Let U be any ideal of R containing the element $(1,0)$. Let $(p,0) \in S$. Then $(p,b) \in R$ for all $b \in \mathbb{Z}$. Since U is an ideal of R, $(1,0) \in U$, $(p,b) \in R \Rightarrow (1,0)(p,b) \in U$ i.e., $(p,0) \in U$. So, $S \subset U$. This shows that S is the smallest ideal of R containing $(1,0)$. Hence S is a principal ideal of the ring R.

<u>Theorem 3.1.16</u> Let R be a commutative ring with unity and $a \in R$. Then the set $Ra = \{ra : r \in R\}$ is a principal ideal of R, generated by a.

Proof: We first prove that Ra is an ideal of R. $0 \in R$ $\Rightarrow 0a \in Ra$, so, $0 \in Ra$. Hence Ra is a non-empty subset of R. Also $a \in Ra$ as $1a = a \in Ra$, 1 being the unity in R.
Let $p, q \in Ra$. So $p = r_1 a$ and $q = r_2 a$ for some $r_1, r_2 \in R$

Then $p - q = r_1 a - r_2 a = (r_1 - r_2) a \in Ra$ since $r_1 - r_2 \in R$

Let $r \in R$ and $p = r_1 a \in Ra$. Then $rp = r(r_1 a) = (rr_1)a \in Ra$ since $rr_1 \in R$. Also $pr \in Ra$, since R is a commutative ring. This proves that Ra is an ideal of R.

To prove Ra is a principal ideal of R and $Ra = \langle a \rangle$, we are to prove that Ra is the smallest ideal of R containing the element a.

Let U be any ideal of R containing the element a and let $ra \in Ra$ for some $r \in R$. Since U is an ideal of R, $r \in R$, $a \in U \Rightarrow ra \in U$. So $ra \in Ra \Rightarrow ra \in U$. So, $Ra \subseteq U$. This proves that Ra is the smallest ideal of R containing the element a. So Ra is the principal ideal generated by a.

Note 3.1.17 If R be a commutative ring (without unity) and $a \in R$, then Ra is an ideal of R but $a \notin Ra$ and therefore it is not the principal ideal of R generated by the element a.

Scanned with CamScanner

For example, in the ring $R = (2\mathbb{Z}, +, \cdot)$, $4 \in R$. The set $S = \{4m : m \in 2\mathbb{Z}\}$ $= \{0, \pm 8, \pm 16, \ldots\}$ is an ideal of R. It is not the principal ideal $\langle 4 \rangle$. Note that S is the principal ideal $\langle 8 \rangle$ of $(\mathbb{Z}, +, \cdot)$

Definition 3.1.18 (Principal ideal Ring) A ring is said to be a principal ideal ring if every ideal of the ring is a principal ideal.

Examples: 1. The ring $(\mathbb{Z}, +, \cdot)$ is a principal ideal ring.

Proof: Let U be an ideal of the ring $\mathbb{Z}$

Case 1 $U = \{0\}$, the null ideal. Then U is the principal ideal $\langle 0 \rangle$.

Case 2 $U \neq \{0\}$. Let $a \in U$ and ~~as~~ $a \neq 0$. Since U is an ideal, $-a \in U$. So, U contains a positive integer. Let m be the least positive integer in U. Such an m exists, by the well ordering property of the set $\mathbb{N}$ of all ~~natural~~ natural numbers. Let p be an arbitrary element of U. By division algorithm, there exist integers q and r such that $p = mq + r$ where $0 \leq r < m$ ...(i)

Since U is an ideal of the ring $\mathbb{Z}$, $m \in U$, $q \in \mathbb{Z} \Rightarrow mq \in U$ and $p \in U$, $mq \in U \Rightarrow p - mq \in U$. So, $p - mq = r \in U$. Since m is the least positive integer in U, it follows from (i) that $r = 0$

Consequently, $p = mq$, where $q \in \mathbb{Z}$. Thus every element of U is of the form mz, where $z \in \mathbb{Z}$. Since ring $\mathbb{Z}$ is a commutative ring with unity, the set $\{mz : z \in \mathbb{Z}\}$ is a principal ideal $\langle m \rangle$. So every ideal in the ring $\mathbb{Z}$ is a principal ideal. So, the ring $\mathbb{Z}$ is a principal ideal ring. ~~Actually~~, Here $m\mathbb{Z} = \{mz : z \in \mathbb{Z}\}$.

2. The ring $\mathbb{Z}_n$ is a principal ideal ring

Proof: Let U be an ideal of the ring $\mathbb{Z}_n$.

