicity one.

Goal: Show $f(x) \in F[x]$ irreducible over F has zeros of mult 1 for $|F| < \infty$ or $\mathrm{char}(F) = 0$.

Thm 51.2 Let $f(x) \in F[x]$ be irreducible. Then all zeros of $f(x)$ have the same multiplicity.

Proof Let α, β be zeros of $f(x)$ $\psi_{\alpha,\beta} : F(\alpha) \to F(\beta)$ conj. iso.

$\psi_{\alpha,\beta}$ fixes F and also extends to $\tau : \overline{F} \to \overline{F}$;

and $\tau_x : \overline{F}[x] \to \overline{F}[x]$ $\tau_x\left(\sum a_i x^i\right) = \sum \tau(a_i) x^i$

So $\tau_x(f(x)) = \sum \tau(a_i)x^i = \sum a_i x^i = f(x)$.
since $a_i \in F$ $\quad f(x) \in F[x]$

get $\tau_x((x-\alpha)^{\nu_\alpha}) = (x-\beta)^{\nu_\alpha}$.

So $f(x) = (x-\alpha)^{\nu_\alpha}(x-\beta)^{\nu_\beta}\prod(x-\alpha_i)^{\nu_{\alpha_i}}$ $\quad \alpha, \beta, \alpha_i$ distinct

$$\begin{array}{c} \| \\ \tau(f(x)) \end{array} = (x-\beta)^{\nu_\alpha}(x-\tau(\beta))^{\nu_\beta}\prod(x-\tau(\alpha_i))^{\nu_{\alpha_i}}$$

$\tau(\beta), \tau(\alpha_i) \neq \beta$ since τ is injective and $\tau(\alpha) = \beta$

so the multiplicity of the zero β is $\nu_\alpha = \nu_\beta$.

Therefore α, β have the same multiplicity as zeros of $f(x)$ $\square$.

<u>Corollary</u>/Thm 51.6 $F \leq E$ and $[E:F] < \infty$ then $\{E:F\}$ divides $[E:F]$.

Proof idea. Show it for simple ext'ns $F(\alpha) = E$.

$[E:F] = \deg \operatorname{irr}(\alpha, F)$.

$\operatorname{irr}(\alpha, F) = f(x) = \left(\prod_{i=1}^{\deg f / \nu} (x - \alpha_i) \right)^{\nu}$

$\alpha_i \in \overline{F} \quad \nu \in \mathbb{Z}_{>0}$

$\{E:F\} =$ # conjugates of α over F

$= \dfrac{\deg \operatorname{irr}(\alpha, F)}{\nu}$ ← multiplicity of all roots of $f(x)$.

$\{E:F\} \cdot \nu = [E:F]$.

For $E = F(\alpha_1, \dots, \alpha_k)$ apply above arg recursively and use product formulas for $[E:F]$ + $\{E:F\}$.

Lemma 51.11 Let $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 \in \overline{F}[x]$

If $(f(x))^m \in F[x]$ and $m \cdot 1 \neq 0$ in F then $f(x) \in F[x]$ ie $a_i \in F$ for all i,

Proof By induction on r show $a_{n-r} \in F$.

$\underline{r=1}$ $(f(x))^m = x^{mn} + (m \cdot 1) a_{n-1} x^{mn-1} + \dots \in F[x]$.

$\Rightarrow (m \cdot 1) a_{n-1} \in F$ $\quad$ $m \cdot 1 \neq 0$ divide by it and stay in F.

$\Rightarrow a_{n-1} \in F$

Inductive step (assume $a_{n-1}, \ldots, a_{n-r} \in F$)

coeff of x^{mn-r+1} in $(f(x))^m$ $= (m\cdot 1)a_{n-(r+1)} + \overbrace{g_{r+1}(a_{n-1}, \ldots, a_{n-r})}^{\in F} \in F$

where g_{r+1} is a polynomial with coefficients in F.

again we obtain $a_{n-(r+1)} \in F$ by dividing by $\underset{\neq 0}{(m\cdot 1)}$

$\Rightarrow \quad f(x) \in F[x]$

Thm 51.13 Every field of characteristic 0 is perfect

Proof Suffices to show $\forall\ \alpha \in \overline{F}$ $irr(\alpha, F)$ has distinct zeros. Let $f(x)$ be irreducible over F.

