Section 26: Homomorphisms and Factor Rings

Def: A map ϕ of a ring R into a ring R' is a *homomorphism* if

$$\phi(a+b) = \phi(a) + \phi(b)$$

and

$$\phi(ab) = \phi(a)\phi(b)$$

for all elements $a, b \in R$.

Example: *The Projection Homomorphisms:* Let $R_1, R_2, \ldots, R_n$ be rings. For each i, the map $\pi_i : R_1 \times R_2 \times \cdots \times R_n \to R_i$ defined by $\pi_i(r_1, r_2, \ldots, r_n) = r_i$ is a homomorphism. This is called the "projection onto the ith component of R_i." It is very easy to see that this meets all the requirements of the homomorphism.

A number of key results easily transfer over from group homomorphisms.

Thm: Let ϕ be a homomorphism of a ring R into a ring R'. The following properties hold:

1. If 0 is the additive identity in R, then $\phi(0) = 0'$ is the additive identity in R'.

2. If $a \in R$, then $\phi(-a) = -\phi(a)$.

3. If S is a subring of R, then $\phi(S)$ is a subring of R'.

4. If S' is a subring of R', then $\phi^{-1}(S')$ is a subring of R.

5. If R has unity 1, then $\phi(1)$ is unity for $\phi(R)$.

Def: Let a map $\phi : R \to R'$ be a ring homomorphism. The subring

$$\phi^{-1}(0') = \{r \in R | \phi(r) = 0'\}$$

is the *kernel* of ϕ, denoted $Ker(\phi)$.

Factor(Quotient) Rings: Now that we have transferred what we know about group homomorphisms to ring homomorphisms, we can extend the concept of a factor group to get a factor ring.

Thm: Let $\phi : R \to R'$ be a ring homomorphism with kernel H. Then the additive cosets of H form a ring R/H whose binary operations are defined by

$$(a+H) + (b+H) = (a+b) + Hb$$

, and

$$(a+H)(b+H) = (ab) + H$$

.

Note: The map $\mu : R/H \to \phi(R)$ defined by $\mu(a + H) = \phi(a)$ is an isomorphism.

Example: This theorem allows us to prove that $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$.

Thm: Let H be a subring of R. The multiplication of additive cosets of H is well-defined if and only if $ah \in H$ and $hb \in h$ for all $a, b \in R$ and $h \in H$.

Def: An adative subgroup N of a ring R satisfying the properties:

- $aN \subseteq N$

- $Nb \subseteq N$

for all $a, b \in R$ is an *ideal*.

Note: The book's notation is very confusing here. The requirements are easier to understand if they are put this way:

$$\forall x \in N, \forall r \in R : \quad xr \in N, rx \in N$$

(Source: Wikipedia).

Note: Ideals are the ring equivalent of normal subgroups.

Note: If R is a field, then the only ideals are $\{0\}$ and R itself. 0 will obviously obliterate anything that gets multiplied by it, and the entire field will contain everything. It is very easy to escape closure if you pick a smaller subring of R.

Example: $n\mathbb{Z}$ is an ideal in $\mathbb{Z}$. $n\mathbb{Z}$ is a subring and $s(mn) = (nm)s = n(ms) \in n\mathbb{Z}$ for all $s \in \mathbb{Z}$. What we did was to show that both left and right cosets are a subset of $n\mathbb{Z}$

Def: Let N be an ideal of a ring R. The additive cosets of N form a ring R/N with the binary operations by defined as

$$(a + N) + (b + N) = (a + b) + N$$

and

$$(a + N)(b + N) = ab + N$$

. This ring is the *factor ring* of *quotient ring* of R by N.

Thm: Let N be and ideal of a ring R. Then $\gamma : R \to R/N$ given by $\gamma(y) = x + N$ is a ring homomorphism with $Ker(\gamma) = N$.

Fundamental Homomorphism Theorem: Let $\phi : R \to R'$ be a ring homomorphism with kernel N. Then $\phi(R)$ is a ring, and the map $\mu : R/N \to \phi(R)$ given by $\mu(x + N) = \phi(x)$ is an isomorphism. If $\gamma : R \to R/N$ is the homomorphism given by $\gamma(x) = x + N$, then for each $x \in R$, we have $\phi(x) = \mu(\gamma(x))$.

Note: This theorem is basically saying that we can consider a homomorphism in two pieces. The ring is first mapped to a factor ring and then another mapping goes from the factor ring to $\phi(R)$. The book says it this way, *"every ring homomorphism with domain R gives rise to a factor ring R/N, and every factor ring R/N gives rise to a homomorphism mapping R into R/N."*

Selected Exercises:

20. Let R be a commutative ring with unity of prime characteristic P. Show that the map $\phi_p : R \rightarrow R$ given by $\phi_p(a) = a^p$ is a homomorphism. (the *Frobenius homomorphism*)

Proof:
$\phi_p(a + b) = (a + b)^p = a^p + b^p$
The last step is true because R has a prime characteristic.
Therefore, $\phi_p(a + b) = \phi_p(a) + \phi_p(b)$.
$\phi_p(ab) = (ab)^p = a^p b^p = \phi_p(a)\phi_p(b)$
Therefore, ϕ_p is a homomorphism. ■

24. Show that a factor ring of a field is either the trivial ring of one element or is isomorphic to a field.

Proof: Recall that a field only has 2 possible ideals, $\{0\}$ and F, the field itself. Therefore, the possible factor rings are $F/\{0\}$ and F/F. $F/\{0\}$ is isomorphic to F and F/F has a single coset that contains everything and is therefore isomorphic to $\{0\}$. ■

30. An element a of a ring R is *nilpotent* if $a^n = 0$ for some $n \in \mathbb{Z}^+$. Show that the collection of all nilpotent elements in a commutative ring R is an ideal, the *nilradical* of R.

Proof: Let a be nilpotent and let $r \in R$.
$(ar)^n = (ra)^n = r^n \dot{a}^n = 0$
Therefore, $a \cdot r$, $rc\dot{a}$ are nilpotent.
(also need to show that the nilpotents are closed, but that takes a while)