Homomorphisms and Factor/Quotient Rings

Just as we discussed group homomorphisms and factor/quotient groups, there are analogous notions for rings.

Recall that:

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

$$\phi(a+b) = \phi(a) + \phi(b) \text{ and}$$

$$\phi(ab) = \phi(a)\phi(b) \text{ for all } a, b \in R.$$

We saw earlier that $\phi: \mathbb{Z} \to \mathbb{Z}_n$ by $\phi(m) = m\ (mod\ n)$ is a ring homomorphism.

Ex. **Projection homomorphism**: Let $R_1, R_2, \ldots, R_n$ be rings for each i, the map:

$$\pi_i: R_1 \times R_2 \times \ldots \times R_n \to R_i$$

$$\pi_i(r_1, r_2, \ldots, r_n) = r_i$$

is a homomorphism. This homomorphism projects an element in $R_1 \times R_2 \times \ldots \times R_n$ on to its i^{th} component.

π_i is a homomorphism because addition and multiplication in $R_1 \times R_2 \times \ldots \times R_n$ are defined componentwise. For example:

$$\begin{aligned}\pi_i((r_1, r_2, \ldots, r_n) + (s_1, s_2, \ldots, s_n)) &= \pi_i(r_1 + s_1, r_2 + s_2, \ldots, r_n + s_n) \\ &= r_i + s_i \\ &= \pi_i(r_1, r_2, \ldots, r_n) + \pi_i(s_1, s_2, \ldots, s_n),\end{aligned}$$

for any $(r_1, \ldots, r_n), (s_1, \ldots, s_n) \in R_1 \times \ldots \times R_n$.

Theorem: Let ϕ be a homomorphism of a ring R into a ring R'.

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 $\phi[R]$.

Proof: 1. and 2. follow from the theorem on pages 5-6 of the section called Group Homomorphisms (which I'll refer to as the Group Homomorphism theorem), since ϕ is a group homomorphism on $(R, +)$.

For 3. and 4., by the Group Homomorphism theorem, $\phi[S, +]$ is a subgroup of R' and $\phi^{-1}[S', +']$ is a subgroup of R. Thus we only need to show that $\phi[S]$ and $\phi^{-1}[S']$ are closed under multiplication.

3. If $\phi(x_1), \phi(x_2) \in \phi[S]$ then $\phi(x_1)\phi(x_2) = \phi(x_1 x_2) \in \phi[S]$
4. If $x_1, x_2 \in \phi^{-1}[S']$ then $\phi(x_1 x_2) = \phi(x_1)\phi(x_2) \in \phi[S]$ so $x_1 x_2 \in \phi^{-1}[S']$.

For 5. Notice that :

$$\phi(x) = \phi(1x) = \phi(1)\phi(x)$$

$$\phi(x) = \phi(x1) = \phi(x)\phi(1)$$

So $\phi(1)$ is unity for $\phi[R]$.

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

$\phi^{-1}[0'] = \{r \in R \mid \phi(r) = 0'\}$ is the **kernel of ϕ**, denoted $\ker(\phi)$.

This $\ker \phi$ is the same as the kernel of the group homomorphism of $(R, +)$ into $(R', +')$ given by ϕ.

Ex. Let $\phi: \mathbb{Z} \to \mathbb{Z}_{12}$ by $\phi(m) = m\ (mod\ 12)$. Find $\ker(\phi)$.

$$\ker(\phi) = \{m \in \mathbb{Z} \mid m\ (mod\ 12) = 0\}$$

$$= \{\ldots - 24, -12, 0, 12, 24, \ldots\} = 12\mathbb{Z}$$

Ex. Consider the ring $F = \{constant\ functions\ from\ \mathbb{R} \to \mathbb{R}\}$ and the evaluation homomorphism $\phi_2: F \to \mathbb{R}$ by $\phi_2(f) = f(2)$. Find $\ker(\phi)$.

