Just as passing from a ring to a subring can gain / lose structure (e.g. there may be a subring which is a field, even though the larger ring has no inverses and non-commutative multiplication) one can also gain or lose structure by taking a quotient.

We will look at two special cases:

① If R is a commutative ring with identity, when does R/I become an integral domain?

② If R is a commutative ring with identity, when is R/I a field?

Answer to question 1:

Definition: An ideal P in a commutative ring R is called prime if $ab \in P$ implies $a \in P$ or $b \in P$, and $P \neq \{0\}$, $P \neq R$.

Theorem: Suppose R is a commutative ring with identity. Then P is a prime ideal in R if and only if R/P is an integral domain.

Proof: Suppose $P \subset R$ is prime, and suppose that in R/P we have

$$(a+P)(b+P) = ab+P = 0+P = P,$$

ie suppose two elements in R/P multiply together to give zero; and suppose $a+P \neq 0+P$ (in R/P). Then because $ab \in P$, and $a \notin P$ since $a+P \neq 0+P = P$, we must have $b \in P$ by definition of a prime ideal. Thus $b+P = P$, so $b+P$ is 0 (in R/P). Thus R/P is an integral domain.

Conversely suppose R/P is an integral domain for some P. Suppose $ab \in P$ and $a \notin P$. Then

$$(a+P)(b+P) = ab+P = P,$$

so $(a+P)(b+P)$ is 0 (in R/P), and $a+P \neq 0$ (in R/P) ~~isn~~ since $a \notin P$. Thus $b+P = 0$ (in R/P) since R/P is an integral domain, meaning $b \in P$. Thus P is a prime ideal.

<u>Example</u>: We saw that $n\mathbb{Z} \subset \mathbb{Z}$ are ideals for all $n \in \mathbb{Z}$. If n is prime, then

$$\begin{aligned} & ab \in n\mathbb{Z} \\ \Rightarrow\ & ab \text{ is a multiple of } n \\ \Rightarrow\ & \left.\begin{array}{l} \text{either } a \text{ is a multiple of } n \text{ or} \\ \qquad b \text{ is a multiple of } n \end{array}\right\} \begin{array}{l} \text{only if} \\ n \text{ is prime} \end{array} \\ \Rightarrow\ & a \in n\mathbb{Z} \text{ or } b \in n\mathbb{Z}. \end{aligned}$$

So the prime ideals in $\mathbb{Z}$ are $n\mathbb{Z}$ for n prime.

Answer to question 2

Definition: An ideal M in a ring R is a maximal ideal of R if no bigger ideal contains M, unless the bigger ideal is all of R.
I.e. M is maximal if $M \subset I$ for some ideal $I \neq M$, implies $R = I$.

Theorem: Let R be a commutative ring with identity and M an ~~maximal~~ ideal of R. Then R/M is a field if and only if M is maximal.

Proof: Let $r + M \in R/M$ be given. We need to show that $r+M$ is a unit (ie, has an inverse).
Set $M' = M + Rr = \{m + r'r \mid m \in M, r' \in R\}$

Claim: M' is an ideal. This claim takes some work, we will omit it for the sake of clarity.

Now $M \subset M'$, since for all $m \in M$, $m + r' \cdot 0 = m \in M'$, and $M' \neq M$ since M' contains r', for example, since
$r' = 0 + r' \cdot 1$.

Since M is maximal, we conclude $M' = R$. Thus M' contains 1, so we can write

$$1 = m + r'r \quad \text{for some } m \in M,\ r' \in R$$

Meaning in the quotient R/M, we have

$$\begin{aligned} 1 + M &= r'r + m + M \\ &= r'r + M \\ &= (r' + M)(r + M) \end{aligned}$$

So $r' + M$ serves as a multiplicative inverse for $r + M$ in R/M.

We will omit the converse, namely that R/M a field $\Rightarrow$ ~~R/M~~ M maximal. The idea is that ideals of R/M correspond to ideals of R containing M; and when R/M is a field the only ideals are R/M itself and $\{0 + M\}$.

