Major Facts about Ring Homomorphisms

Fact 1. **(Properties of Ring Homomorphisms)**

Let $\varphi : R \to S$ be a ring homomorphism, $A \subset R$ be a subring, and $B \subset S$ be an ideal. **Then**

1. for every $r \in R$ and every positive integer n, $\varphi(nr) = n\varphi(r)$ and $\varphi(r^n) = (\varphi(r))^n$;
2. $\varphi(A) = \{\varphi(a) \,|\, a \in A\}$ is a subring of S;
3. **if** A is an ideal and φ is **onto** S, **then** $\varphi(A)$ is an ideal;
4. $\varphi^{-1}(B) = \{r \in R \,|\, \varphi(r) \in B\}$ is an ideal of R;
5. **if** R is commutative, **then** $\varphi(R)$ is commutative;
6. **if** R has unity 1, S is not trivial, and φ is **onto** , **then** $\varphi(1)$ is the unity of S;
7. φ is an isomorphism **if and only if** φ is **onto** and $\ker\varphi = \{0\}$;
8. **if** φ is an isomorphism, **then** $\varphi^{-1} : S \to R$ is also an isomorphism.

Fact 2. **(Kernels Are Ideals)** Let R and S be rings and $\varphi : R \to S$ be a ring homomorphism. **Then** the kernel $\ker\varphi = \{r \in R \,|\, \varphi(r) = 0\}$ is an ideal of R.

Fact 3. **(First Isomorphism Theorem for Rings)** Let $\varphi : R \to S$ be a ring homomorphism. **Then** $R/\ker\varphi \approx \varphi(R)$ with an isomorphism given by $r + \ker\varphi \mapsto \varphi(r)$.

Fact 4. **(Ideals are Kernels)** Every ideal A of a ring R is the kernel of a ring homomorphism $R \to R/A$ given by $r \mapsto r + A$.

Fact 5. **(Homomorphisms from $\mathbb{Z}$ to a Ring with Unity)**

Let R be a ring with unity 1. **Then** the mapping $\varphi : \mathbb{Z} \to R$ given by $n \mapsto n \cdot 1$ is a ring homomorphism.

Corollary 5.1. **If** R is a ring with unity and $\operatorname{char} R = n > 0$, **then** R contains a subring isomorphic to $\mathbb{Z}_n$. **If** $\operatorname{char} R = 0$, **then** R contains a subring isomorphic to $\mathbb{Z}$.

Corollary 5.2. For any positive integer m, the mapping $\varphi : \mathbb{Z} \to \mathbb{Z}_m$ given by $x \mapsto x \bmod m$ is a ring homomorphism.

Corollary 5.3. **If** F is a field and $\operatorname{char} F = p$, **then** F contains a subfield isomorphic to $\mathbb{Z}_p$. **If** $\operatorname{char} F = 0$, **then** R contains a subfield isomorphic to $\mathbb{Q}$.