Let $f(x) = \left(\prod (x-\alpha_i)\right)^{v}$ where $\alpha_i \in \overline{F}$ and v is the common mult. of all zeros of $f(x)$.

In fact,
$g(x) = \prod(x-\alpha_i) \in F[x]$ by previous lemma since

$g(x)^{v} = f(x) \in F[x]$ and $v \cdot 1 \neq 0$ since $\operatorname{char} F = 0$.

So $f(x)$ is irreducible $\Rightarrow$ v must be 1. Hence all zeros of $f(x)$ are mult 1 (all distinct) $\square$.

Thm 51.14 Every finite field is perfect.

Proof Again suffices to show zeros of irred poly's have mult 1. Suppose $f(x) \in F[x]$ is irred

Suppose $|F| < \infty$ and char $F = p$.

$\alpha_i \in \overline{F}$ α_i distinct.

$$f(x) = \left(\prod (x - \alpha_i) \right)^{v}$$

we can factor $v = p^t e$ where $p \nmid e$

$$= \left[\left(\prod (x - \alpha_i) \right)^{p^t} \right]^{e} \in F[x]$$

$\Rightarrow e \cdot 1 \neq 0$ in F.

By Lemma 51.11 $\Rightarrow \left(\prod (x - \alpha_i) \right)^{p^t} \in F[x]$ and divides $f(x)$ $\Rightarrow e = 1$

$\mathbb{Z}_p(y) \leftarrow$ field (field of fractions of $\mathbb{Z}_p[y]$)

$\cup\!|$

$\mathbb{Z}_p[y]$ polynomial ring $\ni \sum^n a_i y^i$

$\not\ni \frac{1}{y}$

$\mathbb{Z}_p(y)$ infinite field extension.

$|$

$\mathbb{Z}_p$

We reduced to considering $\quad F(x) = \left[\prod (x-\alpha_i)\right]^{p^t}$

$$= \prod \left(x^{p^t} - \alpha_i^{p^t}\right)$$

let $g(x) = \prod (x - \alpha_i^{p^t}) \leftarrow$ separable over F and has distinct zeros $\{\alpha_1^{p^t}, \ldots, \alpha_d^{p^t}\}$.
$\qquad \alpha_1^{p^t} = \alpha^{p^t}$

(Notice $g(x^{p^t}) = f(x)$)

This means that $F(\alpha^{p^t})$ is a separable field extension of finite degree over F. Hence $|F(\alpha^{p^t})| < \infty$ and $\operatorname{char}(F(\alpha^{p^t})) = p$

$$\left[\begin{array}{c} F(\alpha) \\ | \\ F(\alpha^{p^t}) \\ | \\ F \end{array}\right]$$

finite ext'n since α is a zero of $x^{p^t} - \alpha^{p^t} \in F(\alpha^{p^t})[x]$

Goal: is to show $F(\alpha) = F(\alpha^{p^t})$

hence $p^t = 1$.

Consider Frobenius automorphism $\sigma_p : F(\alpha^{p^t}) \to F(\alpha^{p^t})$

$\sigma_p(a) = a^p$ $\qquad \sigma_p^t(a) = a^{p^t}$ $\qquad \sigma_p^t$ also automorphism

So $\exists$ $\beta \in F(\alpha^{p^t})$ s.t. $\sigma_p^t(\beta) = \alpha^{p^t}$

So β is a zero of $x^{p^t} - \alpha^{p^t} = (x-\alpha)^{p^t}$

The only zero of $x^{p^t} - \alpha^{p^t}$ is α so $\alpha = \beta$

Hence $F(\alpha) = F(\alpha^{p^t}) \Rightarrow p^t = 1 \Rightarrow v = p^t \cdot e = 1$ hence $F(\alpha)$ separable $\square$

Thm 51.15 The primitive elt thm.

A finite separable ext'n of F is simple.

(i.e. E finite separable extension of F then $E = F(\underbrace{\alpha) \text{ for some } \alpha \in E}_{\text{primitive element}}$.)