<u>Example</u>: Again inside $\mathbb{Z}$, consider $p\mathbb{Z} \subset \mathbb{Z}$ for p prime. We already know $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p$ is a field; so $p\mathbb{Z}$ is actually a maximal ideal (ie there is no $n \in \mathbb{Z}$ with $p\mathbb{Z} \subset n\mathbb{Z}$, aside from $n = 1$)

Also, note that "commutative ring with identity" is a necessary hypothesis if we are to get a field upon quotienting by a maximal ideal:

Example: We already saw $2\mathbb{Z}$ is a ring without unity. Consider $4\mathbb{Z} \subset 2\mathbb{Z}$, it is a maximal ideal since $[2\mathbb{Z} : 4\mathbb{Z}] = 2$ (so the subgroup $4\mathbb{Z} \subset 2\mathbb{Z}$ can be no larger "without becoming all of $2\mathbb{Z}$")

However $2\mathbb{Z}/4\mathbb{Z}$ is not a field: The elements are

$$0 + 4\mathbb{Z} \quad \text{and} \quad 2 + 4\mathbb{Z}$$

and $2 + 4\mathbb{Z}$ does not serve as a multiplicative identity since $(2+4\mathbb{Z})(2+4\mathbb{Z}) = 4 + 4\mathbb{Z} = 0 + 4\mathbb{Z}$.

In particular, $2\mathbb{Z}/4\mathbb{Z}$ has no identity so is not a field.

Chapter 17 Polynomials.

Since we know how to add polynomials:

$$(3x^2+1)+(x^4-x^2+x) = x^4+2x^2+x+1$$

and multiply $(2x+1)(x^2-4) = 3x^3-8x+x^2-4$,
it should come as no surprise that the set of all polynomials forms a ring. We denote the ring by:

$\mathbb{Z}[x]$ — polynomials in x with coefficients in $\mathbb{Z}$

$\mathbb{C}[x]$ - polynomials in x with coefficients in $\mathbb{C}$.

Or in general, if R is a commutative ring with identity then

$$R[x] = \{\text{polynomials in } x \text{ with coefficients in } R\}$$
$$= \left\{ \sum_{i=0}^{n} a_i x^i \;\middle|\; a_i \in R,\ i \in \mathbb{Z}_{\geq 0} \right\}.$$

In this new abstract setting, we use all the same terminology as before - the <u>coefficients</u> are the $a_i \in R$, x is the <u>indeterminate</u>, a_n is the <u>leading coefficient</u> and $a_n = 1$ means the polynomial is <u>monic</u>.

The <u>degree</u> of $a_0 + a_1x^1 + \dots + a_nx^n$ is n, and we write $\deg f = n$. If $f(x) = 0$ then we define $\deg f = -\infty$.

Example: If $R = \mathbb{Z}_{12}$, then $\mathbb{Z}_{12}[x]$ is a polynomial ring. To multiply polynomials, we have:

e.g. $(2x+1)(6x^2-3) = \cancel{12}x^3 - 6x + 6x^2 - 3$

$$= 6x^2 - 6x - 3 \text{ (in } \mathbb{Z}_{12}[x]).$$

In fact, we see that some things can "cancel" and give 0 when the factors are not zero:

$$(3+3x^2)(4+4x+4x^3) = 12 + 12x + 12x^3 + 12x^2 + 12x^3 + 12x^5$$

$$= 0 \text{ in } \mathbb{Z}_{12}[x].$$

So this shows that when R is not an integral domain (like $R = \mathbb{Z}_{12}$), we can't expect $R[x]$ to be an integral domain either.

Proposition: Let $p(x), q(x) \in R[x]$ be given, and suppose R is an integral domain. Then

$$\deg(p(x)q(x)) = \deg p(x) + \deg q(x),$$

in particular $R[x]$ is an integral domain.

Proof: Write out the polynomials in full, say:

$$p(x) = a_m x^m + a_{m-1}x^{m-1} + \dots + a_1 x + a_0$$

$$q(x) = b_n x^n + b_{n-1}x^{n-1} + \dots + b_1 x + b_0$$

where $a_m \neq 0$ and $b_n \neq 0$. Then the leading term of $p(x)q(x)$ is $a_m b_n x^{m+n}$, which cannot be zero since R is an integral domain.

