Math 5402

3/23/20

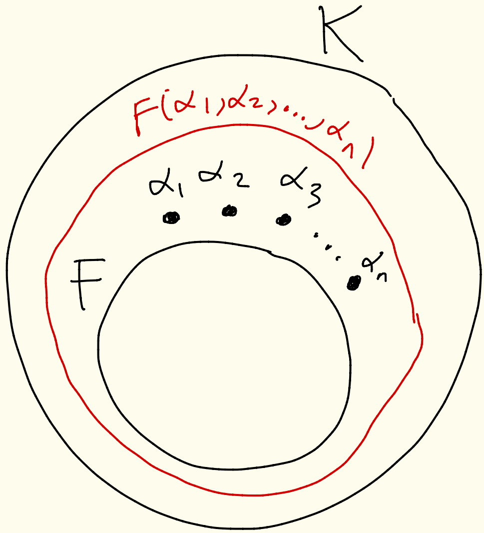
Week 10

Spring Break is still on!

13.1 continued

Def:

Let K be an extension field of a field F. Let $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$.



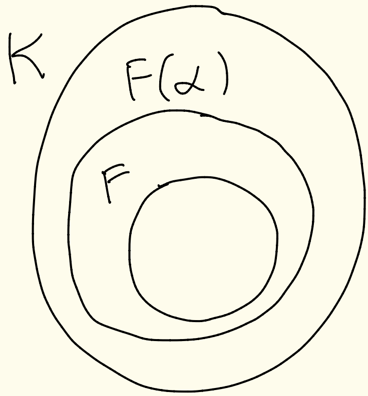
The smallest subfield of K containing both F and the elements $\alpha_1, \alpha_2, \ldots, \alpha_n$ is called <u>the field generated by $\alpha_1, \ldots, \alpha_n$ over F</u> and denoted by $F(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

$$F(\alpha_1, \ldots, \alpha_n) = \bigcap_{\substack{E \text{ is a field} \\ F \subseteq E,\ \alpha_1, \ldots, \alpha_n \in E \\ E \subseteq K}} E$$

If $K = F(\alpha)$, then K is called a <u>simple extension</u> of F.

<u>Theorem:</u> Let F be a field and let $p(x) \in F[x]$ be a non-constant irreducible polynomial. Suppose K is an extension field of F containing a root α of $p(x)$. Then

$$F(\alpha) \cong F[x]/(p(x))$$



<u>pf:</u> Consider the ring homomorphism

$$\varphi : F[x] \longrightarrow F(\alpha)$$

$$\varphi(f(x)) = f(\alpha)$$

You can check this is a ring hom.

<u>Ex:</u> $\varphi(x^2 + x) = \alpha^2 + \alpha$

$$\varphi : F[x] \to F(\alpha), \quad \varphi(f(x)) = f(\alpha)$$

Note that φ maps F to F, ie $\varphi(f)=f$ for all $f \in F$.

Since $\varphi(p(x)) = p(\alpha) = 0$.

So, $p(x) \in \ker(\varphi)$.

We can now define $\psi : F[x]/(p(x)) \longrightarrow F(\alpha)$

by $\psi\left[f(x) + (p(x))\right] = \varphi(f(x)) = f(\alpha)$

ψ is well-defined: Suppose $f(x) + (p(x)) = g(x) + (p(x))$.

Then, $f(x) - g(x) \in (p(x))$. So, $f(x) - g(x) = p(x)h(x)$.

So, $\psi\left[f(x) + (p(x))\right] = f(\alpha) = g(\alpha) + p(\alpha)h(\alpha)$

$$= g(\alpha) + 0 = g(\alpha)$$

$$= \psi\left[g(x) + (p(x))\right].$$

ψ is also a ring homomorphism.

$$\psi\left[\left[f(x) + (p(x))\right] + \left[g(x) + (p(x))\right]\right] = \psi\left[(f(x) + g(x)) + (p(x))\right]$$

$$= f(\alpha) + g(\alpha) = \psi\left[f(x) + (p(x))\right] + \psi\left(g(x) + (p(x))\right)$$

$$\psi\left[(f(x) + (p(x)))(g(x) + (p(x)))\right] = \psi\left[f(x)g(x) + (p(x))\right]$$

$$= f(\alpha)g(\alpha) = \psi\left[f(x) + (p(x))\right]\psi\left[g(x) + (p(x))\right]$$

Since $p(x)$ is irreducible in $F[x]$, we know that $(p(x))$ is maximal.

