Content:

Definition	Ideal
Proposition	Let I be a ideal in R, a ring with unity. (1) $I = R \Leftrightarrow I \cap U(R) \neq \{0\}$. (2) If R is a field, then the only ideals are $\{0\}$ and R. (3) If R is a field and φ is a homomorphism onto a ring with more than one element, S, then $R \cong S$.
Definition	principal ideal
Definition	principal ideal domain
Definition	$(a + I)(b + I) = ab + I$.
Theorem	First Isomorphism Theorem for Rings Let R, S be rings. If $\varphi: R \to S$ is a homomorphism and $K = \ker \varphi$, then $R/K \cong \varphi(R)$.

Warm Up Prove $\mathbb{Q}$ is not a ring isomorphism to $\mathbb{R}$.

Proof:
Suppose $\varphi: \mathbb{Q} \to \mathbb{R}$ is a ring isomorphism.
Then $\exists\ a \in \mathbb{Q}$ such that $\varphi(a) = 2$.
So $\varphi(a^2) = \varphi(a)^2$ by ring homomorphism properties.
And $\varphi(1) = 1$ implies that $\varphi(1 \bullet 2) = \varphi(1) \bullet \varphi(2) = \varphi(2)$.
So $\varphi(2) = \varphi(a^2)$. φ is 1-1, so $2 = a^2$.
But, since a is rational, we have a contradiction.
$\therefore$ $\mathbb{Q}$ is not a ring isomorphism to $\mathbb{R}$.

Example Let $\varphi: R \to S$ and $\ker \varphi = \{r \in R \mid \varphi(r) = 0\}$.
φ is a group homomorphism and $\ker \varphi \leq R$ (so we only need to show φ preserves $\bullet$).
Let $a,b \in \ker \varphi$. $\varphi(ab) = 0 = 0 \bullet 0 = \varphi(a)\varphi(b)$.
(So what did we just show? That $\ker \varphi$ is a subring of R?)

Note If $r \in R$ and $a \in \ker \varphi$, then $\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r) \bullet 0 = 0$.

Definition Let R be a ring. I is an *ideal* in R is $I \subseteq_{\text{subring}} R$ and
$\forall\ r \in R, a \in I, ra \in I$ and $ar \in I$.

Proposition Let I be a ideal in R, a ring with unity.
(1) $I = R \Leftrightarrow I \cap U(R) \neq \{0\}$.
(2) If R is a field, then the only ideals are $\{0\}$ and R.
(3) If R is a field and φ is a homomorphism onto a ring with more than one element, S, then $R \cong S$.
Proof: Homework (Worksheet #4).

Example Find all ideals in $\mathbb{Z}$. Recall a subring of $\mathbb{Z}$ must be of the form $n\mathbb{Z}$.
$n\mathbb{Z}$ is an ideal.

Definition The *principal ideal* generated by a is the smallest ideal containing a, denoted (a).

Question What must be in (a)?
$0, a, ra, ar, na, a^n$.
ra gives us $0a = 0$, $1a = a$, and $a^{n-1}a = a^n$.

Question What if R is commutative with unity?
Does $(a) = \{ra \mid r \in R\}$? Yes.
Commutativity takes care of ra and ar.
Do we have na? Yes.
Unity gives us $na = (1 + 1 + \cdots + 1)a = (n \bullet 1)a$.

Example $(2) \subseteq_{\text{ideal}} \mathbb{Z}$ and $(2) = 2\mathbb{Z}$.
$(2) \subseteq_{\text{ideal}} \mathbb{Z}[x]$ and $(2) = \{\text{all polynomials with even coefficients}\}$

Example $I = \{f(x) \in \mathbb{Z}[x] \mid \text{constant term is even}\} \subseteq_{\text{subring}} \mathbb{Z}[x]$.
Prove this is an ideal on your own.

Proof:
Let $f, g \in I$. Then $f = 2k + f_1x^1 + \cdots + f_nx^n$ $(k \in \mathbb{Z}, n \in \mathbb{N})$
and $g = 2j + g_1x^1 + \cdots + g_nx^n$ $(j \in \mathbb{Z}, n \in \mathbb{N})$.
So $f - g = 2(k - j) + (f_1 - g_1)x^1 + \cdots + (f_n - g_n)x^n \in I$.
And $fg = \sum_{i=0}^{n}\left(\sum_{j+k=i} f_j g_k\right)x^i = 2k \bullet 2j + \sum_{i=1}^{n}\left(\sum_{j+k=i} f_j g_k\right)x^i \in I$.
$\therefore\ I \subseteq_{\text{subring}} \mathbb{Z}[x]$.
Let $f \in I$. Let $g \in \mathbb{Z}[x]$. Then $f = 2k + f_1x^1 + \cdots + f_nx^n$ $(k \in \mathbb{Z}, n \in \mathbb{N})$
and $g = g_0 + g_1x^1 + \cdots + g_nx^n$ $(n \in \mathbb{N})$.
So $fg = \sum_{i=0}^{n}\left(\sum_{j+k=i} f_j g_k\right)x^i = 2kg_0 + \sum_{i=1}^{n}\left(\sum_{j+k=i} f_j g_k\right)x^i \in I$.
$\therefore\ I$ is an ideal of $\mathbb{Z}[x]$.

