Lec 10/9

Wednesday, October 9, 2019 11:43

Def The minimal polynomial of an algebraic element u over F is the monic generator of $\mathrm{Ker}(F[x] \longrightarrow F[u])$.

Def $h(x) \in F[x]$ is irreducible if $h(x) = w(x)\, v(x) \Rightarrow w(x)$ or $v(x) \in F$.
(0 is not considered to be irreducible or reducible).

Thm: Let u be algebraic over F w/ minimal poly. $g(x)$.
If $g(x)$ is irreducible, $F[u]$ is a field. If not, $F[u]$ is not a domain.

Def a root of $f(x) \in F[x]$ is $a \in F$ s.t. $f(a) = 0$.

Thm $f(x) \in F[x]$ has at most $\deg f$ distinct roots in F.

Pf Let $a_1, \dots, a_r$ be some distinct roots of f. Then $\prod_{i=1}^{r} (x - a_i) \mid f(x)$.

To show this, use induction on r.

Base case: $r = 1$. $f(x) = q(x)(x - a_1) + \cancelto{0}{f(a_1)} = q(x)(x - a_1)$.

Induction: $f(x) = q(x) \prod_{i=1}^{r-1} (x - a_i)$. since $\prod_{i=1}^{r-1} (a_r - a_i) \neq 0$,

$q(a_r) = 0$ so $(x - a_r) \mid q(x)$ by base case. $\square$

Thm Let F be a field Any finite subgp of $F^\times$ is cyclic.

Pf Let $G \leq F^\times$, $|G| < \infty$. G is abelian.

G is cyclic iff $\exp(G) = |G|$ $\left[\exp(G) := \min\{\ell \mid g^\ell = 1\ \forall g \in G\}\right]$

Note that $\exp(G) = \max\{\mathrm{ord}(g) \mid g \in G\} \leq |G|$.

We have $x^{\exp(G)} - 1$ has at most $\exp(G)$ roots in F,

So it has at most $\exp(G)$ roots in G.

But all $g \in G$ are roots. So $\exp(G) = |G|$. $\square$

Consider the ring $\underbrace{F^F}_{\substack{\text{pointwise} \\ \text{mult \& addition}}}$. $\mathbb{1}_F$ is the id map, e.g. $\mathbb{1}_F^n : s \longmapsto s^n$.

View F as a subring of F^F by $a = x \longmapsto a$.

We write $F[\mathbb{1}_F]$ in the form $F[s]$, the ring of <u>polynomial functions</u> in one var. over F.

We have a surj. hom $\eta_s : F[x] \longrightarrow F[s]$ extending $F \hookrightarrow F[s]$ and mapping $x \longmapsto s$.

<u>Prop</u> η_s is an isomorphism $F[x] \cong F[s]$ iff F is infinite.