Subrings and Ideals

Let R be a ring. Let S be a subset of R. S is called a subring of R iff:

a) With respect to addition, S is a subgroup of R

AND

b) S is closed under multiplication.

Recalling our chapter on subgroups, the above definition could be rewritten:

a) When $a \in S$ and $b \in S$ then $a + b \in S$

b) When $a \in S$ then $-a \in S$

c) When $a \in S$ and $b \in S$ then $a \cdot b \in S$

A subring of a ring is a ring in its own right. However, a lot of odd things can occur. It is possible for R to have a unity, but S doesn't. It is possible for S to have a unity but R doesn't. It is possible for both R and S to have unity elements but they are two different elements!

Every ring has two trivial subrings. The ring itself and the set $\{0\}$.

Example #1

Let $R = Z_{12}$. Let $S = \{0, 3, 6, 9\}$. We already know from previous chapters that S is a subgroup of R with respect to addition. A quick look at a multiplication table confirms that S is a subring of R.

	0	3	6	9
0	0	0	0	0
3	0	9	6	3
6	0	6	0	6
9	0	3	6	9

Note that Z_{12} possesses unity but S does not.

Example # 2

Let R be the set of all reals. Let Q be the subset of all rational numbers. Multiplication and addition are closed on rational numbers. The additive inverse of a rational number is a rational number. $\therefore$ Q is a subring of R. Both R and Q have the same unity 1.

Example # 3

Let R be the ring of 2×2 matrices. Let S be the set of matrices of the form $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$.

Additive Closure: $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a+b & 0 \\ 0 & 0 \end{pmatrix} \in S$

Additive Inverse Closure: $-\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} -a & 0 \\ 0 & 0 \end{pmatrix} \in S$

Multiplicative Closure: $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} \in S$

S is a subring of R. $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the unity of R. However $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \notin S$. Consider the following two products: $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$

and $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$

$\therefore$ S has unity $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. The unity of R is not the same as the unity of the subring S.

Theorem: Let R be a non-trivial ring. Let S be a non-trivial subring of R. If 1 is the unity of R and x is the unity of S where $x \neq 1$, then x is a zero divisor in R.

Proof: Since x is not the unity for R, there exists $r \in S$ such that $r \cdot x \neq r$ or $x \cdot r \neq r$. Without loss of generality we will assume $r \cdot x \neq r$.

However $(r \cdot x) \cdot x = r \cdot (x \cdot x) = r \cdot x$

$\therefore (r \cdot x) \cdot x = r \cdot x$

$\Rightarrow (r \cdot x) \cdot x - r \cdot x = 0$

$\Rightarrow (r \cdot x - r) \cdot x = 0$

Since $r \cdot x \neq r$, $r \cdot x - r$ can not equal 0

$\therefore$ x is a zero divisor in R.

QED

Take note of our last example. $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ was the unity of a subring of the ring of all 2×2 matrices. Note that $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. $\therefore$ $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ is a zero divisor in the ring of all 2×2 matrices. This was guaranteed by our previous theorem.

Definition: Let R be a ring. A subset S of R is said to be an ideal iff:

a) S is a subgroup of R under addition

b) Whenever $r \in R$ and $s \in S$ then sr and rs are elements of S.

We will call this last property Multiplicative Absorption. If an element of S is involved in a product, the result ends up in S.

Example #1

For any ring R, the set $\{0\}$ is an ideal. This can be verified by considering:

Additive Closure: $0 + 0 = 0$
Additive Inverse Closure: $-0 = 0$
Multiplicative Absorption: $r \cdot 0 = 0 \cdot r = 0$ for every $r \in R$

This ideal and the ideal consisting of the set R itself are called trivial ideals.

Example #2

Let R be the ring of all integers. Let S be the set $\{\dots, -4, -2, 0, 2, 4, \dots\}$.
In other words S is the set of all even integers or $S = \{2x \,|\, x \text{ is an integer}\}$.
S is an ideal of R.
Consider: $2x + 2y = 2 \cdot (x + y) \in S$ (Additive Closure)
$-(2x) = 2(-x) \in S$ (Additive Inverse Closure)
$2x \cdot z = z \cdot 2x = 2(xz) \in S$ (Multiplicative Absorption)

Example #3

Let R be the ring of all real numbers. Let S be the set $\{\dots, -4, -2, 0, 2, 4, \dots\}$.
S is no longer an ideal! The problem is absorption. $2 \in S$ and $\pi \in R$. 2π is not an element of S.

Example #4

$\{0, 4\}$ is an ideal in Z_8. You should confirm this by considering carefully each of the three properties that are required for a subset to be an ideal. You have undoubtedly noticed that by the nature of their definitions, every ideal is a subring. However, is every subring an ideal? The answer is no. If you recall, we showed that the set S of matrices of the form $\left(\begin{smallmatrix} a & 0 \\ 0 & 0 \end{smallmatrix}\right)$ are a subring of the ring of all 2×2 matrices. This set S is not an ideal. Consider the product of $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 0 \end{smallmatrix}\right) \in S$ and $\left(\begin{smallmatrix} 4 & 6 \\ 2 & 3 \end{smallmatrix}\right) \in R$.

$$\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 4 & 6 \\ 2 & 3 \end{pmatrix} = \begin{pmatrix} 8 & 12 \\ 0 & 0 \end{pmatrix} \notin S.$$

$\therefore$ S does not absorb multipliers from R and is not an ideal.

In group theory, it turned out that normal subgroups were much more important that subgroups that were not normal. Analogously, ideals are more important in ring theory than subrings that are not ideals.

