Definition 15.1 (Ring Homo/Isomorphism). *A mapping ϕ from ring R to S is a ring homomorphism, if it preserve the operations, that is:*

$$\phi(a+b) = \phi(a) + \phi(b) \quad \phi(ab) = \phi(a)\phi(b0)$$

If the mapping is one-to-one and onto, then it is also a ring isomorphism.

Theorem 15.1 (Properties of Ring Homomorphism). *Let ϕ a homomorphism from ring R to ring S.*

1. *For any $r \in R$ and any positive integer n, $\phi(nr) = n\phi(r)$ and $\phi(r^n) = (\phi(r))^n$*
2. *Let A a subring of R, then $\phi(A) = \{\ \phi(a) \mid a \in A\ \}$ is a subring of S.*
3. *If A is an ideal and ϕ is onto, then $\phi(A)$ is an ideal of S.*
4. *Let B a ideal of S, then $\phi^{-1}(B) = \{\ a \in R \mid \phi(a) \in B\ \}$ is an ideal of R.*
5. *If R is commutative, then $\phi(R)$ is commutative.*
6. *If R has a unity, $S \neq \{0\}$, and ϕ is onto, then $\phi(1)$ is the unity of S, and for any $r \in R$ where r is a unit, then $\phi(r)$ is also a unit.*
7. *ϕ is a isomorphism iff ϕ is onto and $\operatorname{Ker}\phi = \{\ a \in R \mid \phi(a) = 0\ \} = \{0\}$.*
8. *If ϕ is a isomorphism, then ϕ^{-1} is a isomorphism.*

Proof.

- Trivial, since homomorphism preserve operations.
- Trivial.
- For any $s \in S$, there is $r \in R$ such that $\phi(r) = s$ since ϕ onto, then for any $\phi(a) \in \phi(A)$, $\phi(a)s = \phi(a)\phi(r) = \phi(ar) \in \phi(A)$, same for $s\phi(a)$.
- For any $r \in R$, $\phi(r\phi^{-1}(B)) = \phi(r)B \subseteq B$, therefore $r\phi^{-1}(B) \subseteq \phi^{-1}(B)$.
- Trivial.
- For any $s \in S$, $s = \phi(1\phi^{-1}(s)) = \phi(1)s$, therefore $\phi(1)$ is the unity.

- For any $ab \in R$, $\phi(a) = \phi(b) \to \phi(a) - \phi(b) = 0 \to \phi(a-b) = 0$, therefore $a - b = 0$ since $\operatorname{Ker}\phi = \{0\}$, and $a = b$. Then ϕ is one-to-one.
- ...

□

Theorem 15.2 (Kernals are Ideals)**.** *Let ϕ a ring homomorphism from R to S, then $\operatorname{Ker}\phi$ is an ideal of R.*

Proof. By ideal-test:

0. $\operatorname{Ker}\phi$ is non-empty, since $0 \in \operatorname{Ker}\phi$.
1. For any $a\ b \in \operatorname{Ker}\phi$, $\phi(a-b) = \phi(a) - \phi(b) = 0 - 0 = 0$.
2. For any $a \in \operatorname{Ker}\phi$ and $b \in R$, $\phi(ab) = \phi(a)\phi(b) = 0\phi(b) = 0$.

□

Theorem 15.3 (First Isomorphism Theorem for Rings)**.** *Let ϕ a ring homomorphism from R to S, then the mapping from $R/\operatorname{Ker}\phi$ to $\phi(R)$, given by $\psi(r + \operatorname{Ker}\phi) = \phi(r)$ is a isomorphism, that is, $R/\operatorname{Ker}\phi \approx \phi(R)$.*

Proof. We know First Isomorphism Theorem works on (additive) groups, so we need to check that ϕ preserve multiplication. For any $s + \operatorname{Ker}\phi$ and $t + \operatorname{Ker}\phi$:

$$\begin{aligned}
&\psi((s + \operatorname{Ker}\phi)(t + \operatorname{Ker}\phi)) \\
=&\psi(st + \operatorname{Ker}\phi) \\
=&\phi(st) \\
=&\phi(s)\phi(t) \\
=&\psi(s + \operatorname{Ker}\phi)\psi(t + \operatorname{Ker}\phi)
\end{aligned}$$

□

Theorem 15.4 (Ideals are Kernals)**.** *For any ideal I of some ring R, I is the kernal of homomorphism: $\phi(r \in R) = r + I$.*

Theorem 15.5 (Homomorphism from Z to a Ring with Unity)**.** *Let R be a ring wuth unity, the mapping $\phi(n) = n \cdot 1$ is a homomorphism from Z to R.*

