As in the case of a group isomorphism, the homomorphism g is unique and denoted by h^{-1}, and it is easy to show that a bijective ring homomorphism $h\colon A \to B$ is an isomorphism.

Definition 2.20. Given a ring A, a subset A' of A is a *subring* of A if A' is a subgroup of A (under addition), is closed under multiplication, and contains 1.

For example, we have the following sequence in which every ring on the left of an inlcusion sign is a subring of the ring on the right of the inclusion sign:

$$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}.$$

The ring $\mathbb{Z}$ is a subring of both $\mathbb{Z}[\sqrt{d}]$ and $\mathbb{Z}[\sqrt{-d}]$, the ring $\mathbb{Z}[\sqrt{d}]$ is a subring of $\mathbb{R}$ and the ring $\mathbb{Z}[\sqrt{-d}]$ is a subring of $\mathbb{C}$.

If $h\colon A \to B$ is a homomorphism of rings, then it is easy to show for any subring A', the image $h(A')$ is a subring of B, and for any subring B' of B, the inverse image $h^{-1}(B')$ is a subring of A.

As for groups, the *kernel* of a ring homomorphism $h\colon A \to B$ is defined by

$$\mathrm{Ker}\ h = \{a \in A \mid h(a) = 0\}.$$

Just as in the case of groups, we have the following criterion for the injectivity of a ring homomorphism. The proof is identical to the proof for groups.

Proposition 2.18. *If $h\colon A \to B$ is a homomorphism of rings, then $h\colon A \to B$ is injective iff* $\mathrm{Ker}\ h = \{0\}$. *(We also write* $\mathrm{Ker}\ h = (0)$.*)*

The kernel of a ring homomorphism is an abelian subgroup of the additive group A, but in general it is not a subring of A, because it may not contain the multiplicative identity element 1. However, it satisfies the following closure property under multiplication:

$$ab \in \mathrm{Ker}\ h \quad \text{and} \quad ba \in \mathrm{Ker}\ h \quad \text{for all } a \in \mathrm{Ker}\ h \text{ and all } b \in A.$$

This is because if $h(a) = 0$, then for all $b \in A$ we have

$$h(ab) = h(a)h(b) = 0h(b) = 0 \quad \text{and} \quad h(ba) = h(b)h(a) = h(b)0 = 0.$$

Definition 2.21. Given a ring A, an additive subgroup $\mathfrak{I}$ of A satisfying the property below

$$ab \in \mathfrak{I} \quad \text{and} \quad ba \in \mathfrak{I} \quad \text{for all } a \in \mathfrak{I} \text{ and all } b \in A \tag{$*_{\text{ideal}}$}$$

is called a *two-sided ideal*. If A is a commutative ring, we simply say an *ideal*.

It turns out that for any ring A and any two-sided ideal $\mathfrak{I}$, the set $A/\mathfrak{I}$ of additive cosets $a + \mathfrak{I}$ (with $a \in A$) is a ring called a *quotient ring*. Then we have the following analog of Proposition 2.12, also called the *first isomorphism theorem*.