Therefore the degree of $p(x)q(x)$ is $m+n = \deg(p(x)) + \deg(q(x))$.
From this we can also conclude that $R[x]$ is an integral domain: If $p(x) \neq 0$ and $q(x) \neq 0$ then $\deg(p(x)) > 0$ ~~and~~ or $\deg(q(x)) > 0$ then $\deg(p(x)q(x)) > 0$. If $\deg(p(x)) = 0$ and $\deg(q(x)) = 0$ then $p(x) = a \in R$ and $q(x) = b \in R$, so $p(x)q(x) = ab \neq 0$ as long as $a \neq 0$ and $b \neq 0$.
In either case, we conclude $p(x)$ and $q(x)$ are not zero divisors and $R[x]$ is an integral domain.

<u>Remark</u>: ① We can also consider polynomials with more than one variable, with coefficients in a ring R. In this case we write $R[x,y]$ or $R[x_1, \dots, x_n]$.

② Be sure to use square brackets. $R(x)$ is something different from $R[x]$.

<u>Example</u>: Recall we saw an example of a homomorphism $\phi_{x_0} : C[a,b] \longrightarrow \mathbb{R}$ called the "evaluation homomorphism" on functions $f(x) \in C[a,b]$:

$$\phi_{x_0} = f(x_0) \quad \text{for} \quad x_0 \in [a,b].$$

There are also evaluation homomorphisms for polynomials, one for each $a \in R$.

We define $\phi_a : R[x] \longrightarrow R$ by $\phi_a(p(x)) = p(a)$.

Then checking $\phi_a(p(x)q(x)) = \phi_a(p(x))\phi_a(q(x))$

and $\phi_a(p(x)+q(x)) = \phi_a(p(x)) + \phi_a(q(x))$

is like our checking in the case $\phi_{x_0} : C[a,b] \longrightarrow \mathbb{R}$.

Recall from high school that we can do long division of polynomials:

$$\begin{array}{r|l} & \quad x^2+3x+18 \\ \hline x-5 & x^3-2x^2+3x-1 \\ & -(x^3-5x^2) \\ \hline & \qquad 3x^2+3x-1 \\ & \quad -(3x^2-15x) \\ \hline & \qquad\qquad 18x-1 \\ & \qquad -(18x-90) \\ \hline & \qquad\qquad\quad 89 \end{array}$$

So we know $x^3-2x^2+3x-1 = (x-5)(x^2+3x+18) + 89$.

It turns out we can do this in general, for any polynomial ring $R[x]$ (as long as R is a field).

Theorem: Let $f(x)$ and $g(x)$ be polynomials in $F[x]$, where F is a field and $g(x) \neq 0$. Then there exist unique polynomials $q(x), r(x) \in F[x]$ such that

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

where $\deg(r(x)) < \deg g(x)$ or $r(x) = 0$.

[Cf. the division algorithm for integers].

Proof: First we show $q(x)$ and $r(x)$ exist, and consider uniqueness second. Let $f(x) \in F[x]$ be given.

First suppose $f(x) = a$ is constant ($a \in F$).

Then

$$f(x) = g(x) \cdot 0 + a$$

so choosing $q(x) = 0$ and $r(x) = a$ works.

Now suppose $\deg f = n > 0$ and $\deg g(x) = m$. If $m > n$ then $q(x) = 0$ and $r(x) = f(x)$ works.

$$f(x) = g(x) \cdot 0 + f(x)$$

So assume $\deg g(x) = m \leq \deg f = n$. Say

$$f(x) = a_n x^n + \dots + a_1 x + a_0$$

$$g(x) = b_m x^m + \dots + b_1 x + b_0.$$

We'll induct on n

Assume: If $\deg f < n$ then $q(x)$ and $r(x)$ exist

Then the polynomial

$$h(x) = f(x) - \frac{a_n}{b_m} x^{n-m} g(x)$$

has $\deg h(x) < n$, or $h(x) = 0$, because we've engineered $h(x)$ to that the coefficient of x^n is zero.

So, there exist polynomials $q'(x)$ and $r'(x)$ with

$$h(x) = q'(x)g(x) + r'(x) \text{ and } \deg r'(x) < \deg g(x) = m, \text{ or } r = 0$$

by induction.

