# HW 12

1. a. True: If $f(x)$ has $\alpha$ as a root and $m(x)$ is the minimal polynomial of $\alpha$ over $F$, then do poly. division alg to write

$$f(x) = q(x)\,m(x) + r(x), \quad \deg(r(x)) < \deg(m(x)).$$

then $\quad f(\alpha) = q(\alpha)\,m(\alpha) + r(\alpha)$

$\Rightarrow \quad 0 = 0 + r(\alpha)$

$\quad \Rightarrow \alpha$ is a root of $r(x)$.

if $r(x) \neq 0$ then this contradicts the minimality of $m(x)$.

so $r(x) = 0$ and $m(x) \mid f(x)$.

b. False. if $E$ is algebraic but not finite degree $/F$, then suppose it's simple: $E = F(\alpha)$, $\alpha \in E$.

then $\alpha$ is algebraic, and $[E:F]$ = degree of the min poly of $\alpha$, which is impossible for a not-finite-degree alg extension.

Ex: $\mathbb{Q} \subseteq \overline{\mathbb{Q}}$ is algebraic, but not finite degree, so definitely not simple.

c. False: if $t$ is transcendental over $F$, then $F(t)$ is not algebraic, but it is simple.

d. True: if $y^2$ is algebraic over $F$, say $y^2$ is a root of $f(x) = \sum_{i=0}^{n} a_i x^i$.

$$\text{i.e.} \quad f(y^2) = \sum_{i=0}^{n} a_i y^{2i} = 0$$

then let $g(x) = \sum_{i=0}^{n} a_i x^{2i}$ and note that $g(y) = f(y^2) = 0$, so $y$ is algebraic $/F$.

e. True: if $f(x) \in F[x]$ is a polynomial with $\alpha$ as a root, then we can think of $f(x)$ as a polynomial in $E[x]$ to conclude $\alpha$ is also algebraic over $E$.

f. False: Let $t$ be transcendental over $F$ and consider

$$F \subseteq F(t^2) \subseteq F(t).$$

$t$ is a root of $f(x) = x^2 - t^2 \in F(t^2)$, so it is algebraic over $F(t^2)$.

2. $|G(E/F)|$ is the number of <u>auto</u>morphisms of $E$ that are extensions of $id : F \to F$.

$\{E:F\}$ is the number of isomorphism from $E$ to any other subfield of $\overline{F}$ extending $id : F \to F$. Since the automorphisms in $G(E/F)$ form a subset of the set of <u>all</u> iso extensions, we have

$$|G(E/F)| \leq \{E:F\}$$

By theorem 51.6, $\{E:F\} \mid [E:F]$,

so $$\{E:F\} \leq [E:F].$$

3. Let $F \leq E$ be a finite field extension and assume that the fixed field of $G(E/F)$ is $F$. To show $E$ is a finite normal extension, we need to show that for all $\alpha \in E$, $\alpha$ is separable and its minimal polynomial splits in $E$.

A priori, the minimal polynomial of $\alpha/F$ factors in $\overline{F}$ as $f(x) = (x-\alpha_1)^{\vee} \ldots (x-\alpha_m)^{\vee}(x-\beta_1)^{\vee} \ldots (x-\beta_n)^{\vee}$

where $\alpha_1, \dots, \alpha_m \in E$, $\beta_1, \dots, \beta_n \notin E$, $(\alpha_1 = \alpha)$

and $v \geq 1$ is the multiplicity of the roots of $f(x)$. we want to show that actually, $v = 1$ (separability) and there are no $\beta$ terms (splitting of minimal polynomial).

Consider $g(x) = (x - \alpha_1) \dots (x - \alpha_m) \in \overline{F}[x]$.

its coefficients are the elementary symmetric expressions in $\alpha_1, \alpha_2, \dots, \alpha_m$, so:

constant term: $\pm \alpha_1 \alpha_2 \cdots \alpha_m$

coeff on $x$ : $\pm \sum_{i=1}^{m} \alpha_1 \alpha_2 \cdots \alpha_{i-1} \alpha_{i+1} \cdots \alpha_m$

$\vdots$

coeff on $x^{n-2}$ : $\pm (\alpha_1 \alpha_2 + \alpha_1 \alpha_3 + \dots + \alpha_{m-1} \alpha_m)$

coeff on $x^{n-1}$ : $\pm (\alpha_1 + \alpha_2 + \dots + \alpha_m)$.

Any $\sigma \in G(E/F)$ permutes the $\alpha_1 \dots \alpha_m$ roots, which means $\sigma$ fixes $g(x)$. so $g(x) \in F[x]$. But $\deg(f(x)) = v(m+n)$ while $\deg(g(x)) = m$.

by minimality, $v(m+n) \leq m$, which only happens if $v = 1$ and $n = 0$. so $g(x)$ is the minimal polynomial of $\alpha$, which is therefore separable with a splitting min poly over $F$.

4. see the proof of thm 56.3 (p 451) for the arguments we used in class.