Last time

- A field F has only two ideals: $\{0\}$ and F.
- We defined maximal ideals of a ring.
- The quotient ring R/I is a field $\iff I$ maximal ideal.

- Remarks: If R is an integral domain
  - $\langle a \rangle \subseteq \langle b \rangle \iff b \mid a$.
  - $\langle a \rangle = \langle b \rangle \iff a$ and b are associates.

- Proposition: Let R be a principal ideal domain (PID) and $a \neq 0$ in R. Then

$\langle a \rangle$ is a maximal ideal $\iff$ a is irreducible

Proof: ($\Rightarrow$) Suppose $\langle a \rangle$ is a maximal ideal. To prove that a is irreducible, suppose $a = b \cdot c$. If b is not a unit, the ideal $\langle b \rangle \supseteq \langle a \rangle$, but $\langle b \rangle$ is not the whole ring as b is not a unit, so $\langle b \rangle = \langle a \rangle$ as $\langle a \rangle$ is maximal. This means that a and b are associates. This shows that a is irreducible.

($\Leftarrow$). Suppose $\langle a \rangle$ is irreducible. Consider the ideal $\langle a \rangle$. Whenever

$\langle b \rangle \supseteq \langle a \rangle$, we have that $b \mid a$

and since a is irreducible, this means that b is a unit or b is associate to a. If b is a unit then $\langle b \rangle = R$, and if b is associate to a then $\langle b \rangle = \langle a \rangle$. This shows that $\langle a \rangle$ is a maximal ideal.

— // —

<u>Theorem:</u> Let F be a field. Let f be an irreducible polynomial in $F[x]$. Then $\langle f \rangle$ is an maximal ideal (by our previous proposition), so

$$K := F[x] / \langle f \rangle$$ is a field (by last lecture)

that contains F (K is called a <u>field extension</u> of F) and the element $\alpha = [x] \in K$ satisfies $f(\alpha) = 0$.

— // —

<u>Example.</u> $F = \mathbb{R}$. In $\mathbb{R}[x]$, x^2+1 is irreducible.

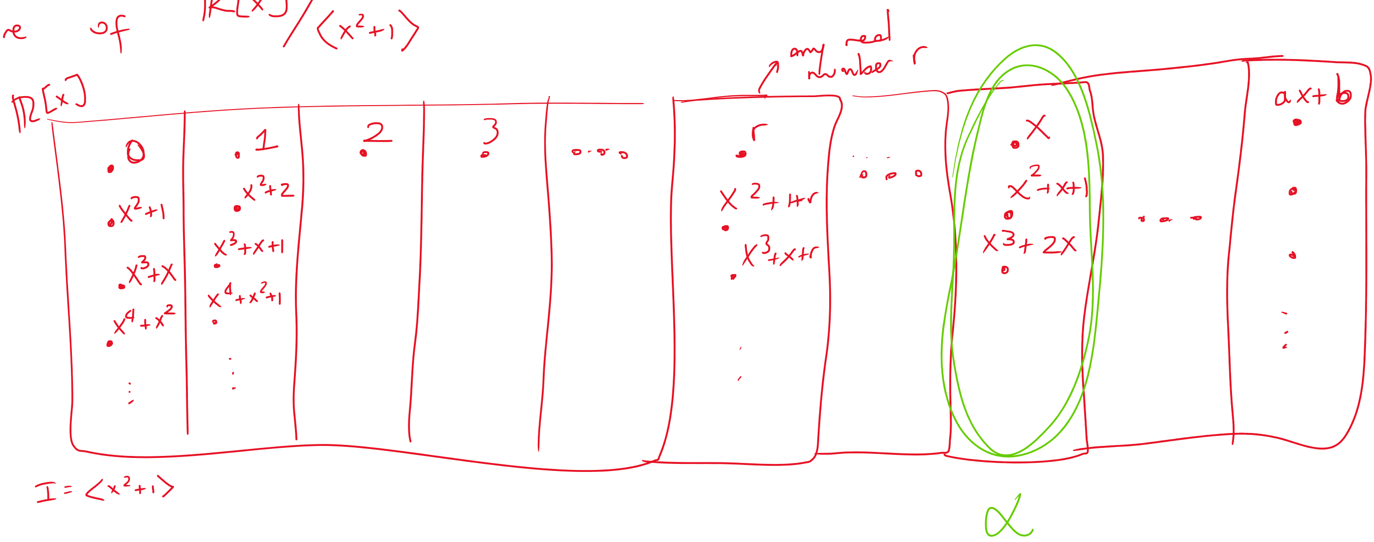
$$K := \mathbb{R}[x] / \langle x^2+1 \rangle$$ is a field.