Let R_1 and R_2 be rings. Let $f : R_1 \rightarrow R_2$ be a surjective function. f is called a ring homomorphism if and only if:

a) $f(a+b) = f(a) + f(b)$ for every a and b in R_1
b) $f(a \cdot b) = f(a) \cdot f(b)$ for every a and b in R_1

In the above equations, the binary operations on the left are from R_1 and the ones on the right are from R_2. You should notice that a ring homomorphism is automatically also a group homomorphism between R_1 and R_2 with respect to their addition operators. Therefore the following results are immediate:

Theorem: If $f : R_1 \rightarrow R_2$ is a ring homomorphism then $f(0) = 0$.

Theorem: If $f : R_1 \rightarrow R_2$ is a ring homomorphism then $f(-x) = -f(x)$ for every x in R_1.

The following theorems require special treatment since neither R_1 nor R_2 need be groups with respect to their multiplication operations.

Theorem: Suppose $f : R_1 \rightarrow R_2$ in a ring homomorphism. If R_1 possesses unity 1 and R_2 possesses unity $1'$ then $f(1) = 1'$

Proof: $f(x \cdot 1) = f(x)$ and $f(1 \cdot x) = f(x)$ for any x in R_1
Also, $f(x \cdot 1) = f(x) \cdot f(1)$ and $f(1 \cdot x) = f(1) \cdot f(x)$ for any x in R_1
$\therefore f(x) = f(x) \cdot f(1)$ and $f(x) = f(1) \cdot f(x)$
Since a binary operator can have only one identity, we can deduce that $f(1) = 1'$.

Theorem: Suppose $f : R_1 \rightarrow R_2$ is a ring homomorphism where R_1 and R_2 are rings with unity. Suppose x is a unit in R_1. Then $f(x)$ is a unit in R_2 and $f(x^{-1}) = [f(x)]^{-1}$

Proof: $f(x \cdot x^{-1}) = f(1) = 1'$ and $f(x^{-1} \cdot x) = f(1) = 1'$
Also, $f(x \cdot x^{-1}) = f(x) \cdot f(x^{-1})$ and $f(x^{-1} \cdot x) = f(x^{-1}) \cdot f(x)$
$\therefore f(x) \cdot f(x^{-1}) = 1'$ and $f(x^{-1}) \cdot f(x) = 1'$
$\therefore f(x^{-1}) = [f(x)]^{-1}$

Definition: Let $f : R_1 \rightarrow R_2$ be a ring homomorphism. The set $K = \{x | x \in R_1$ and $f(x) = 0\}$ is called the kernel of the ring homomorphism.

Theorem: Let $f : R_1 \rightarrow R_2$ be a ring homomorphism. The kernel K of f is an ideal of R_1.

Proof:

Additive Closure

Let $x \in K$ and $y \in K$

$$f(x+y) = f(x) + f(y) = 0 + 0 = 0$$

$$\therefore x + y \in K$$

Additive Inverse Closure

Let $x \in K$

$$f(-x) = -f(x) = -0 = 0$$

$$\therefore -x \in K$$

Multiplicative Absorption

Let $x \in K$ and let $r \in R_1$

$$f(x \cdot r) = f(x) \cdot f(r) = 0 \cdot f(r) = 0$$

$$f(r \cdot x) = f(r) \cdot f(x) = f(r) \cdot 0 = 0$$

$\therefore$ Both $x \cdot r$ and $r \cdot x$ are elements of K

QED

We can see from the above Theorem that ideals play a similar role in ring theory to the role played by normal subgroups in group theory. Further, ideals create cosets in a ring. If R is a ring and I is an ideal, then the set $x + I$ where $x \in R$ is called the coset generated by x and R. Note that addition is used to create cosets. As with groups, two cosets are either equal or disjoint. Further, the collection of all distinct cosets creates a ring itself denoted R/I and called the quotient ring when R is factored by I. All of this leads to a theorem that should be of no surprise. We will not take the time to prove this theorem since we took great pains to prove its analog in group theory.

Theorem: Let $f : R_1 \rightarrow R_2$ be a ring homomorphism. Let K be the kernel of f. R_1/K is isomorphic to R_2.

Subrings and Ideals **Problem Set**

1. Let R be a commutative ring. Let $a \in R$. Let $S = \{x | x \in R \text{ and } xa = 0\}$. Prove that S is an ideal of R.

2. If U and V are ideals of the ring R, show that the set $U + V = \{u + v | u \in U \text{ and v} \in \text{V}\}$ is also an ideal of R.

3. Determine whether the set of matrices of the form $\begin{pmatrix} x & x \\ y & y \end{pmatrix}$ is a subring, ideal, both or neither of the ring of all 2×2 matrices.

4. Repeat exercise #3 for the set of matrices of the form $\begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix}$.

5. Determine whether the function f : reals → reals defined by $f(x) = |x|$ is a ring homomorphism or not.

6. Prove that the integers are a subring of the ring rational numbers but not an ideal.

7. Find an example of a ring R with two ideals I_1 and I_2 such that $I_1 \cup I_2$ is not an ideals.

8. Prove that if R is a ring and I_1 and I_2 are ideals of R then $\text{I}_1 \cap I_2$ is also an ideal.

9. Let S be the set of all matrices of the form $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$. S forms a ring. Prove that the function f : complex number system $\rightarrow S$ defined by $f(x + yi) = \begin{pmatrix} x & y \\ -y & x \end{pmatrix}$ is a ring homomorphism.