$\phi_2(f) = 0 \Longrightarrow f(2) = 0$. But f is a constant function so

$$\ker(\phi) = \{f(x) = 0\}.$$

Ex. Consider the subring $S' = \{0,4,8\} \subseteq \mathbb{Z}_{12}$. Using the homomorphism $\phi(m) = m\ (mod\ 12)$, of $\mathbb{Z}$ onto $\mathbb{Z}_{12}$, find $\phi^{-1}[S']$.

$$\phi^{-1}(0) = 12\mathbb{Z},$$

$$\phi^{-1}(4) = \{\ldots - 20, -8, 4, 16, 28, \ldots\} = 4 + 12\mathbb{Z}$$

$$\phi^{-1}(8) = \{\ldots - 16, -4, 8, 20, 32, \ldots\} = 8 + 12\mathbb{Z}$$

$$\Longrightarrow \phi^{-1}\{0,4,8\} = \{\ldots, -12, -8, -4, 0, 4, 8, 12 \ldots\} = 4\mathbb{Z}.$$

If R has unity 1, then $\phi(1)$ is unity for $\phi[R]$, but not necessarily for R'.

Ex. Let $\phi: \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ by $\phi(x) = (x, 0)$. ϕ is a homomorphism and $\phi(1) = (1,0)$ which is unity for $\phi[\mathbb{Z}] = \mathbb{Z} \times \{0\}$, but $(1,1)$ is unity for $\mathbb{Z} \times \mathbb{Z}$.

Analogous to our theorem for kernels of group homomorphism we have:

Theorem: Let $\phi: R \to R'$ be a ring homomorphism and let $H = \ker(\phi)$. Let $a \in R$. Then $\phi^{-1}[\phi(a)] = a + H = H + a$, where $a + H = H + a$ is the coset containing a of the commutative additive group $H, +$.

Ex. Let $\phi: \mathbb{Z} \to \mathbb{Z}_{12}$ by $\phi(m) = m \ (mod\ 12)$. Find $\phi^{-1}[\phi(28)]$ and $\phi^{-1}[\phi(17)]$.

$$\phi^{-1}[\phi(28)] = \phi^{-1}\big(28\ (mod\ 12)\big) = \phi^{-1}(4) = 4 + 12\mathbb{Z}.$$

$$\phi^{-1}[\phi(17)] = \phi^{-1}\big(17\ (mod\ 12)\big) = \phi^{-1}(5) = 5 + 12\mathbb{Z}.$$

Corollary: A ring homomorphism $\phi: R \to R'$ is a 1-1 map, if, and only if, $\ker \phi = \{0\}$.

We can now develop the analogue to factor/quotient groups, i.e. factor/quotient rings.

Theorem: 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 given by : The sum of the two cosets is defined by:

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

and the product of the cosets is defined by:

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

Also, the map $\tau: R/H \to \phi[R]$ defined by:

$$\tau(a + H) = \phi[a]$$

is an isomorphism.

Ex. Let $\phi: \mathbb{Z} \to \mathbb{Z}_n$ by $\phi(m) = m\ (mod\ n)$, $\mathrm{H} = \ker(\phi) = n\mathbb{Z}$.

By the previous theorem, $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$ as a ring by:

$$\phi(a + \{\dots, -3n, -2n, -n, 0, n, 2n, 3n, \dots\}) = a$$

where $0 \leq a < n - 1$.

Ex. Show that $\mathbb{Z}_8/\{0,4\}$ is isomorphic to $\mathbb{Z}_4$.

Consider the homomorphism:

$$\phi: \mathbb{Z}_8 \to \mathbb{Z}_4 \text{ by } \phi(m) = m\ (mod\ 4) \text{ where } H = \ker(\phi) = \{0,4\}.$$

By the previous theorem $\mathbb{Z}_8/H \cong \mathbb{Z}_4$; which says $\mathbb{Z}_8/\{0,4\}$ is isomorphic to $\mathbb{Z}_4$.