If U be the null ring $\{\bar{0}\}$ then $U = \langle \bar{0} \rangle$ and it is a principal ideal

If $U \neq \{\bar{0}\}$, let m be the least positive integer such that $\bar{m} \in U$

Let $\bar{a} \in U$. By division algorithm, there exist q and r such that $a = mq + r$, $0 \leq r < m$, $0 \leq q < n$ (Such a q is possible)

So, $\bar{a} = \bar{m}\bar{q} + \bar{r}$ or, $\bar{a} - \bar{q}\bar{m} = \bar{r}$. Since U is an ideal, $\bar{m} \in U, \bar{q} \in \mathbb{Z}_n \Rightarrow \bar{q}\bar{m} \in U$. As $\bar{a} \in U$, $\bar{q}\bar{m} \in U$

So, $\bar{a} - \bar{q}\bar{m} = \bar{r} \in U$. Since m is the least positive integer such $\bar{m} \in U$, it follows from (i) that $r = 0$. So, $\bar{r} = 0$

Consequently, $\bar{a} = \bar{q}\bar{m}$ for some $\bar{q} \in \mathbb{Z}_m$. Thus every element of U is of the form $\bar{q}\bar{m}$, where $\bar{q} \in \mathbb{Z}_n$. Since the ring $\mathbb{Z}_n$ is a commutative ring with unity, the set $\{\bar{q}\bar{m} : \bar{q} \in \mathbb{Z}_n\}$ is a principal ideal $\langle \bar{m} \rangle$ by Theorem 3.1.16.

So, every ideal in the ring $\mathbb{Z}_n$ is a principal ideal and therefore the ring $\mathbb{Z}_n$ is a principal ideal ring.

~~Definition 3.1.19 (Prime ideal in a ring): In a ring R, $R \neq \{0\}$ an ideal $P \neq R$ is said to be a prime ideal if for $a, b \in R$, $ab \in P$ implies either $a \in P$ or $b \in P$~~

Definition 3.1.19 (Prime ideal in a ring). Let R be a ring such that $R \neq \{0\}$. A proper ideal P of R is called a prime ideal if for $a, b \in R$, $ab \in P$ implies either $a \in P$ or $b \in P$.

Example: 1. The null ideal $\{0\}$ of $\mathbb{Z}$ is a prime ideal. As $ab = 0 \Rightarrow a = 0$ or $b = 0$.

Example: 2. The ideal $2\mathbb{Z}$ in the ring $\mathbb{Z}$ is a prime ideal.

Let $ab \in \mathbb{Z}$ for some $a, b \in \mathbb{Z}$. $ab \in 2\mathbb{Z} \Rightarrow ab = 2m$ for some integer m. This implies 2 is a divisor of ab and

This again implies either 2 is a divisor of a or 2 is a divisor of b.

2 is a divisor of a implies $a \in 2\mathbb{Z}$, 2 is a divisor of b

Scanned with CamScanner

implies ~~$a \in 2\mathbb{Z}$~~ $b \in 2\mathbb{Z}$. This proves that $2\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$.

2. The ideal $4\mathbb{Z}$ in the ring $2\mathbb{Z}$ is not a prime ideal as $2.2 \in 4\mathbb{Z}$ but $2 \notin 4\mathbb{Z}$

Prime ideals in the ring $\mathbb{Z}$:

The prime ideals in the ring $\mathbb{Z}$ are the ideals $p\mathbb{Z}$, where p is either 0 or a prime.

Proof: Let $ab \in p\mathbb{Z}$ for some $a, b \in \mathbb{Z}$ where p is a prime. Then $ab = pm$ for some integer m. So, p is a divisor of ab. This implies either p is a divisor of a or p is a divisor of b.

p is a divisor of a implies $a \in p\mathbb{Z}$, p is a divisor of b implies $b \in p\mathbb{Z}$. So, $ab \in p\mathbb{Z}$ implies either $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$. This proves that $p\mathbb{Z}$ is a prime ideal in the ring $\mathbb{Z}$. When $p = 0$ $p\mathbb{Z} = \{0\}$ is a prime ideal.

Conversely, let P be a ~~prime~~ prime ideal and $P \neq \{0\}$. Since every ideal in the ring is a principal ideal, $P = p\mathbb{Z}$ for some positive integer p. Since $P \neq \mathbb{Z}$, $p \neq 1$. Let p be a composite number. Then $p = uv$ for some integers u, v satisfying $1 < u < p$, $1 < v < p$. Since P is a prime ideal and ~~$p = uv \in p\mathbb{Z} = P$ implies either $u \in P$ or~~ $p = uv \in P$ implies either $u \in P$ or $v \in P$, i.e., either $u \in p\mathbb{Z}$ or $v \in p\mathbb{Z}$. $u \in p\mathbb{Z} \Rightarrow p \mid u$, a contradiction. $v \in p\mathbb{Z} \Rightarrow p$ divides v, a contradiction. So, p is a prime.

If $P = \{0\}$ then $P = p\mathbb{Z}$ where $p = 0$. This completes the proof.

Scanned with CamScanner