Question Is I a principal ideal? No.

Proof:
Suppose I is principal, so $I = (g(x)$ for some $g(x) \in \mathbb{Z}[x])$.
We know $2 \in$ I, so $\exists$ h(x) $\in \mathbb{Z}[x]$ such that 2 = g(x)h(x).
Since A is an integral domain, then deg g(x)h(x) = deg g(x) + deg h(x).
So deg (2) = 0 = deg g(x) + deg h(x). $\therefore$ deg g(x) = 0.
Thus, $g(x) = c$ and $h(x) = d$ for some $c, d \in \mathbb{Z}$. So $2 = c \bullet d$.
So $c = \pm 1, \pm 2$.
± 1 can't happen as $\pm 1 \notin I$.
We know $x + 0 = x \in I$, so $x = \pm 2f(x)$ for some $f(x) \in \mathbb{Z}[x]$.
But, the coefficients do not match. The coefficient of x is odd while the coefficients of $\pm 2f(x)$ are even, a contradiction.
$\therefore\ I \neq (g(x))\ \forall\ g(x) \in \mathbb{Z}[x]$.

Definition Let R be an integral domain. Then R is a *principal ideal domain* if all ideals in R are principal.

Example $\mathbb{Z}$ is a PID.

Example $\mathbb{Z}[x]$ is not a PID (just proven above).

3.8 Quotient Rings

Let R be a commutative ring with unity.
We know that $R/I = \{r + I \mid r \in R\}$ is a group.
When does $a + I = b + I$?
$a + I = b + I$ when $a - b \in I$.

Definition $(a + I)(b + I) = ab + I$.

We will check that this multiplication of representatives is well-defined.
Suppose $a + I = c + I$ and $b + I = d + I$.
Then $a - c = x$ and $b - d = y$ for some $x, y \in I$.
Since $b, c \in$ R, then $(a - c)b \in$ I and $(b - d)c \in I$.
So $(a - c)b + (b - d)c =$
$ab - cb + bc - dc =$
$ab - bc + bc - cd =$ (since R is commutative)
$ab - cd \in I$.
$\therefore$ $ab + I = cd + I$. Hence multiplication as defined is well-defined.

Note We can show this multiplication is well-defined even if R is not commutative. Just multiply on left by c. (i.e. $c(b - d) \in I$,
so $(a - c)b + c(b - d) =$
$ab - cb + cb - cd =$
$ab - cd \in I$.

Conclusion R/I is a ring $\Leftrightarrow$ I is an ideal.

Note ker φ is an ideal.

Theorem First Isomorphism Theorem for Rings
Let R, S be rings. If φ: $R \to S$ is a homomorphism and $K =$ ker φ, then $R/K \cong \varphi(R)$.
Proof:
We know there exists a group isomorphism ψ: R/K → φ(R) defined by $\psi(r + K) = \varphi(r)$. So we need only check that ψ preserves multiplication. (Do on your own).
$\psi((r + K)(s + K)) = \psi((rs + K)) = \varphi(rs) = \varphi(r)\varphi(s) = \psi(r + K)\psi(s + K)$.
$\therefore$ $R/K \cong \varphi(R)$.

Example Let I be an ideal of a ring R. Let $\pi: R \to R/I$ be defined by $\pi(r) = r + I$.
Any ideal is the kernel of some homomorphism.

Example Let $I = \{f(x) \in \mathbb{Z}[x] \mid \text{constant term is even}\}$
Consider $\mathbb{Z}[x]/I$.
$\circ(1 + I) =$ **?**
$(1 + I) + (1 + I) = 2 + I = 0 + I$.
So $\circ(1 + I) = 2$.
So 2 kills everything in this ring.
$x + I = I$. (Since $x = x + 0 \in I$)
$\mathbb{Z}[x]/I = \{I, 1 + I\} \cong \mathbb{Z}_2$.

$4x^2 + 7x - 3 + I \stackrel{?}{=} 1 + I$
$4x^2 + 7x - 3 - 1 = 4x^2 + 7x - 4 \in I$.

So $\varphi: \mathbb{Z}[x] \to \mathbb{Z}_2$ is a homomorphism with $\ker \varphi = I$.
Check this on your own.
$\varphi_0: \mathbb{Z}[x] \to \mathbb{Z}$ defined by $\varphi_0(f(x)) = f(0)$ and $\pi: \mathbb{Z} \to \mathbb{Z}_2$ defined by $\pi(n) = [n]$ are homomorphisms, then $\varphi = \pi \circ \varphi_0$ is a homomorphism.
And $\ker \varphi = \{f \in \mathbb{Z}[x] | \varphi(f(x)) = \pi(f(0)) = [0]\} = I$.