Rings

Discussing ways to build new rings out of old ones.

- R ring $\longrightarrow$ polynomial ring $R[x]$

$R \subseteq S$, $a \in S$ $\quad \phi_a : R[x] \longrightarrow S$

$\qquad\qquad\qquad\qquad p(x) \longmapsto p(a)$

- Image of ϕ_a is $R[a]$ (extension of R by a)

- ring of fractions

- quotient rings

Today: extensions of fields

Def: If F, E are fields and $F \subseteq E$ we call F a <u>subfield</u> and E an <u>extension field</u> of F.

Ex: $\mathbb{Q} \subseteq \mathbb{Q}(x)$ is a field extension

Ex: $\mathbb{Q} \subseteq \mathbb{R}$ is a field extension

Ex: $\mathbb{R} \subseteq \mathbb{C}$

Def: Let $F \subseteq E$ be a field extension. An element $a \in E$ is called <u>algebraic</u> over F if $p(a) = 0$ for some non-constant polynomial $p(x) \in F[x]$. An element which is not algebraic is <u>transcendental</u>.

Ex: $\mathbb{Q} \subseteq \mathbb{C}$ $\quad i \in \mathbb{C}$

Is i algebraic over $\mathbb{Q}$?

Michelle: $\underline{p(x) = x^2 + 1}$ $\quad p(i) = i^2 + 1 = -1 + 1 = 0$

Ex: $\mathbb{Q} \subseteq \mathbb{C}$, $\quad \sqrt{2} \in \mathbb{C}$

Luis: $p(x) = x^2 - 2$ $\quad p(\sqrt{2}) = (\sqrt{2})^2 - 2 = 0$ ✓

Ex: $\mathbb{Q} \subseteq \mathbb{C}$ $\quad \pi \in \mathbb{C}$

$p(x) = x - \pi$ $\quad p(\pi) = \pi - \pi = 0$

↑ not rational

π is transcendental! Proof is hard!

Def: A real number is called an <u>algebraic number</u> if it is algebraic / $\mathbb{Q}$ and a <u>transcendental number</u> if it transcendental / $\mathbb{Q}$.

Weird fact: most numbers are transcendental

$\{x \mid x \in \mathbb{R} \text{ is algebraic} / \mathbb{Q}\}$ is countable

$\{x \mid x \in \mathbb{R} \text{ is transcendental} / \mathbb{Q}\}$ is uncountable

Give some examples of transcendental #'s:

π, e, ???

Open problem: Is $\pi + e$ algebraic?

Ex: $\mathbb{Q} \subseteq \mathbb{C}$ $\sqrt{\sqrt{2}+1}$ algebraic or transcendental?

$$\left(\sqrt{\sqrt{2}+1}\right)^2 = \sqrt{2}+1$$

$$\left(\sqrt{\sqrt{2}+1}\right)^2 - 1 = \sqrt{2}$$

$$\left(\left(\sqrt{\sqrt{2}+1}\right)^2 - 1\right)^2 = 2$$

$$\left(\left(\sqrt{\sqrt{2}+1}\right)^2 - 1\right)^2 - 2 = 0$$

$$p(x) = (x^2-1)^2 - 2 = x^4 - 2x^2 + 1 - 2$$

$p(x) = x^4 - 2x^2 - 1$ $\leftarrow$ root of this!

$\therefore$ algebraic!!

Ex: $\mathbb{Q} \subseteq \mathbb{C}$, $\sqrt{2}+\sqrt{3} \in \mathbb{C}$

Show this is algebraic!

$$(\sqrt{2}+\sqrt{3})^2 = 2 + 2\sqrt{6} + 3 = 5 + 2\sqrt{6}$$

$$(\sqrt{2}+\sqrt{3})^2 - 5 = 2\sqrt{6}$$

$$\left((\sqrt{2}+\sqrt{3})^2 - 5\right)^2 = 24$$

$$\left((\sqrt{2}+\sqrt{3})^2 - 5\right)^2 - 24 = 0$$

$\sqrt{2}+\sqrt{3}$ is a root of $p(x) = (x^2-5)^2 - 24$

$= x^4 - 10x^2 + 1$

We want to study algebraic field extensions

Def: A field extension $F \subseteq E$ is algebraic if every element of E is algebraic over F.

