Notation We will write $\bar{a}$ for $a+I$ in R/I.

Ex 1) Given $f(x) \in \mathbb{C}[x]$, $f(0)=0 \iff f(x) = x\,g(x)$

So the homomorphism $\psi: \mathbb{C}[x] \longrightarrow \mathbb{C}$

$$f \longmapsto f(0)$$

has $\ker \psi = (x)$.

Let's think of $\mathbb{C}[x]/(x)$. Elements are of the form $a_0 + a_1 x + \dots + a_n x^n + (x) = a_0 + (x)$!

Moreover $\bar{x} = \bar{0}$ i.e. $x \mapsto 0$.

2) Consider $\mathbb{R}[x]/(x^2+1)$.

Here $\overline{x^2+1} = \bar{0} \iff \bar{x}^2 = -\bar{1}$ ...

Moreover every $\bar{a} \in \mathbb{R}[x]/(x^2+1)$ can be written as $a_0 + a_1\bar{x}$.

This is just $\mathbb{C}$!

Pf $\psi: \mathbb{R}[x] \longrightarrow \mathbb{C}$, $p(x) \longmapsto p(i)$

Note that $p(i) = 0 \Rightarrow i$ is a root, since p is real coefficients $\Rightarrow -i$ is a root

$\Rightarrow x^2+1$ divide p

Thus $p \in (x^2+1)$. Conversely every $p \in (x^2+1)$ is in the kernel.

3) $ev_1 : \mathbb{R}[x] \longrightarrow \mathbb{R}$, $f(x) \longmapsto f(1)$ ("set $x=1$")

Then $\mathbb{R}[x]/(x-1) \cong \mathbb{R}$.

4) $\mathbb{Q}[x]/(x^2-1)$ is not a domain.

$(\bar{x}-1)(\bar{x}+1) = \bar{x}^2 - 1 = \bar{0}$.

But $\bar{x}-1$, $\bar{x}+1 \neq \bar{0}$.

5) On your assignment you show $\mathbb{Q}[\sqrt{2}]$ is a subfield of $\mathbb{C}$.

How do we "algebraically" obtain $\sqrt{2}$ from $\mathbb{Q}$? Here's how:

Consider $\mathbb{Q}[x]/(x^2-2)$. Our previous discussion says this is $\mathbb{Q}$ along with $\bar{x}$ satisfying $\bar{x}^2 = 2$ i.e. a square root of 2.

Remark We can of course extend our definition of polynomial rings to $R[x_1, \ldots, x_n]$ in any number of variables:

$R[x,y]$ has elements like $x+y$, $x+1$, $xy + x^3y + y^4$ etc.

6) limits done algebraically: Consider $\mathbb{R}[x, \varepsilon]$ and "set" $\varepsilon^2 = 0$ i.e. $R = \mathbb{R}[x, \varepsilon]/(\varepsilon^2)$.

We can compute derivatives of $F(x)$ as follows:

- $f(x) = x^3$: $F(x+\varepsilon) = (x+\varepsilon)^3$

$$= x^3 + 3x^2\varepsilon + 3x\varepsilon^2 + \varepsilon^3$$
$$= x^3 + \underbrace{3x^2}_{\leftarrow \text{ derivative}}\varepsilon$$

More generally, $F(x+\varepsilon) = F(x) + f'(x)\varepsilon$.

- If you set $\varepsilon^n = 0$ i.e. work in $R = \mathbb{R}[x, \varepsilon]/(\varepsilon^n)$, expanding $f(x+\varepsilon)$ gives the n-th order taylor expansion.

From now onwards K will be reserved for the letter of a field. (so $\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}$ etc).

Defn Let $p \in K[x]$ be a non-zero polynomial

- If $p = a_0 + a_1 x + \dots + a_n x^n$ with $a_n \neq 0$, then degree of p, $\deg p = n$.
- Given $f, g \in K[x]$, we say f divides g, written $f \mid g$, if $\exists\, h \in K[x]$ s.t. $g = fh$. f is called a factor of g.
- $p \in K[x]$ is said to be 'irreducible' if it's non-constant and it's only proper divisors are constant.

Thm [Division algorithm]

① If $f, g \in K[x]$, $g \neq 0$, then $\exists\, q, r \in K[x]$ such that $f = gq + r$, with $r = 0$ OR $0 \leq \deg r < \deg g$.

② If f, g have no common constant factors, $\exists$ polynomials r, s such that $fr + gs = 1$.

③ If $p \in K[x]$ is irreducible and $p \mid fg$ then $p \mid f$ or $p \mid g$

④ Every non-zero polynomial f can be written as $f = c\, p_1 \cdots p_r$ with c a unit and p_i irreducible polynomials. This is unique upto reordering and multiplication by units.

① Follows from "long division" (Thm 23.1)

② Is the Euclidean algorithm of polynomials

④ I prove in class assuming ③.

Ex
- $x^2 + 1$ is irreducible in $\mathbb{R}[x]$
- $x^3 + x + 1 = (x+1)(x^2 - x + 2) - 1$
- $x + 1$ is a factor of $x^3 + 1$

Defn
- Let $f \in K[x]$. An element $\alpha \in K[x]$ is called a root/zero of f is $f(\alpha) = 0$ in K.
- If $K' \supseteq K$ is a larger field and $\alpha \in K'$