Prop 42: In any ring, the following hold:

1) \(0 \cdot a = 0 = a \cdot 0\) for all \(a \in R\)
2) \((-a)(b) = (a)(-b) = -(ab)\)
3) If \(1 \in R\), then \(-a = (-1)a\)
4) If \(1 \in R\), \((1, R + 303)\) then \(1 + 0\).

Def: \(a, b \in R\) are zero divisors if \(ab = 0\).
\(a\) is a """" if \(\exists b \neq 0\) s.t. \(ab = 0\).

Ex: \(R = M_2(\mathbb{R})\)
\[a = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \quad b = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}\]
\(ab = 0\)

Ex: \(R = \mathbb{Z}/n\mathbb{Z}\) if \(n\) is composite, then \(R\) has zero divisors
\[n = a \cdot b \Rightarrow [a] \cdot [b] = [n] = [0]\]

Def: A ring \(R\) is an integral domain if \(R\) is unital, commutative, and has no zero divisors.

Ex: Any field.
- \(\mathbb{R}\)
- \(\mathbb{C}\)
- Rings inside subfields of \(\mathbb{C}\).

Prop 43: A finite integral domain is a field.

Pf: \(\phi_a : R \rightarrow R\)
\[b \mapsto ab\]
\[b + c \mapsto a(b + c) = ab + ac = \phi_a(b) + \phi_a(c)\]
\[\ker(\phi_a) = \{b \mid ab = 0\} = \{0\} = \{0\}\]
(a not a zero divisor)
\[\Rightarrow \phi_a : R - \{0\} \rightarrow R - \{0\} \text{ is injective } \Rightarrow \text{ surjective.}\]
\[\Rightarrow \exists b \text{ s.t. } ab = 1. \Rightarrow a \text{ is invertible.}\]

Cor 44: \(\mathbb{Z}/p\mathbb{Z}\) is a field for all primes \(p\).
Def: Given a unital ring \( R \), the group of units \( R^* \) is the set of all invertible elements \( \{ a \mid \exists b \in R \text{ such that } ab = ba = 1 \} \). \( R^* \) is a group under multiplication.

Ex: \((\mathbb{Z})^* = \mathbb{Z} \pm 1\)

\((\mathbb{F})^* = \mathbb{F} \pm 1\), \( \mathbb{F} \) a field

\((\mathbb{D})^* = \mathbb{D} \pm 1\), \( \mathbb{D} \) a division ring / skew field.

\( ( )^* \) is a functor.

\( ( )^* : \text{Ring} \to \text{Grp} \)

Def: A homomorphism of rings is a function \( f : R \to S \) s.t.

1) \( f \) is a homomorphism of the underlying additive groups

2) \( f(ab) = f(a)f(b) \)

3) if \( R \neq S \) are unital, \( f(1) = 1 \)

\( u : \text{Ring} \to \text{Grp} \) is a functor.

\( ( )^* : \text{Ring} \to \text{Grp} \quad ( f : R \to S \text{, } a,b \in R^*, \text{ then } f(a), f(b) \in S^* ) \)

is a functor \( ab = 1 \Rightarrow f(a_0 b) = f(1) = 1 \)

\( f(a) f(b) \)

Def: A subset \( I \) of \( R \) is an ideal if

1) \( I \) is an additive s.g.

2) \( \forall r, s \in R, i.e. I, \quad ri, si \in I, \quad ir, si \in I \).

Prop 45: If \( K \) is the kernel of \( f : R \to S \), then \( K \) is an ideal.

If: \( \text{ker } K, r, s \in R, \text{ then } r, s \in K, \text{ then } f(r) = f(s) \).

\( f(r) f(s) = f(rs) = f(0) = 0 \) by Prop 42.

If \( I \) is an ideal, then there is a ring structure on \( R/I \) s.t.

\( R \to R/I \) is a homomorphism.

\( R/I = R/\sim \text{ where } a \sim b \text{ iff } a - b \in I \).

Abelian, additive group = \( R/I : [a] + [b] = [a+b] \)
\[ [a] \cdot [b] = [a \cdot b] \]
\[ a' = a + i \quad i, j \in I \]
\[ b' = b + j \]
\[ (a \cdot b) - (a' \cdot b') \in I \]
\[ (a \cdot b) - (a \cdot i)(b + j) \]
\[ = (a \cdot b) - (a \cdot i) - (b \cdot a) - (i \cdot b) \in I \]
\[ = -(i \cdot b + a \cdot j + i \cdot j) \in I \]
\[ I \quad I \quad I \]

**Def**: If \( I \) is an ideal, then the quotient of \( R \) by \( I \) is \( R/I \) with \([a] \cdot [b] = [a \cdot b]\).

**Prop 46**: If \( I \) is an ideal, then \( I \) is the kernel of the map \( R \rightarrow R/I \) \[ a \mapsto [a] \]

**Thm 47**: If \( f \) is a homomorphism \( R \rightarrow S \), then \( f \) induces an isomorphism \( R/\ker(f) \cong \text{Im}(f) \subseteq S \)

**Pf**: \[ \frac{R}{\ker(f)} \xrightarrow{\tilde{f}} \text{Im}(f) \]
\[ [a] \quad \mapsto \quad f(a) \]
\[ \tilde{f}([a] \cdot [b]) = \tilde{f}([a \cdot b]) = f(a \cdot b) = f(a) \cdot f(b) = \tilde{f}([a]) \cdot \tilde{f}([b]). \]

1st isom thm for groups \( \Rightarrow \) \( \tilde{f} \) is a 1-1, onto homomorphism of groups, \( \tilde{f} \) is a hom of rings \( \Rightarrow \) \( \tilde{f} \) an iso.

**Prop 48**: \( R/I \) has a universal property: If \( f : R \rightarrow S \) has \( \ker(f) = I \), then there is a unique map \( \tilde{f} : R/I \rightarrow S \) s.t.
\[ \begin{array}{ccc}
R & \xrightarrow{f} & S \\
\downarrow & & \downarrow \tilde{f} \\
R/I & \xrightarrow{\tilde{f}} & S
\end{array} \]

**Def**: If \( I \) and \( J \) are ideals, then \( I \cap J \) is an ideal!
\[ I + J = \{ i + j \mid i \in I, j \in J \} \]
\[ IJ = \{ i \cdot j + i \cdot j' + \ldots \mid i^{(i)} \in I, j^{(j)} \in J \} \]

**Thm 49**: \( I + J ) / J \cong I / I \cap J \)
Thm 5.30: \( R/I \equiv (R/J)/(I/J) \quad J \leq I \leq R \) , I, J ideals.