Proof. Obviously, ϕ is a function, then we need to check whether ϕ is a homomorphism, for all $a\ b \in Z$:

- $\phi(a+b) = (a+b)\cdot 1 = a\cdot 1 + b\cdot 1 = \phi(a)+\phi(b)$
- $\phi(ab) = (ab)\cdot 1 = (a\cdot 1)(b\cdot 1) = \phi(a)\phi(b)$

$\square$

Corollary 15.1. *Let R a ring with unity, then R contains Z_n where $n > 0$ is the characteristic of R or $\mathbb{Z}$ if the characteristic of R is 0.*

Proof. By Theorem 15.5, we know $\phi(n) = n\cdot 1$ is a homomorphism from $\mathbb{Z}$ to R, if $\operatorname{char} R = m$ where $m > 0$, then we know $\operatorname{Ker}\phi =$ the set of multiple of m $= m\mathbb{Z} = \langle m\rangle$, therefore $\phi(\mathbb{Z}) \approx \mathbb{Z}/m\mathbb{Z} \approx Z_m$ is a subring of R. If $\operatorname{char} R = 0$, then $\operatorname{Ker}\phi = \{0\}$, therefore $\phi(\mathbb{Z}) \approx \mathbb{Z}$ is a subring of R. $\square$

Corollary 15.2. *For any positive integer m, the mapping $\phi(x) = x \bmod m$ is a homomorphism from Z to Z_m.*

Corollary 15.3. *Let F a field, then F contains Z_p if F has a non-zero characteristic p or Q if F has a zero characteristic.*

Proof. By Corollary 15.1, we know F contains Z_p if $\operatorname{char} F$ is non-zero. We claim the mapping $\phi(\frac{a}{b}) = (a\cdot 1)(b\cdot 1)^{-1}$ is a homomorphism from Q to F. We need to show that ϕ **is** a function. For any $\frac{a}{b} = \frac{c}{d}$, we know $ad = bc$,

$$\begin{aligned} ad\cdot 1 =& bc\cdot 1 \\ (a\cdot 1)(d\cdot 1) =& (b\cdot 1)(c\cdot 1) \\ (a\cdot 1)(b\cdot 1)^{-1} =& (c\cdot 1)(d\cdot 1)^{-1} \end{aligned}$$

therefore $\phi(\frac{a}{b}) = \phi(\frac{c}{d})$.

Then we need to check that ϕ preserves operations, for any $\frac{a}{b}\ \frac{c}{d}\ in \mathbb{Q}:$

- $$\begin{aligned}
&\phi(\frac{a}{b}+\frac{c}{d}) \\
=&\phi(\frac{ad+bc}{bd}) \\
=&((ad+bc)\cdot 1)(bd\cdot 1)^{-1} \\
=&(ad\cdot 1+bc\cdot 1)(bd\cdot 1)^{-1} \\
=&(ad\cdot 1)(bd\cdot 1)^{-1}+(bc\cdot 1)(bd\cdot 1)^{-1} \\
=&\phi(\frac{ad}{bd})+\phi(\frac{bc}{bd}) \\
=&\phi(\frac{a}{b})+\phi(\frac{c}{d})
\end{aligned}$$

- $$\begin{aligned}
&\phi(\frac{a}{b}\times\frac{c}{d}) \\
=&\phi(\frac{ac}{bd}) \\
=&(ac\cdot 1)(bd\cdot 1)^{-1} \\
=&(a\cdot 1)(c\cdot 1)(d\cdot 1)^{-1}(b\cdot 1)^{-1} \\
=&(a\cdot 1)(b\cdot 1)^{-1}(c\cdot 1)(d\cdot 1)^{-1} \\
=&\phi(\frac{a}{b})\phi(\frac{c}{d})
\end{aligned}$$

Therefore ϕ is a homomorphism from $\mathbb{Q}$ to F, then $\phi(\mathbb{Q}) \approx \mathbb{Q}/\operatorname{Ker}\phi$ is a subring of F. We claim $\operatorname{Ker}\phi = \langle 0\rangle$. For any $\frac{a}{b} \in \operatorname{Ker}\phi$, we know $\phi(\frac{a}{b}) = \phi(0) = 0$, therefore $(a\cdot 1)(b\cdot 1)^{-1} = 0$, we know F is an integral domain, so one of $(a\cdot 1)$ and $(b\cdot 1)^{-1}$ is zero. But we know no one have 0 as invert element, so $(a\cdot 1)$ must be 0. By $\operatorname{char} F = 0$, we know no positive a such that $a\cdot 1 = 0$, so $a = 0$ and $\frac{a}{b} = 0$. □