Content:

Examples	Using 1st Isomorphism Theorem for rings
Definition	root
Lemma	Let F be a field. Let $f(x) \in F[x]$ and $a \in F$. Then $\exists\ q(x) \in F[x]$ such that $f(x) = (x-a)q(x) + f(a)$.

Warm Up

(1) $\mathbb{Z}[x]/(x) \cong$ _____
(2) $\mathbb{Z}[x]/(2) \cong$ _____
(3) $\mathbb{Z}[x]/I \cong$ _____
(where I is the set of polynomials with even constant term)

(1) $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$

Note that $(x) = \{x \bullet f(x) : f(x) \in \mathbb{Z}[x]\}$.
Find a homomorphism φ: $\mathbb{Z}[x] \to$ _____ such that $\ker \varphi = (x)$.
We want $\{f(x) \in \mathbb{Z}[x]: \varphi(f(x)) = 0\} = (x)$.
That is, we want $x \bullet f(x) = 0, \forall f(x) \in \mathbb{Z}[x]$.
The evaluation homomorphism, φ_0 gives us $\varphi_0(f(x)) = f(0)$,
which is 0 only when the constant term is 0.
Since $\varphi_0(f(x)) = f(0) =$ the constant term of $f(x)$, then $\text{im}\ \varphi = \mathbb{Z}$.
So, by the 1st Isomorphism theorem, $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$.

(2) $\mathbb{Z}[x]/(2) \cong \mathbb{Z}_2[x]$

Note that $(2) = \{2 \bullet f(x) : f(x) \in \mathbb{Z}[x]\}$.
Find a homomorphism φ: $\mathbb{Z}[x] \to$ _____ such that $\ker \varphi = (2)$.
We want $\{f(x) \in \mathbb{Z}[x]: \varphi(f(x)) = 0\} = (2)$.
That is, we want $2 \bullet f(x) = 0, \forall f(x) \in \mathbb{Z}[x]$.
So define φ: $\mathbb{Z}[x] \to$ _____ so that for $f(x) = a_0 + a_1x + \cdots + a_nx^n$,
$\varphi(f(x)) = [a_0]_2 + [a_1]_2x + \cdots + [a_n]_2x^n$.
Thus, $\text{im}\ \varphi = \mathbb{Z}_2[x]$.
Then, by the 1st Isomorphism theorem, $\mathbb{Z}[x]/(2) \cong \mathbb{Z}_2[x]$.

(3) $\mathbb{Z}[x]/I \cong \mathbb{Z}_2$

Note that $I = \{ f(x) \in \mathbb{Z}[x]: f(x)$ has an even constant term$\}$
Find a homomorphism φ: $\mathbb{Z}[x] \to$ _____ such that $\ker \varphi = I$.
We want $\{f(x) \in \mathbb{Z}[x]: \varphi(f(x)) = 0\} = I$.
That is, we want $\varphi(f(x)) = 0$ if $f(x)$ has an even constant term.
So define φ: $\mathbb{Z}[x] \to$ _____ so that

$$\varphi(f(x)) = \begin{cases} 0 : f(x) \text{ has an even constant term} \\ 1 : \text{ otherwise} \end{cases}$$

Or, since φ_0: $\mathbb{Z}[x] \to \mathbb{Z}$, and π: $\mathbb{Z} \to \mathbb{Z}_2$ defined by $\pi(n) = [n]$ are homomorphisms, then $\varphi = \varphi_0 \circ \pi$ is a homomorphism.
Thus, $\text{im}\ \varphi = \mathbb{Z}_2$.

Then, by the 1st Isomorphism theorem, $\mathbb{Z}[x]/I \cong \mathbb{Z}_2$.

Note $7x^2 + 3x + 5 + I = 1 + I$ since $7x^2 + 3x + 5 - 1 \in I$.

Example $\mathbb{Q}[x]/(x^2 - 2)$. Intuitive thinking: "$x^2 - 2$" = 0, so "$x^2 = 2$".
This only works when working with cosets.

$x^3 + 3x + I = 5x + I$? Yes.
$x^3 + 3x - 5x = x^3 - 2x = x(x^2 - 2) \in I$.

Or, we can see it as
$x^3 + 3x + I = x \bullet x^2 + 3x + I = x \bullet 2 + 3x + I = 5x + I$.

Aside $\mathbb{Q}$ is a field. Is $\mathbb{Q}[x]$ a field? No. There is no inverse for x.
Is $\mathbb{Q}[x]$ an integral domain? Yes. Since $\mathbb{Q}$ is an integral domain, then so is $\mathbb{Q}[x]$.