So, $\boxed{F[x]/(p(x)) \text{ is a field.}}$

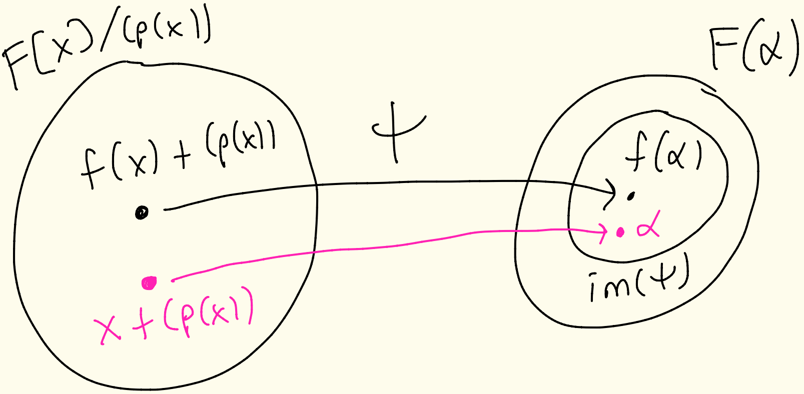
We know $\ker(\psi)$ is an ideal of the field $F[x]/(p(x))$ so $\ker(\psi) = \{0 + (p(x))\}$ or $\ker(\psi) = F[x]/(p(x))$.

Since ψ is not the zero map [for ex $\psi(1 + (p(x))) = 1 \neq 0$] we know $\ker(\psi) \neq F[x]/(p(x))$.

So, $\boxed{\ker(\psi) = \{0 + (p(x))\}.}$

So, ψ is one-to-one.

Let's now show ψ is onto $F(\alpha)$.



Note,

$$\underbrace{F[x]/(p(x))}_{\text{field}} \underset{\uparrow\ \boxed{R \cong R/\{0\}}}{\cong} \big(F[x]/(p(x))\big)/\ker(\psi) \underset{\uparrow\ \text{1st isomorphism theorem}}{\cong} \operatorname{im}(\psi)$$

So, $\operatorname{im}(\psi)$ is a subfield of $F(\alpha)$.

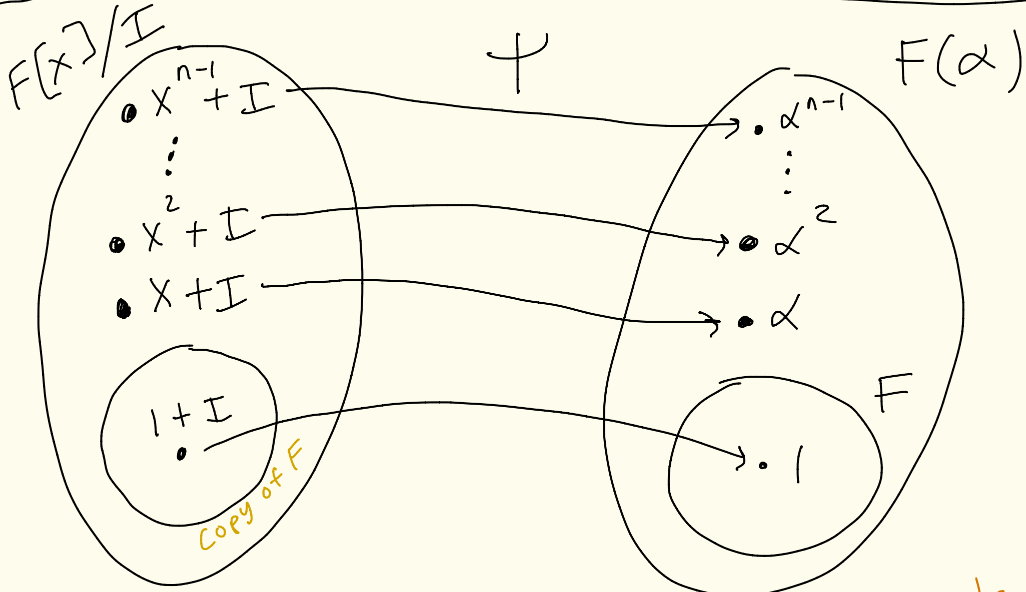
$\underline{F \subseteq \operatorname{im}(\psi)}$: Let $f \in F$. Then, $\psi(f + (p(x))) = f$.

$\underline{\alpha \in \operatorname{im}(\psi)}$: $\psi(x + (p(x))) = \alpha$.