Example $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ is separable since $\mathbb{Q}$ is perfect, so $\exists\ \alpha \in \overline{\mathbb{Q}}$ s.t. $\mathbb{Q}(\sqrt{2}, \sqrt{5}) = \mathbb{Q}(\alpha)$

Proof If F is a finite field, and $[E:F] < \infty$ then $E = F(\alpha)$ where α is any generator of $\underbrace{\langle E^*, \times \rangle}_{\text{cyclic group}}$ (Thm 33.5)

If F is infinite, suffices to consider $E = F(\beta, \gamma)$

and $F(\beta + a\gamma) \leq F(\beta, \gamma)$ for some $a \in F$

Suppose $F(\beta + a\gamma)$ is a <u>proper</u> subfield of $F(\beta, \gamma)$

$$1 < [F(\beta,\gamma) : F(\beta + a\gamma)] = \{F(\beta,\gamma) : F(\beta + a\gamma)\}$$

$\Rightarrow \exists$ an isom $\tau : F(\beta, \gamma) \to \tau[F(\beta,\gamma)] \leq \overline{F}$

fixing $F(\beta + a\gamma)$ and <u>not</u> equal to the identity on $F(\beta, \gamma)$.

$$\Rightarrow \tau(\beta + a\gamma) = \tau(\beta) + a\tau(\gamma) = \beta + a\gamma.$$

$\Rightarrow \quad a = \dfrac{\beta - \tau(\beta)}{\tau(\gamma) - \gamma}$ when $F(\beta + a\gamma)$ is a proper subfield

$\tau(\gamma) \neq \gamma.$

However there are at most $[F(\beta):F]$ conjugates of β / F and at most $[F(\gamma):F]$ conjugates of γ / F.

$\Rightarrow$ There are at most $[F(\beta):F][F(\gamma):F]$ possible $a \in F$ for which $F(\beta + a\gamma)$ is a proper subfield. Yet we have infinite choices for a!

$\exists$ $a \in F$ for which $F(\beta + a\gamma) = F(\beta, \gamma)$.

$\square$

Galois Theory §53

Def 53.1 A finite extension K of F is a **finite normal extension** of F if K is a separable splitting field over F.

Def 53.5 If K is a finite normal ext'n of F then $G(K/F)$ is the Galois group of K over F.

Thm 53.6.

(Main Theorem of Galois Theory) Let K be a finite normal extension of a field F, with Galois group $G(K/F)$. For a field E, where $F \leq E \leq K$, let $\lambda(E)$ be the subgroup of $G(K/F)$ leaving E fixed. Then λ is a one-to-one map of the set of all such intermediate fields E onto the set of all subgroups of $G(K/F)$. The following properties hold for λ:

1. $\lambda(E) = G(K/E)$.
2. $E = K_{G(K/E)} = K_{\lambda(E)}$.
3. For $H \leq G(K/F)$, $\lambda(K_H) = H$.
4. $[K : E] = |\lambda(E)|$ and $[E : F] = (G(K/F) : \lambda(E))$, the number of left cosets of $\lambda(E)$ in $G(K/F)$.
5. E is a normal extension of F if and only if $\lambda(E)$ is a normal subgroup of $G(K/F)$. When $\lambda(E)$ is a normal subgroup of $G(K/F)$, then
$$G(E/F) \simeq G(K/F)/G(K/E).$$
6. The diagram of subgroups of $G(K/F)$ is the inverted diagram of intermediate fields of K over F.

$K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$

σ :

τ :

γ :

$$\begin{tikzcd}
 & G(K/\mathbb{Q}) \arrow[dl, no head] \arrow[d, no head] \arrow[dr, no head] & \\
\langle \sigma \rangle \arrow[dr, no head] & \langle \tau \rangle \arrow[d, no head] & \langle \gamma \rangle \arrow[dl, no head] \\
 & \{id\} &
\end{tikzcd}$$

subgroup diagram

$$\begin{tikzcd}
 & K \arrow[dl, no head] \arrow[d, no head] \arrow[dr, no head] & \\
\mathbb{Q}(\sqrt{5}) \arrow[dr, no head] & \mathbb{Q}(\sqrt{2}) \arrow[d, no head] & \mathbb{Q}(\sqrt{10}) \arrow[dl, no head] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Intermediate field diagram