Theorem: Let H be a subring of the ring R. Multiplication of additive cosets of H is well defined by:

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

if, and only if, $ah \in H$ and $hb \in H$ for all $a, b \in R$ and $h \in H$.

For groups in order for G/H to form a group we need H to be a normal subgroup of G. The analogue for rings follows.

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

$aN \subseteq N$ and $Nb \subseteq N$ for all $a, b \in R$ is an **ideal**.

Ex. $n\mathbb{Z}$ is an ideal in $\mathbb{Z}$ since $n\mathbb{Z}$ is a subgroup and because,

$t(nm) = (nm)t = n(mt) \in n\mathbb{Z}$ for all $t \in \mathbb{Z}$.

Ex. Let F be the ring of all functions $f: \mathbb{R} \to \mathbb{R}$. Let C be the subring of F of all constant functions. Is C an ideal of F?

No! In order for C to be an ideal of F we would need:

$$f \cdot c \in C, \quad c \cdot f \in C \text{ for all } f \in F \text{ and } c \in C.$$

But, in general $f \cdot c$ is not a constant function so C is not an ideal in F.

So not all subrings are ideals.

Ex. Let F be the ring of functions $f: \mathbb{R} \to \mathbb{R}$. Let N be the subgroup of functions f such that $f(6) = 0$. Is N an ideal?

Yes! Notice that if $g(x) \in F$ and $f(x) \in N$, then if:

$h(x) = g(x)f(x)$ then $h(6) = g(6)f(6) = g(6)(0) = 0.$

And if $j(x) = f(x)g(x)$ then $j(6) = f(6)g(6) = 0\big(g(6)\big) = 0.$

so N is an ideal.

Ex. Show that $\{0,4\}$ is an ideal in $\mathbb{Z}_8$.

$a(0) = (0)a = 0,$ for all $a \in \mathbb{Z}_8$.

$a(4) = (4)a \equiv 0$ or 4 for all $a \in \mathbb{Z}_8$.

So $\{0,4\}$ is an ideal in $\mathbb{Z}_8$.

Ex. Show that $S[x] \subseteq \mathbb{Z}[x]$, where $f \in S[x]$ if

$f(x) = a_n x^n + \cdots + a_1 x;$ i.e. $a_0 = 0$ is an ideal in $\mathbb{Z}[x]$.

If $g(x) \in \mathbb{Z}[x]$, then $g(x)f(x) = f(x)g(x)$ and the constant term is 0.

So $S[x]$ is an ideal in $\mathbb{Z}[x]$.

Ex. Show that $S[x] \subseteq \mathbb{Z}[x]$, where $f \in S[x]$ if

$f(x) = a_n x^n + \cdots + a_1 x + a_0;\ a_i \in 2\mathbb{Z}$ is an ideal in $\mathbb{Z}[x]$.

If $g(x) \in \mathbb{Z}[x]$, then $g(x)f(x) = f(x)g(x)$ and the coefficients of the product will be even because an even integer times any integer is even.

So $S[x]$ is an ideal in $\mathbb{Z}[x]$.

Ex. Show that the subring $S \subseteq M_2(\mathbb{R}) = 2 \times 2$ matrices over $\mathbb{R}$, given by

$S = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \middle| \ a \in \mathbb{R} \right\}$ is not an ideal.