Back to $\mathbb{Q}[x]/(x^2 - 2)$. Let $I = (x^2 - 2)$. Does $(x + I)^{-1}$ exist?
$(x + I)(\_\_\_ + I) = 1 + I$.
Since "$x^2 = 2$" gives us that "$(1/2)x^2 = 1$", then
$(x + I)((\underline{1/2)x} + I) = 1 + I$, as
$(x + I)((\underline{1/2)x} + I) =$
$x \bullet (1/2)x + I =$
$(1/2)x^2 + I =$
$(1/2) \bullet 2 + I =$
$1 + I$.

So is $\mathbb{Q}[x]/(x^2 - 2)$ a field?

Note $x^7 + 5x^4 - 3x^2 + 2x - 8 + I$ collapses down to $ax + b + I, a, b \in \mathbb{Q}$.

Claim $\mathbb{Q}[x]/(x^2 - 2) = \{ax + b + I: a, b \in \mathbb{Q}\}$.
Proof:
$\{ax + b + I: a, b \in \mathbb{Q}\} \subseteq \mathbb{Q}[x]/(x^2 - 2)$ "for free".
Let $f(x) + I \in \mathbb{Q}[x]/(x^2 - 2)$ where
$f(x) = a_0 + a_1x + \cdots + a_nx^n, a_0, a_1, \ldots, a_n \in \mathbb{Q}$.
Let $k \in \{0, 1, \ldots, n\}$.
If k is even, then $a_kx^k + I = a_k(2)^{k/2} + I$.
If k is odd, then $a_kx^k + I = a_k(2)^{(k-1)/2} + I$.
So, $f(x) + I = b_0 + b_1x$ for some $b_0, b_1 \in \mathbb{Q}$.
$\therefore \mathbb{Q}[x]/(x^2 - 2) = \{ax + b + I: a, b \in \mathbb{Q}\}$.

To show $\mathbb{Q}[x]/(x^2 - 2)$ a field, we need only show that $(ax + b + I)^{-1}$ exists if one of a or b is nonzero.
Find c, d such that
$1 + I = (ax + b + I)(cx + d + I)$
$= (ax + b)(cx + d) + I$
$= acx^2 + (ad + bc)x + bd + I$
So we need to solve the system

$$\begin{cases} ad + bc = 0 \\ bd + 2ac = 1 \end{cases}$$

With a little help from Math 9 ☺ we get
$c = -a/(b^2 - 2a^2)$ and
$d = b/(b^2 - 2a^2)$.

Discussion So, what was special about $x^2 - 2$ that made $\mathbb{Q}[x]/(x^2 - 2)$ a field?
$x^2 - 2$ is maximal (i.e. $x^2 - 2$ is irreducible). $x^2 - 4$ would not work.

A little bit of 3.4

There are a lot of similarities between $\mathbb{Z}$ and $F[x]$, F a field.

Recall Standard Division Algorithm
$\forall\, m, n \in \mathbb{Z}, n \neq 0, \exists\, !\, q, r \in \mathbb{Z}$ such that $m = nq + r, 0 \leq r < |n|$.

Division Algorithm for $F[x]$, F a field.
Let $f(x), g(x) \in F[x]$ with $f(x) \neq 0$, then $\exists\, !\, q(x), r(x) \in F[x]$ such that $g(x) = f(x)\, q(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg f(x)$.
Proof:
(1) Existence
(2) Uniqueness.
Analogous to the proof in $\mathbb{Z}$. Can read it in text (p. 131).

Definition Let F be a field. If $f(x) \in F[x]$, then a *root* of $f(x)$ in F is an element $a \in F$ such that $f(a) = 0$.

Example $f(x) = x^3 - 2$. Is 2 a root?
In $\mathbb{Q}$, no. In $\mathbb{Z}_2$, yes. In $\mathbb{Z}_3$, yes.

Lemma Let F be a field. Let $f(x) \in F[x]$ and $a \in F$.
Then $\exists\, q(x) \in F[x]$ such that $f(x) = (x - a)q(x) + f(a)$.
Proof:
By the Division Algorithm, $\exists\, !\, q(x), r(x) \in F[x]$ such that
$f(x) = (x - a)q(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg f(x)$.
So $r(x) = 0$ or $\deg r(x) < \deg(x - a) = 1$. Thus $r(x) = 0$ or $\deg r(x) = 0$.
So $r(x) = c$ for some $c \in F$.
This gives us $f(x) = (x - a)q(x) + r(x) = (x - a)q(x) + c$.
Thus, $f(a) = (a - a)q(x) + c = c$.

$$\therefore f(x) = (x - a)q(x) + f(a).$$