Math 5402

3/25/20

Weds

(13.1 continued...)

pg 1

Ex: Consider $q(x) = x^3 - 3x^2 + 3x - 3$

By Eisenstein with $p = 3$, $x^3 - 3x^2 + 3x - 3$ is irreducible over $\mathbb{Q}$.

Let $I = (x^3 - 3x^2 + 3x - 3)$ in $\mathbb{Q}[x]$. Then

$$\underbrace{K = \mathbb{Q}[x]/I}_{\text{field}} = \{(a + bx + cx^2) + I \mid a, b, c \in \mathbb{Q}\}$$

Eisenstein

$a_i \in \mathbb{Z}$

$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$

p prime

$p \nmid a_n$

$p \mid a_i \quad 0 \le i < n$

$p^2 \nmid a_0$

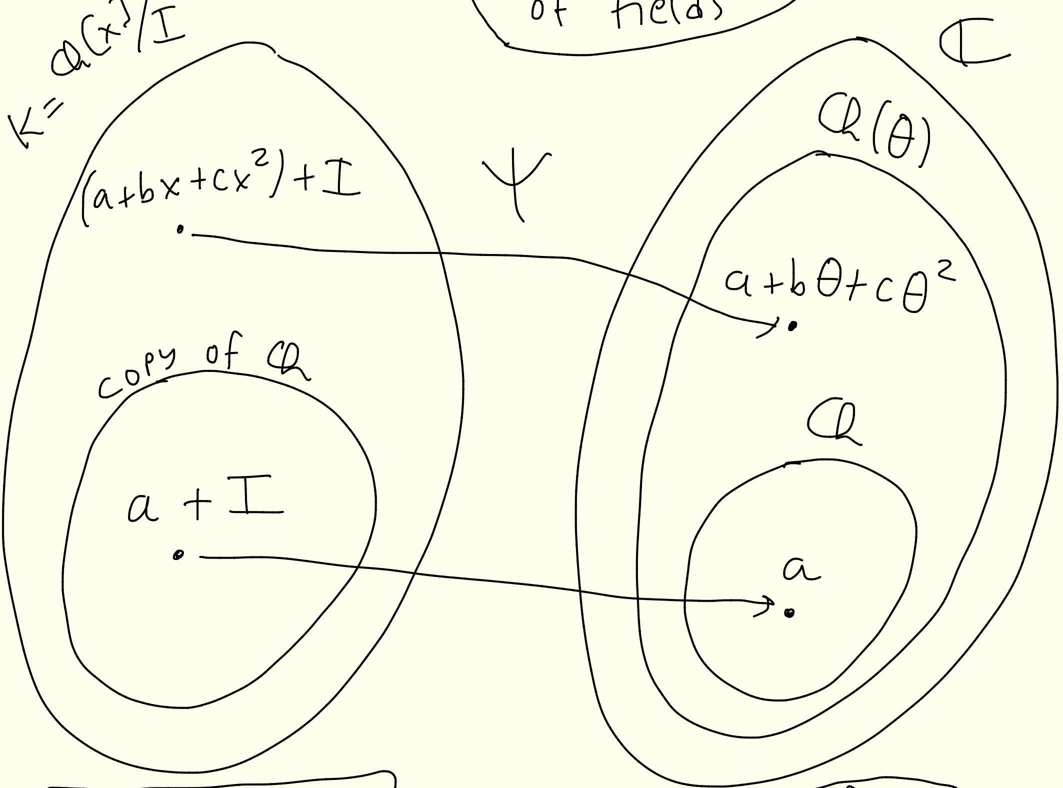
Then poly is irreducible over $\mathbb{Q}$

Let $\theta \in \mathbb{C}$ that is a root of $x^3 - 3x^2 + 3x - 3$. Note $\theta \notin \mathbb{Q}$ since q is irreducible over $\mathbb{Q}$

$$\mathbb{Q}(\theta) = \{a + b\theta + c\theta^2 \mid a, b, c \in \mathbb{Q},\ \underbrace{\theta^3 - 3\theta^2 + 3\theta - 3 = 0}_{q(\theta) = 0}\}$$

$K \cong \mathbb{Q}(\theta)$

ψ is an isomorphism of fields



basis for K over copy of $\mathbb{Q}$ $\xrightarrow{\psi}$ basis for $\mathbb{Q}(\theta)$ over $\mathbb{Q}$

$1+I \to 1$

$x+I \to \theta$

$x^2+I \to \theta^2$

Let's compute in

$$\mathbb{Q}(\theta) = \left\{ a + b\theta + c\theta^2 \;\middle|\; \begin{array}{l} a,b,c \in \mathbb{Q} \\ \theta^3 - 3\theta^2 + 3\theta - 3 = 0 \end{array} \right\}$$

Let's calculate $\frac{1}{\theta}$ in $\mathbb{Q}(\theta)$.

$$\boxed{\begin{array}{l} \underline{\text{Key}}: \; \theta^3 - 3\theta^2 + 3\theta - 3 = 0 \\ \qquad\quad \theta^3 = 3\theta^2 - 3\theta + 3 \end{array}}$$

$\frac{1}{\theta} \in \mathbb{Q}(\theta)$ since $\theta \neq 0$ and $\theta \in \mathbb{Q}(\theta)$ and $\mathbb{Q}(\theta)$ is a field.

So, $\frac{1}{\theta} = a + b\theta + c\theta^2$ for some $a,b,c \in \mathbb{Q}$.