To see that S is a subring:

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a+b & 0 \\ 0 & 0 \end{pmatrix}; \quad \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix}$$

$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$. However,

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} x & y \\ w & z \end{pmatrix} = \begin{pmatrix} ax & ay \\ 0 & 0 \end{pmatrix} \notin S.$$

Corollary: Let N be an ideal of a ring R. Then the additive cosets on N form a ring R/N with the binary operations defined by:

$$(a + N) + (b + N) = (a + b) + N \text{ and}$$

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

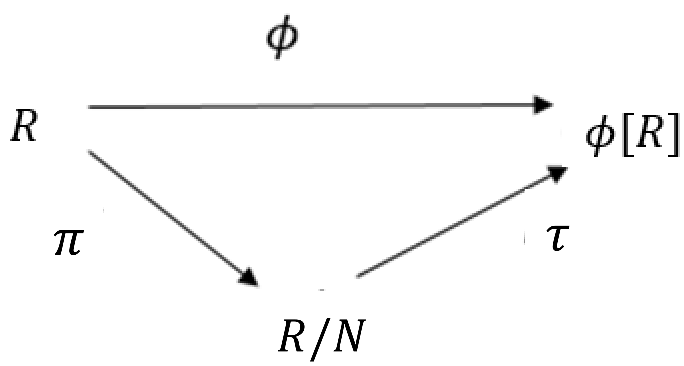
Def. The ring R/N is the **factor ring (or quotient ring) of $\boldsymbol{R}$ by $\boldsymbol{N}$**.

Theorem: Let N be an ideal of a ring R.

Then $\gamma: R \to R/N$ by $\gamma(x) = x + N$ is a ring homomorphism with kernel equal to 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 $\tau: R/N \to \phi[R]$ given by $\tau(x + n) = \phi(x)$ is an isomorphism. If $\pi: R \to R/N$ is the homomorphism given by $\pi(x) = x + N$ then for each $x \in R$, we have $\phi(x) = \tau\,\pi(x)$.



Ex. Find all of the ideals N of $\mathbb{Z}_{12}$. In each case compute $\mathbb{Z}_{12}/N$, that is, find a known ring that is isomorphic to it.

The ideals are subrings of $\mathbb{Z}_{12}, N$ such that $aN \subseteq N$ and $Na \subseteq N$ for all $a \in \mathbb{Z}_{12}$.

The subgroups of $\mathbb{Z}_{12}$ are:

$\mathbb{Z}_{12} = \{0, 1, 2, \ldots, 11\}$ $\quad$ $4\mathbb{Z}_{12} = \{0,4,8\}$

$2\mathbb{Z}_{12} = \{0, 2, 4, 6, 8, 10\}$ $\quad$ $6\mathbb{Z}_{12} = \{0,6\}$

$3\mathbb{Z}_{12} = \{0, 3, 6, 9\}$ $\quad$ $12\mathbb{Z}_{12} = \{0\}$

Notice that $n\mathbb{Z}_{12}$, where n is relatively prime to 12, just gives $\mathbb{Z}_{12}$.

Each of these subrings is an ideal.

For example, if we take $3\mathbb{Z}_{12}$ notice if we multiply an element by $c \in \mathbb{Z}_{12}$:

$$(3a)(c)\ (mod\ 12) = 3(ac)\ (mod\ 12).$$

So $3ac \in 3\mathbb{Z}_{12}$. Multiplication is commutative in $\mathbb{Z}_{12}$ so multiplication on the right also works.

Notice: $\mathbb{Z}_{12}/3\mathbb{Z}_{12} =$ the set of cosets of the form $a + \{0, 3, 6, 9\}$ where $a = 0, 1, \text{or } 2$. Thus $\mathbb{Z}_{12}/3\mathbb{Z}_{12} \cong \mathbb{Z}_3$. Similarly:

$$\mathbb{Z}_{12}/2\mathbb{Z}_{12} \cong \mathbb{Z}_2$$

$$\mathbb{Z}_{12}/4\mathbb{Z}_{12} \cong \mathbb{Z}_4$$

$$\mathbb{Z}_{12}/6\mathbb{Z}_{12} \cong \mathbb{Z}_6$$

$$\mathbb{Z}_{12}/12\mathbb{Z}_{12} \cong \mathbb{Z}_{12}$$

$$\mathbb{Z}_{12}/\mathbb{Z}_{12} \cong \{0\}.$$