Set $q(x) = q'(x) + \frac{a_n}{b_m} x^{n-m}$. Then we check that

$f(x) = g(x)q(x) + r(x)$: Substituting, we get:

$$g(x)\left(q'(x) + \frac{a_n}{b_m} x^{n-m}\right) + r(x)$$

$$= g(x)q'(x) + \frac{a_n}{b_m} x^{n-m} g(x) + r(x)$$

$$= h(x) + \frac{a_n}{b_m} x^{n-m} g(x)$$

$$= f(x) - \frac{a_n}{b_m} x^{n-m} g(x) + \frac{a_n}{b_m} x^{n-m} g(x)$$

$$= f(x).$$

So by induction, $q(x)$ and $r(x)$ exist. Now to show uniqueness, suppose

$$f(x) = g(x)q(x) + r(x) \text{ with } \deg r(x) < g(x) \text{ or } r = 0$$

and

$$f(x) = g(x)q_1(x) + r_1(x) \text{ with } \deg r_1(x) < g(x) \text{ or } r_1 = 0.$$

Then $g(x)(q(x)-q_1(x)) = r(x)-r_1(x)$,
and if $g(x)$ is not the zero polynomial then

$$\deg(g(x)(q(x)-q_1(x))) \geq \deg g(x), \text{ as long as } q_1(x) \neq q(x).$$

This means $\deg(r(x)-r_1(x)) \geq \deg g(x)$, which is not possible since both r and r_1 have degree less than $g(x)$. So we must have $q(x)-q_1(x)=0$, ie $q(x)=q_1(x)$. Then

$$g(x)(q(x)-q_1(x)) = r(x)-r_1(x)$$

becomes $\quad 0 = r(x) - r_1(x)$

so $\quad r(x) = r_1(x)$.

Thus $q(x)$ and $r(x)$ are unique.

Example: Divide x^5-1 by x^2+1.

$$\begin{array}{r l}
 & x^3 - x \\
x^2+1 \,\big) & x^5+0x^4+0x^3+0x^2+0x-1 \\
 & -(x^5+0x^4+x^3) \\
\hline
 & -x^3+0x^2+0x \\
 & -(-x^3+0x^2-x) \\
\hline
 & x-1
\end{array}$$

So

$$\underset{f(x)}{x^5-1} = \underset{g(x)}{(x^2+1)}\underset{q(x)}{(x^3-x)} + \underset{r(x)}{x-1}.$$

Definition: If $p(x) \in F[x]$, we say that $a \in F$ is a zero or a root of $p(x)$ if $p(a) = 0$.

Corollary: Let F be a field and $p(x) \in F[x]$. Then $a \in F$ is a root of $p(x)$ if and only if

$$p(x) = (x-a)\,q(x) \text{ for some } q(x).$$

Proof: Suppose $a \in F$ and $p(a) = 0$. Using the division algorithm, we find $g(x)$ and $r(x)$ with

$$p(x) = g(x)(x-a) + r(x),$$

where the degree of $r(x)$ is less than the degree of $(x-a)$, or $r(x) = 0$. If $r(x) = 0$ then

$$p(x) = g(x)(x-a)$$

and we're done. So suppose $r(x) \neq 0$, then since $\deg(r(x)) = 0$, $r(x) = b \in F$ is a constant polynomial. So

$$p(x) = g(x)(x-a) + b.$$

Plugging in $x = a$ allows us to solve for b:

$$0 = p(a) = g(x)(a-a) + b$$

$$\Rightarrow 0 = 0 + b$$

$$\Rightarrow b = 0.$$

So in fact $p(x) = g(x)(x-a)$ in this case as well, and the proof is complete. //

Corollary: Let F be a field. A nonzero polynomial $p(x) \in F[x]$ can have at most n distinct zeroes in F.

Proof: We induct on $\deg(p(x))$.

As a base case, if $\deg(p(x)) = 0$ then $p(x)$ is a constant polynomial and so it has no zeroes in F. Therefore the base case holds.

Now assume $\deg p(x) > 0$. If it has no zero in F, we're done, so suppose that $a \in F$ is a zero of $p(x)$. Then $p(x) = (x-a)q(x)$ by the previous corollary, ~~so~~ where $q(x) = \deg(p(x)) - 1$ since degrees are additive in $F[x]$. Now for any other root $b \neq a$ of $p(x)$, we see that

$$0 = p(b) \quad \text{iff} \quad (b-a)q(b) = 0 \Rightarrow q(b) = 0.$$

So the remaining zeroes of $p(x)$ are in 1-1 correspondence with zeroes of $q(x)$. By induction, there are at most $n-1$ zeroes of $q(x)$. Thus means there are at most n zeroes of $p(x)$.

