

Remark 3.5 (1) The unital assumption in Theorem 3.4(2) is unnecessary. Indeed let $R = \mathbb{Z}_3$ with trivial ring structure. It is easy to see that R has no nontrivial ideals, but the set

$$I = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in R \right\}$$

is a nontrivial ideal of $M_2(R)$.

(2) If R is a division ring, $M_n(R)$ has nontrivial left and right ideals for $n > 1$ as seen in Example 3.2(4)

Proposition 3.6 Let $I_j \subseteq R$ be a family of right ideals for $j \in J$. Then $I = \bigcap_{j \in J} I_j$ is a right ideal in R .

Proof. Since $0 \in I_j \forall j \in J$, we have that $0 \in I$. Let $a, b \in I$ and $r \in R$. Then $a, b \in I_j \forall j \in J$ and so $a - b \in I_j$ and $ar \in I_j \forall j \in J$. Hence $a - b \in I$ and $ar \in I$ and so I is a right ideal in R . \square

Proposition 3.6 holds when we replace "right" by "left" or "two-sided".

Definition 3.7. (1) Let $S \subseteq R$ be a subset. The set

$$(S)_r = \bigcap_{\substack{I \subseteq R \\ I \text{ right ideal}}} I$$

is the smallest (with respect to \subseteq) right ideal of R containing S and is called the right ideal generated by S . If $S = \{a_1, \dots, a_m\}$ is finite, then we write $(S)_r = (a_1, \dots, a_m)_r$.

(2) A right ideal $I \subseteq R$ is called finitely generated if $I = (a_1, \dots, a_m)$ for some $a_1, \dots, a_m \in R$ and it is called principal if $I = (a)$ for some $a \in R$.

Similarly we define the corresponding notions and notation for left and two-sided ideals.

Proposition 3.8. Let $a \in R$. Then $(a)_r = aR$, $(a)_l = Ra$ and $(a) = RaR$, where

$$aR := \{ar + ua \mid r \in R, u \in \mathbb{Z}\},$$

$$Ra := \{ra + ua \mid r \in R, u \in \mathbb{Z}\},$$

$$RaR := \left\{ \sum_{j \in \mathbb{S}} r_j a s_j + ra + as + ua \mid |\mathbb{S}| < \infty, r_j, s_j \in R, u \in \mathbb{Z} \right\}.$$

If moreover R is unital, then

$$aR = \{ar \mid r \in R\},$$

$$Ra = \{ra \mid r \in R\},$$

$$RaR = \left\{ \sum_{j \in \mathbb{S}} r_j a s_j \mid |\mathbb{S}| < \infty, r_j, s_j \in R \right\}.$$

Proof. Exercise.

Definition 3.9. A ring in which every ideal is principal is called a principal ideal ring (PIR). A commutative integral domain with unity that is a PIR is called a principal ideal domain (PID).

Similarly we define principal right and principal left ideal rings.

Example 3.10 \mathbb{Z} is a PID. Indeed, let $I \subseteq \mathbb{Z}$ be an ideal. If $I = (0)$, we are done. Otherwise there exists a smallest positive integer n in I . Now let $m \in I$. Then there exist $q \in \mathbb{Z}$ and $0 \leq r < n$ such that $m = qn + r$. Then $r = m - qn \in I$ and minimality of n implies $r = 0$. Hence $m = qn$ and so $I = (n)$. Similarly if F is a field, then $F[X]$ is a PID.

Let $I \subseteq R$ be an ideal. For $a, b \in R$ define $a \equiv b \pmod{I}$ if $a - b \in I$.

Then \equiv is an equivalence relation in R (exercise). For $a \in R$ we denote by \bar{a} the equivalence class containing a , that is $\bar{a} = \{b \in R \mid a \equiv b \pmod{I}\} = \{b \in R \mid a - b \in I\}$. We also set $a + I := \{a + x \in R \mid x \in I\}$. We claim that $\bar{a} = a + I$. Indeed:

- If $b \in \bar{a}$, then $a - b \in I \xrightarrow{I \text{ ideal}} b - a \in I$. Hence $b = a + (b - a) \in a + I$ and so $\bar{a} \subseteq a + I$.
- If $a + x \in a + I$, then $x \in I \xrightarrow{I \text{ ideal}} -x \in I$. Hence $a - (a + x) = -x \in I$ and so $a + x \in \bar{a}$. We conclude that $a + I \subseteq \bar{a}$.

Let $R/I := \{\bar{a} \mid a \in R\}$. For $\bar{a}, \bar{b} \in R/I$ we define

$$\bar{a} + \bar{b} := \overline{a + b}, \quad \bar{a} \cdot \bar{b} := \overline{a \cdot b}.$$

These are well-defined. Indeed, if $\bar{a} = \bar{c}$, $\bar{b} = \bar{d}$, then $a - c \in I$, $b - d \in I$. Hence $(a + b) - (c + d) = (a - c) + (b - d) \in I$ and so $\overline{a + b} = \overline{c + d}$. Similarly for multiplication. One may also see quite straightforwardly that the ring axioms are satisfied (see page 184 in book) and so R/I becomes a ring called the quotient ring modulo I .

Remark 3.11. (1) If R is unital respectively commutative, then R/I is unital respectively commutative.

(2) If $I = R$, then R/R is the zero ring. If $I = (0)$, then R/I can be identified with R via $\bar{a} = a$.

Example 3.12. (1) If $(n) \subseteq \mathbb{Z}$ is an ideal, then $\mathbb{Z}/(n)$ is \mathbb{Z}_n .

(2) Let R be unital and let $I = (X) \subseteq R[X]$. Then

$$R[X]/I = \{\bar{a} \mid a \in R\}$$

can be identified with R . Indeed, since $X \in (X)$ we have $\bar{X} = \bar{0}$ and so for $\overline{P(X)} = \overline{a_0 + a_1 X + \dots + a_n X^n} \in R[X]/I$ we have

$$\begin{aligned} a_0 + a_1 X + \dots + a_n X^n &= \bar{a}_0 + \bar{a}_1 \bar{X} + \dots + \bar{a}_n \bar{X}^n \\ &= \bar{a}_0 + \bar{a}_1 \bar{0} + \dots + \bar{a}_n \bar{0}^n \\ &= \bar{a}_0 + \bar{a}_1 \bar{0} + \dots + \bar{a}_n \bar{0}^n = \bar{a}_0. \end{aligned}$$