So, since $F(\alpha)$ is the smallest field containing F and α, and $F \subseteq \operatorname{im}(\psi)$ and $\alpha \in \operatorname{im}(\psi)$, we have $F(\alpha) = \operatorname{im}(\psi)$.

So, ψ is onto. $\blacksquare$

Using the same objects as in the previous theorem, suppose $p(x)$ has degree n. Let $I = (p(x))$.



basis for $F[x]/I$ over F

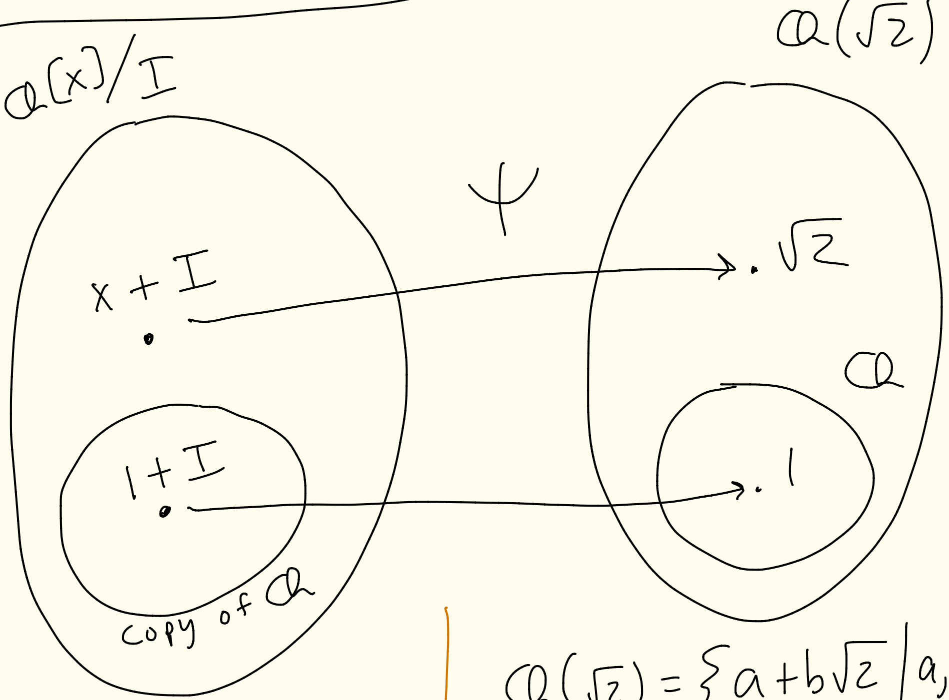
$\boxed{\text{basis for } F(\alpha) \text{ over } F \text{ is } 1, \alpha, \alpha^2, \ldots, \alpha^{n-1}}$

pg 7

Ex: $F = \mathbb{Q}$ $\quad I = (x^2 - 2)$

$p(x) = x^2 - 2$

$p(\sqrt{2}) = 0$



$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$

$1, \sqrt{2}$ are basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$

$\mathbb{Q}[x]/I$

$= \{(a + bx) + I \mid a, b \in \mathbb{Q}\}$

Thm 8 from book (pf in book) pg. 8

Let $\varphi : F \to F'$ be an isomorphism of fields. Let $p(x) \in F[x]$ is irreducible and $p'(x) \in F'[x]$ is obtained by applying φ to the coefficients of $p(x)$. Let α be a root of $p(x)$ [in some extension of F] and let β be a root of $p'(x)$ [in some extension of F']. Then there is an isomorphism $\sigma : F(\alpha) \to F'(\beta)$ where $\sigma(\alpha) = \beta$ and σ extends φ, that is $\sigma(f) = \varphi(f)$ for all $f \in F$.

$$\begin{array}{cccc} \sigma: & F(\alpha) & \xrightarrow{\cong} & F'(\beta) \\ & | & & | \\ \varphi: & F & \xrightarrow{\cong} & F' \end{array}$$

$$p(x) \longmapsto p'(x)$$

Special case:

$F = F'$, $\varphi(f) = f \ \forall f \in F$

$p(x) = p'(x)$ and α, β are two roots of $p(x)$.

Then $F(\alpha) \cong F(\beta)$.

$$\begin{array}{cccc} \sigma: & F(\alpha) & \xrightarrow{\cong} & F(\beta) \\ & | & & | \\ \varphi: & F & \xrightarrow{\cong} & F \end{array}$$