As with integers, polynomials can also have a gcd:

Definition: Let $p(x), q(x) \in F[x]$ be given, where F is a field. A polynomial $d(x)$ is called a common divisor of $p(x)$ and $q(x)$ if there exist polynomials $p_1(x)$ and $q_1(x)$ such that

$$p(x) = d(x)p_1(x) \text{ and } q(x) = d(x)q_1(x).$$

The polynomial $d(x)$ is called the greatest common divisor of $p(x)$ and $q(x)$ (written $\gcd(p,q)$) if every other common divisor $d'(x)$ of $p(x)$ and $q(x)$ we have $d(x) = d'(x) \cdot f(x)$ for some $f(x)$. (I.e, if $d'(x)$ divides $d(x)$).

We say p, q are relatively prime if $\gcd(p,q) = 1$.

Proposition: Let F be a field and $p(x), q(x) \in F[x]$. Set $d = \gcd(p(x), q(x))$. Then there exist $s(x), r(x) \in F[x]$ such that $d(x) = r(x)p(x) + s(x)q(x)$.

Further, the $\gcd(p(x), q(x))$ is unique.

Quotients of $F[x]$:

In order to best understand quotients of the ring $F[x]$, we need to know what kind of ideals $F[x]$ can contain. Recall that if $p(x) \in F[x]$, then the principal ideal generated by $p(x)$ is

$$\langle p(x) \rangle = \{ p(x)q(x) \mid q(x) \in F[x] \}.$$

Example: The ideal $\langle x^2 \rangle$ is

$$\{ x^2 q(x) \mid q(x) \in F[x] \},$$

meaning $\langle x^2 \rangle$ is all polynomials which have a factor of x^2.

In fact, all ideals in $F[x]$ are of this form:

Theorem: If F is a field, then every ideal $I \subset F[x]$ is a principal ideal.

Proof: Suppose $I \subset F[x]$ is an ideal. If $I = \{0\}$ then $I = \langle 0 \rangle$, so it is principal. If I contains nonzero elements, proceed as follows:

Let $p(x) \in I$ be a nonzero element of minimal degree. If $\deg p(x) = 0$ then $p(x) = a \in F$, meaning that $a \in I$. But then $a^{-1} \cdot a = 1 \in I$ (recall F is a field).

Any ideal containg 1 must be the whole ring; since $g(x) \cdot 1 \in I$ for all $g(x) \in R = F[x]$. So here $I = \langle 1 \rangle$ is again a principal ideal.

Finally the interesting case: $\deg p(x) \geq 1$. Let $f(x) \in I$ be arbitrary, and using the division algorithm write:

$$f(x) = p(x)q(x) + r(x), \text{ where } \deg r(x) < \deg p(x) \text{ or } r=0.$$

Since $p(x) \in I$ and I is an ideal, $p(x)q(x) \in I$. Since $f(x)$ is also in I and $r(x) = p(x)q(x) - f(x)$, we conclude that $r(x) \in I$. Therefore if $r \neq 0$, $r(x) \in I$ violates minimality of the degree of $p(x)$, a contradiction. Thus $p(x)q(x) = f(x)$, so $f(x) \in \langle p(x) \rangle$.

We conclude $I \subset \langle p(x) \rangle$, the reverse inclusion $\langle p(x) \rangle \subset I$ is obvious. Thus $I = \langle p(x) \rangle$.

So when considering examples of quotients of $F[x]$, we only need to consider $F[x]/\langle p(x) \rangle$ to capture all possible quotients.