Thus, $1 = a\theta + b\theta^2 + c\theta^3$

$= a\theta + b\theta^2 + c(3\theta^2 - 3\theta + 3)$

So, $0 = -1 + a\theta + b\theta^2 + c(3\theta^2 - 3\theta + 3)$

Thus, $0 = (-1 + 3c) + (a - 3c)\theta + (b + 3c)\theta^2$

Since $1, \theta, \theta^2$ are linearly independent, we must have

$$\left.\begin{array}{r} -1 + 3c = 0 \\ a - 3c = 0 \\ b + 3c = 0 \end{array}\right\} \to \boxed{\begin{array}{rl} & 3c = 1 \\ a & -3c = 0 \\ b & +3c = 0 \end{array}} \to \begin{array}{l} a = 1 \\ b = -1 \\ c = \frac{1}{3} \end{array}$$

$$\frac{1}{\theta} = a + b\theta + c\theta^2 = 1 - \theta + \frac{1}{3}\theta^2$$

Method 2:

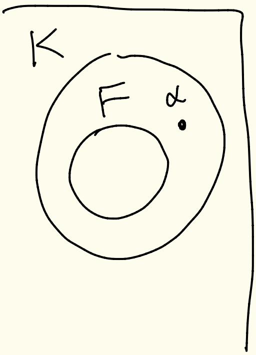
$$\theta^3 = 3\theta^2 - 3\theta + 3$$

$$\theta^2 = 3\theta - 3 + \frac{3}{\theta}$$

$$\frac{1}{\theta} = \frac{1}{3}\theta^2 - \theta + 1$$

13.2 – Algebraic Extensions

Def: Let K be an extension of a field F. An element $\alpha \in K$ is said to be algebraic over F if α is a root of some nonzero polynomial $f(x) \in F[x]$. If no such f exists then α is called transcendental over F. The extension K/F is algebraic if every $\alpha \in K$ is algebraic over F.



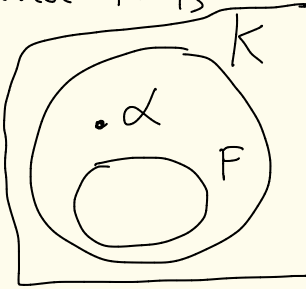
<u>Ex:</u> $\sqrt{2}$ is algebraic over $\mathbb{Q}$
since $\sqrt{2}$ is a root of $x^2-2 \in \mathbb{Q}[x]$

i is algebraic over $\mathbb{Q}$ since
i is a root of $x^2+1 \in \mathbb{Q}[x]$

π is transcendental over $\mathbb{Q}$.
Proof not short.

<u>Def:</u> $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$
is called <u>monic</u> if $a_n = 1$.

Theorem: Let α be algebraic over a field F where $\alpha \in K$ and K is some extension field of F.



Then there exists a unique, monic, irreducible polynomial $g(x) \in F[x]$ with $g(\alpha)=0$.
Moreover, $f(x) \in F[x]$ has α as a root iff $g(x)$ divides $f(x)$ in $F[x]$.

proof:

① Since α is algebraic over F, there exists some non-zero polynomial $g(x) \in F[x]$ with α as a root. Let $g(x) \in F[x]$ be a polynomial of minimal degree with α as a root.
We can assume g is monic by multiplying by a constant. ie divide off leading coefficient

Let's show $g(x)$ is irreducible over F.

Suppose $g(x)$ is reducible.

Then, $g(x) = a(x)b(x)$ where $a(x), b(x) \in F[x]$ are not units.

So, $0 < \deg(a(x)) < \deg(g(x))$

and $0 < \deg(b(x)) < \deg(g(x))$.

And, $0 = g(\alpha) = a(\alpha)b(\alpha)$.

So, either $a(\alpha) = 0$ or $b(\alpha) = 0$

but this contradicts the minimality of g.

So, $g(x)$ is irreducible in $F[x]$.

Thus there exists a monic, irreducible poly. $g(x) \in F[x]$ with $g(\alpha) = 0$.

② (Moreover) Let $f(x) \in F[x]$.

($\Leftarrow$) If $g(x)$ divides $f(x)$ in $F[x]$ then $f(x) = g(x)h(x)$ for some $h(x) \in F[x]$.

So, $f(\alpha) = g(\alpha)h(\alpha) = 0 \cdot h(\alpha)$
$= 0$.

($\Rightarrow$) Suppose $f(\alpha)=0$.
By the division algorithm there exists $q(x), r(x) \in F[x]$ where

$$f(x) = g(x)q(x) + r(x)$$

and either $r(x)=0$ or $\deg(r(x)) < \deg(g(x))$

Then,

$$\begin{aligned} 0 = f(\alpha) &= g(\alpha)q(\alpha) + r(\alpha) \\ &= 0\,q(\alpha) + r(\alpha) \\ &= r(\alpha). \end{aligned}$$

r has α as a root

So we can't have $\deg(r(x)) < \deg(g(x))$ because of the minimality of $g(x)$, unless $r(x)=0$.
Thus, $f(x) = g(x)q(x)$.
So, $g(x)$ divides $f(x)$ in $F[x]$.

③ (uniqueness of $g(x)$) Suppose $h(x) \in F[x]$ is another monic irreducible polynomial with $h(\alpha)=0$. By part 2, $g(x)$ divides $h(x)$ in $F[x]$.

So, $h(x) = g(x)\,a(x)$
where $a(x) \in F[x]$.

Since $h(x)$ is irreducible either $g(x)$ or $a(x)$ is a unit. $g(x)$ isn't a unit because $g(\alpha) = 0$, and its non-zero.

So, $a(x) = a \in F$.

Thus, $\underbrace{h(x)}_{\text{monic}} = a\,\underbrace{g(x)}_{\text{monic}}$, where $a \in F$.

$$(x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0)$$
$$= a(x^n + b_{n-1}x^{n-1} + \dots + b_1 x + b_0)$$

So, $a = 1$ and $h(x) = g(x)$. $\blacksquare$

So, $g(x)$ is unique.