In K, $[x^3+x+1] = [1]$ since $(x^3+x+1)-(1) \in \langle x^2+1 \rangle$.

$$[x^2+1] = [0]$$

$$[2] \neq [7]$$

Picture of $\mathbb{R}[x]/\langle x^2+1\rangle$



Take $\alpha=[x]$. In K, $\alpha^2+1=0$.

In fact, $K\cong\mathbb{C}$.

$$[ax+b]\longmapsto b+ai.$$

Proof of theorem:

- **K is an extension of F:**

Let's define the function

$$\phi: F\longrightarrow K=F[x]/\langle f\rangle$$

$$c\longmapsto [c]$$

It is an injection because

if $[c]=[d]$ then $\underbrace{c-d}_{\text{constant polynomial}}\in\langle \underbrace{f}_{\text{degree at least 1}}\rangle$

So $c-d=0$ so $c=d$.

Now ϕ is a homomorphism.

so $c - 0 = 0$ so $c = 0$.

Moreover ϕ is a homomorphism, by our definition of the operations on $F[x]/\langle f \rangle$.

- <u>The element $\alpha = [x]$ satisfies $f(\alpha) = 0$</u>:

If $f = c_n x^n + c_{n-1} x^{n-1} + \dots + c_1 x + c_0$

then
$$\begin{aligned} f(\alpha) &= c_n \alpha^n + c_{n-1} \alpha^{n-1} + \dots + c_1 \alpha + c_0 \\ &= c_n [x]^n + c_{n-1} [x]^{n-1} + \dots + c_1 [x] + c_0 \\ &= c_n [x^n] + c_{n-1} [x^{n-1}] + \dots + c_1 [x] + c_0 \\ &= [c_n x^n] + [c_{n-1} x^{n-1}] + \dots + [c_1 x] + [c_0] \\ &= [c_n x^n + c_{n-1} x^{n-1} + \dots + c_1 x + c_0] \\ &= [f] \\ &= [0] \end{aligned}$$
since $f - 0 \in \langle f \rangle$

<u>CW3</u>:

<u>2a</u>: Enough to say that $\mathbb{R}[x]$ is in some class of rings that is contained inside the class of PIDs..

- <u>Application to number theory</u> (non-examinable)

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16...

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 ...

blue = squares

red = cubes

Theorem: The equation $y^2 = x^3 - 1$ has only one solution in the integers: $x = 1$, $y = 0$.

Proof: We have $x^3 = y^2 + 1$ $(= y^2 - i^2)$

$$x^3 = (y+i)(y-i)$$

Claim: $\gcd(y+i, y-i) = $ units.

- If $\delta \mid y+i$ and $\delta \mid y-i$ then

$$\delta \mid (y+i) - (y-i) = 2i$$

$$\delta \mid 2 \qquad \text{associates} \quad (\cdot i)$$

but $2 = (1+i)(1-i)$ ← unique factorisation into irreducibles.

So if δ is not a unit then $1+i$ divides δ.

$$\Rightarrow (1+i)^2 \mid \delta^2 \mid x^3$$

$$2i \mid x^3$$

$$2 \mid x^3. \qquad \boxed{x \text{ is even}}.$$

x^3 is a multiple of 4
$\shortparallel$
y^2+1 is a multiple of 4. $\longrightarrow$ no solutions modulo 4 as y^2 is only 0 or 1 mod 4.

$\Rightarrow$ $\underline{y+i \text{ and } y-i}$ are $\underline{\text{relatively prime}}$.

Since $x^3 = (y+i)(y-i)$

then each of $y+i$ and $y-i$ is a cube. (as $\mathbb{Z}[i]$ is a UFD!)

$$y+i = (m+ni)^3.$$