<u>Example</u>: Consider $x^2 + 3x + 2 \in \mathbb{R}[x]$. There is a corresponding principal ideal

$$\langle x^2 + 3x + 2 \rangle \subset \mathbb{R}[x].$$

and consider the elements

$$(x+2)+\langle x^2+3x+2\rangle \text{ and } (x+1)+\langle x^2+3x+2\rangle$$

in $\mathbb{R}[x]/\langle x^2+3x+2\rangle$. Note that $x+2,\ x+1 \notin \langle x^2+3x+2\rangle$, because every element in $\langle x^2+3x+2\rangle$ is of the form

$$q(x)\cdot(x^2+3x+2),$$

so in particular, every element of $\langle x^2+3x+2\rangle$ must have degree ≥ 2. Since $x+2,\ x+1 \notin \langle x^2+3x+2\rangle$, the elements

$$(x+2)+\langle x^2+3x+2\rangle,\ (x+1)+\langle x^2+3x+2\rangle$$

are nonzero in $\mathbb{R}[x]/\langle x^2+3x+2\rangle$.

However, their product <u>is</u> zero:

$$\big((x+2)+\langle x^2+3x+2\rangle\big)\big((x+1)+\langle x^2+3x+2\rangle\big)$$

$$= x^2+3x+2+\langle x^2+3x+2\rangle = 0+\langle x^2+3x+2\rangle.$$

So $\mathbb{R}[x]/\langle x^2+3x+2\rangle$ is not an integral domain.

<u>Remark</u>: From the previous example, it is clear that $F[x]/\langle p(x)\rangle$ will not be an integral domain if

$p(x)$ factors: $p(x)=q_1(x)q_2(x)$.

What happens when $p(x)$ does <u>not</u> factor?

<u>Example</u>: Consider $\mathbb{R}[x]$ and the polynomial $x^2+1 \in \mathbb{R}[x]$. The polynomial x^2+1 does not factor in $\mathbb{R}[x]$: If it did, it would have a root in $\mathbb{R}$, and we know it does not. Its roots are $\pm i \in \mathbb{C}$.

Consider the quotient $\mathbb{R}[x]/_I$, where $I = \langle x^2+1 \rangle$. Use the shortcut notation:

$$[f] \text{ in place of } f + \langle x^2+1 \rangle,$$

so our multiplication and addition formulas become

$$[f]+[g] = [f+g] \text{ and } [f]\cdot[g] = [fg].$$

<u>Claim</u> $\mathbb{R}[x]/_I$ is isomorphic to $\mathbb{C}$.

We need some lemmas to prove this claim. Note that our first lemma explains why we may expect $\mathbb{C}$ as the quotient: The element $[x] \in \mathbb{R}[x]/_I$ serves as "a square root of minus 1".

<u>Lemma</u>: The equality $[x]^2 = -[1]$ holds in $\mathbb{R}[x]/_I$.

<u>Proof</u>: This is because

$[x]^2 - (-[1]) = [x^2] + [1] = [x^2+1] = [0]$, since $x^2+1 \in I$. So $[x]^2 - (-[1]) = 0 \Rightarrow [x]^2 = -[1]$.

Lemma: For every $f \in \mathbb{R}[x]$ there exist unique $a, b \in \mathbb{R}$ with $[f] = [a+bx]$.

Proof: We apply the division algorithm with $g = x^2+1$. This means there exist unique q, r with $\deg r < 2$ or $r = 0$ such that

$$f = (x^2+1)q(x) + r(x).$$

Since $\deg r < 2$, write $r = a+bx$. Then

$$f(x) - r(x) = (x^2+1)q(x) \in \langle x^2+1 \rangle$$

so $[f] = [r]$, meaning $[f] = [a+bx]$, as wanted.

Thinking of x as $\sqrt{-1} = i$, we define an isomorphism

$$\varphi : \mathbb{R}[x]/I \longrightarrow \mathbb{C}$$

by $\varphi([f]) = \varphi([a+bx]) = a+bi$.

Now we check φ is an isomorphism.

① φ is well-defined by our previous lemma, since every $[f] \in \mathbb{R}[x]/I$ can be written uniquely as $[a+bx]$.

② φ is bijective again by the previous lemma: If $\varphi([f]) = \varphi([g])$ for some $[f], [g] \in \mathbb{R}[x]/I$

Then $[f] = [a+bx]$ and $[g] = [c+dx]$ where

$a+bi = c+di \implies a=c,\ b=d$. Thus $[f]=[g]$.

Surjectivity is clear from the definition.