Ex: $\mathbb{Q} \subseteq \mathbb{Q}$ $\quad r \in \mathbb{Q} \Rightarrow p(r) = 0$ for $p(x) = x - r$

Ex: $\mathbb{Q} \subseteq \mathbb{Q}[i] = \{a + ib \mid a, b \in \mathbb{Q}\}$ is an algebraic field extension!

$$\left((a+ib) - a\right)^2 = (ib)^2 = -b^2$$

$$\left((a+ib) - a\right)^2 + b^2 = 0$$

$a+ib$ is a root of $p(x) = (x-a)^2 + b^2$
$= \boxed{x^2 - 2ax + a^2 + b^2}$

Ex: $\mathbb{R} \subseteq \mathbb{C}$ is algebraic

$a+ib$ is a root of $x^2 - 2ax + a^2 + b^2$

Theorem: If $F \subseteq E$, $a \in E$ algebraic $/F$ then $F[a]$ is an algebraic field extension

Ideal picture: $F \subseteq E$ field extension, $a \in E$ algebraic$/F$

$$I = \{f(x) \in F[x] \mid f(a) = 0\} \subseteq F[x]$$

Proposition: I is an ideal.

<u>Proof (David)</u>: Show I is the kernel of some homomorphism. Then since kernels are ideals, done!

Consider $\phi_a : F[x] \longrightarrow E$

$$f(x) \longmapsto f(a)$$

$$\ker(\phi_a) = \{ f(x) \in F[x] \mid \phi_a(f(x)) = 0 \}$$

$$= \{ f(x) \in F[x] \mid f(a) = 0 \} = I !!$$

$\square$

<u>A long, long time ago:</u>

If $f(x) \in F[x]$, $p(x) \in F[x]$ and $\deg(f) \geq \deg(p)$ then there exists $q(x), r(x) \in F[x]$ with

$\frac{f}{p} = q + \frac{r}{p}$

- $f(x) = p(x)q(x) + r(x)$ ← remainder
- $\deg(p) > \deg(r)$

<u>Def</u>: A polynomial is monic if its leading coefficient is 1

$x^3 + 3x^2 + 25x - 4$ monic $\qquad 2x^2 + 7x - 3$ not monic

<u>Def</u>: Let $F \subseteq E$, $a \in E$ algebraic. The <u>minimal polynomial</u> of a is the unique monic polynomial of smallest degree which has a as a root.

Notation: $p_a(x)$ = minimal polynomial of a.

<u>Q</u>: Why is $p_a(x)$ unique?

S'pose not! Find $\tilde{p}(x)$ monic with $\tilde{p}(a) = 0$ and $\deg(\tilde{p}) = \deg(p_a)$

$\deg(p_a - \tilde{p}) < p_a$ <u>but</u> $p_a(a) - \tilde{p}(a) = 0 - 0 = 0$

Thus $p_a(x) - \tilde{p}(x)$ is a poly of smaller degree with a as a root.

Since $p_a(x)$ has smallest degree, the only way this makes sense is if $p_a(x) - \tilde{p}(x)$ is identically 0 $\therefore$ $p_a(x) = \tilde{p}(x)$.

Ex: $\mathbb{Q} \subseteq \mathbb{C}$ $\quad \sqrt{i}$ is algebraic

$$(\sqrt{i})^{16} - 1 = i^8 - 1 = (i^2)^4 - 1 = (-1)^4 - 1 = 0$$

$\sqrt{i}$ is a root of $p(x) = x^{16} - 1$

$\sqrt{i}$ is a root of $q(x) = x^8 - 1 \leftarrow$!!

$$(\sqrt{i})^8 - 1 = i^4 - 1 = (-1)^2 - 1 = 1 - 1 = 0$$

$$\boxed{p_{\sqrt{i}}(x) = x^4 + 1} \longleftarrow \text{minimal polynomial}$$

$$(\sqrt{i})^4 + 1 = i^2 + 1 = -1 + 1 = 0$$

<u>Theorem</u>: The ideal $I = \{ f(x) \in F[x] \mid f(a) = 0 \}$ is the same as

$$I = \langle p_a(x) \rangle = \{ p_a(x) g(x) \mid g(x) \in F[x] \}.$$

In particular it's a <u>principal ideal</u>, an ideal generated by a single element.

<u>Proof</u>:

Start with $f(x) \in \langle p_a(x) \rangle$.

Then $f(x) = p_a(x) g(x)$ for some $g(x) \in F[x]$

so $f(a) = \underbrace{p_a(a)}_{0} g(a) = 0 \Rightarrow f(x) \in I$.

Now suppose instead $f(x) \in I$ and $f(x)$ is not 0.
I know $f(a)=0$.
Since $p_a(x)$ has minimal degree, $\deg(p_a) \leq \deg(f)$.

Using polynomial division, I can find $q(x), r(x) \in F[x]$ with

- $f(x) = q(x)p_a(x) + r(x)$
- $\deg(r) < \deg(p_a)$

$$0 = f(a) = q(a)\cancel{p_a(a)} + r(a) \quad \Rightarrow \quad r(a) = 0$$

This means $r(x) = 0$ so $f(x) = q(x)p_a(x)$
$\in \langle p_a(x) \rangle$

$\square$