Review for Exam 2

Theme: Polynomials in 1 variable.

Let R be comm. ring with 1.

Theorem: Consider an ideal $I \subseteq R$.

(1) R/I field $\iff$ I is maximal

(2) R/I domain $\iff$ I is prime.

Proof of (2): Recall ring R/I has $1_{R/I} = 1 + I$ and $0_{R/I} = 0 + I = I$.

Sp. I is prime and consider $a+I, b+I \neq I$ (i.e. $a \notin I, b \notin I$). Then I prime $\Rightarrow ab \notin I$ $\Rightarrow (a+I)(b+I) = ab + I \neq I$. ///

Conversely, sp. R/I a domain. Consider $a, b \in R$ with $ab \in I$ (i.e. $ab + I = I$). Then R/I domain $(a+I)(b+I) = I \Rightarrow a + I = I$ (i.e. $a \in I$) OR $b + I = I$ (i.e. $b \in I$) ///

$\blacksquare$

Given any ring R define

$R[x] := \{ \sum_{i \geq 0} a_i x^i \mid a_i \in R, a_i = 0$ almost always $\}$

x is just a formal placeholder ("variable")

Now let R be a domain.

FACTS:

① $R[x]$ is a domain with $\deg(fg) = \deg(f) + \deg(g)$ and $(R[x])^\times = R^\times$
(Think: What does $R \subseteq R[x]$ mean?).

② Given $f, g \in R[x]$, g monic, $\exists q, r \in R[x]$

$$f = qg + r, \quad \deg(r) < \deg(g) \text{ OR } r = 0.$$

Proof: long division. $\boxtimes$

② Cor: For F a field, $F[x]$ is a Euclidean Domain ($\Rightarrow$ PID $\Rightarrow$ UFD).

③ Cor: Given $f(x) \in R[x]$, $\alpha \in R$.

"$f(\alpha)$" $= 0 \iff (x - \alpha) \mid f(x)$ in $R[x]$.

Say α is root of multiplicity k if $k \in \mathbb{N}$ largest such that $(x-\alpha)^k \mid f(x)$.

(4) Cor: Given $\deg(f) = n$, then f has $\leq n$ roots counting multiplicity.

Issue: What does "$f(\alpha)$" mean?

Consider $R \subseteq S$. Then $\forall \alpha \in S$ $\exists!$ ring hom $\varphi_\alpha : R[x] \to S$

$$\begin{cases} x \longmapsto \alpha \\ a \longmapsto a \quad \forall a \in R. \end{cases}$$

Notation: $f(\alpha) := \varphi_\alpha(f(x)) \in S$.

DEF: $R[\alpha] := \operatorname{im} \varphi_\alpha \subseteq S$

FACT: $R[\alpha]$ is the smallest subring of S containing $R \cup \{\alpha\}$.

SAY: $R[\alpha]$ = "R adjoin α".

1st Iso Thm:

$$\frac{R[x]}{\ker \varphi_\alpha} \approx \operatorname{im} \varphi_\alpha = R[\alpha] \subseteq S$$

$$f(x) + \ker \varphi \longmapsto f(\alpha).$$

Now let F be a field, so $F[x]$ is PID.

Given $F \subseteq K$ with $\alpha \in K$ alg. / F we have

$$F[\alpha] = \operatorname{im} \varphi_\alpha \approx F[x]/\ker\varphi_\alpha = F[x]/(f_\alpha(x))$$

for unique, monic $f_\alpha \in F[x]$.

FACTS:

(1) $f_\alpha(x)$ is irreducible.
Proof: If $f_\alpha(x) = g(x)h(x)$ then
$g(\alpha)h(\alpha) = f_\alpha(\alpha) = 0 \implies$ WLOG $g(\alpha) = 0$
$\implies g \in \ker\varphi_\alpha = (f_\alpha) \implies (g) = (f_\alpha)$. ///

(2) Cor: $F[\alpha] = F(\alpha)$ = the smallest subfield of K containing $F \cup \{\alpha\}$.

(3) If $\deg(f_\alpha)$ then $F(\alpha)$ is a vector space over F with basis $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$

i.e. $[F(\alpha) : F] = \dim_F F(\alpha) = \deg(f_\alpha)$.

Tower Law: Given fields $F \subseteq K \subseteq L$,

$$[L:F] = [L:K]\cdot[K:F]$$

Proof: If $L:K$ has basis $\alpha_1, \dots, \alpha_m$ and $K:F$ has basis $\beta_1, \dots, \beta_n$

Then $L:F$ has basis $\{\alpha_i \beta_j\}\ \forall i,j$

Kronecker's Theorem (1887).

Given field F and $f(x) \in F[x]$, $\deg(f) \geq 1$, $\exists$ field $K \supseteq F$ and $\alpha \in K$ with $f(\alpha) = 0$.

i.e. $\varphi_\alpha : F[x] \longrightarrow K$.

$$f(x) \longmapsto 0$$

Proof: sp. $f(x) = g(x)p(x)$, p irred.

Take $K = F[x]/(p(x))$, $\alpha = x + (p(x))$.

$$f(x) \longmapsto f(x) + (p(x))$$

$$\begin{array}{ccccc}
F[x] & \twoheadrightarrow & F[x]/(p(x)) & & K \\
\cup & & \cup \text{ field extension.} & & \cup \\
F & \xrightarrow{\sim} & F & & F \\
a & \longmapsto & a + (p(x)) & &
\end{array}$$

$$\underbrace{\varphi_{x+(p(x))}}_{\alpha} : F[x] \longrightarrow \overbrace{F[x]/(p(x))}^{K}.$$

$$\text{DEF:} \begin{cases} x \longmapsto x + (p(x)). \\ a \longmapsto a + (p(x)). \end{cases}$$

Then $f(x) \longmapsto f(x) + (p(x))$.

But since $f(x) = g(x)p(x)$ we have

$$\begin{aligned} f(x) \longmapsto\ & g(x)p(x) + (p(x)) \\ &= (p(x)) = \text{“}0\text{”} \text{ in } \frac{F[x]}{(p(x))}. \end{aligned}$$

So by definition:

$$\text{“}f(x + (p(x)))\text{”} = \text{“}0\text{”}.$$

this is a root of f in an extension field.

$\blacksquare$

Cor: Every poly has a splitting field.

Proof: Induction on degree.

Discuss the FTA.