(3) We have to check that φ respects the ring operations. First, for all $a,b,c,d \in \mathbb{R}$ we have, if $[f] = [a+bx]$, $[g] = [c+dx]$

$$\begin{aligned}\varphi([f]+[g]) &= \varphi([a+bx]+[c+dx]) \\ &= \varphi([a+c+(b+d)x]) \\ &= a+c+(b+d)i\end{aligned}$$

while

$$\begin{aligned}\varphi([f]) + \varphi([g]) &= \varphi([a+bx]) + \varphi([c+dx]) \\ &= a+bi+c+di = (a+c)+(b+d)i.\end{aligned}$$

Next, we check multiplication.

$$\begin{aligned}\varphi([f][g]) &= \varphi([a+bx][c+dx]) \\ &= \varphi([ac+adx+bcx+bdx^2]) \\ &= \varphi([ac+(ad+bc)x]+[bd][x^2]) \\ &= \varphi([ac+(ad+bc)x]+[bd](-[1])) \\ &= \varphi([ac+(ad+bc)x]-[bd]) \\ &= \varphi([ac-bd+(ad+bc)x]) = ac-bd+(ad+bc)i\end{aligned}$$

And

$\varphi([f])\varphi([g])$

$= \varphi([a+bx])\varphi([c+dx])$

$= (a+bi)(c+di) = ac-bd+(ad+bc)i.$

So φ is an isomorphism.

So, we see that when $p(x)$ does not factor, we can actually get a field from the quotient $\mathbb{R}[x]/\langle p(x)\rangle$.

<u>Definition</u>: A nonconstant polynomial $f(x) \in F[x]$ (F a field) is called <u>irreducible</u> <u>over F</u> if $f(x)$ cannot be expressed as a product

$$f(x) = g(x)h(x)$$

where

$$0 < \deg(g(x)), \deg(h(x)) < \deg f(x).$$

<u>Theorem</u>: Let F be a field, and $f(x) \in F[x]$ be given. Then the ideal $\langle f(x)\rangle$ is maximal if and only if $f(x)$ is irreducible.

<u>Proof</u>: First suppose that $\langle f(x)\rangle$ is maximal, and that $f(x)$ factors as $f(x) = g(x)h(x)$, where both g and h are nonconstant with degrees less than $\deg f$.

Then $\langle f(x)\rangle \subset \langle g(x)\rangle$ and $\langle f(x)\rangle \subset \langle h(x)\rangle$, Since any polynomial that can be written as $r(x)f(x)$ can also be written as a multiple of either $g(x)$ or $h(x)$. Since $g(x)$ and $h(x)$ are nonconstant, neither $\langle h(x)\rangle$ nor $\langle g(x)\rangle$ is equal to $F[x]$; since $\deg(g(x))$ and $\deg(h(x))$ are both less than $\deg f(x)$, neither $g(x)$ nor $h(x)$ is contained in $\langle f(x)\rangle$. Thus we have

$$\langle f(x)\rangle \subset \langle g(x)\rangle \subset F[x]$$

and $$\langle f(x)\rangle \subset \langle h(x)\rangle \subset F[x]$$

with all containments proper. This contradicts maximality of $\langle f(x)\rangle$, so $f(x)$ must be irreducible.

On the other hand suppose $f(x)$ is irreducible, and suppose I is an ideal containing $\langle f(x)\rangle$. Then since every ideal in $F[x]$ is principal, we have $I = \langle p(x)\rangle$ for some $p(x)$. Then $\langle f(x)\rangle \subset \langle p(x)\rangle$ means that f can be written as

$$f(x) = p(x)h(x)$$

for some $h(x) \in F[x]$. This contradicts irreducibility of $f(x)$, unless one of $p(x)$ or $h(x)$ has degree zero. If $p(x)$ has degree zero then $p(x) = a \in F$, and then $I = \langle a\rangle = F[x]$. If $h(x) = a \in F$ then $p(x)$

is a scalar multiple of $f(x)$ and so $I = \langle b \cdot f(x) \rangle$ for some $b \in F$, and $\langle b \cdot f(x) \rangle = \langle f(x) \rangle$.

We conclude that I is maximal.

So

irreducible polynomials in $F[x]$

give

fields!

So if we can come up with a way of finding irreducibles in $F[x]$, then we can make a corresponding collection of fields.