Proposition 1.4 Let R be a ring and $r,s,t \in R$. Then the following hold.

(1) $r0 = 0 = 0r$.

(2) $r(-s) = -(rs) = (-r)s$. We denote this simply by $-rs$.

(3) $r(s-t) = rs - rt$ and $(r-s)t = rt - st$.

Proof. (1)
$$\begin{aligned} r0 &= r(0+0) && \text{(zero element)} \\ &= r0 + r0 && \text{(distributivity)} \end{aligned}$$
$$\begin{aligned} \Rightarrow\quad \underbrace{r0 - r0}_{0} &= (r0+r0) - r0 \\ \Rightarrow\quad 0 &= r0 + \underbrace{(r0 - r0)}_{0} && \text{(associativity)} \\ \Rightarrow\quad 0 &= r0 + 0 \\ \Rightarrow\quad 0 &= r0 && \text{(zero element)} \end{aligned}$$
Similarly one shows $0 = 0r$.

(2) Using (1) we have
$$\begin{aligned} 0 &= r0 \\ &= r(s-s) && \text{(additive inverse)} \\ &= rs + r(-s) && \text{(distributivity)} \end{aligned}$$
$$\begin{aligned} \Rightarrow\quad -(rs) &= (rs + r(-s)) + (-(rs)) \\ \Rightarrow\quad -(rs) &= (r(-s) + rs) + (-(rs)) && \text{(commutativity)} \\ \Rightarrow\quad -(rs) &= r(-s) + \underbrace{(rs + (-(rs)))}_{0} && \text{(associativity)} \\ \Rightarrow\quad -(rs) &= r(-s) + 0 \\ \Rightarrow\quad -(rs) &= r(-s) && \text{(zero element).} \end{aligned}$$
Similarly one shows $-rs = (-r)s$.

(3)
$$\begin{aligned} r(s-t) &= rs + r(-t) && \text{(distributivity)} \\ &= rs - rt && \text{(part (2))} \end{aligned}$$
Similarly $(r-s)t = rt - st$. $\square$

Let R be a ring and $r \in R$. Let $n \in \mathbb{Z}$. We set

$$nr := \begin{cases} \underbrace{r + \dots + r}_{n \text{ times}}, & \text{if } n > 0, \\ 0, & \text{if } n = 0, \\ \underbrace{(-r) + \dots + (-r)}_{-n \text{ times}}, & \text{if } n < 0, \end{cases}$$

and

$$r^n := \begin{cases} \underbrace{r \cdots r}_{n \text{ times}}, & \text{if } n > 0, \\ 1, & \text{if } n = 0 \text{ and } R \text{ is unital}, \\ \underbrace{r^{-1} \cdots r^{-1}}_{-n \text{ times}}, & \text{if } n = 0 \text{ and } r \text{ is a unit.} \end{cases}$$

<u>Proposition 1.5</u> Let $n, m \in \mathbb{Z}$ and $r, s \in R$. The following hold.

(1) $(n+m)r = nr + mr$,

(2) $n(mr) = (nm)r$,

(3) $(nr)(ms) = (nm)(rs) = (mr)(ns)$.

Moreover, the following also hold whenever the respective powers are defined.

(4) $r^n r^m = r^{n+m}$,

(5) $(r^n)^m = r^{nm}$.

<u>Proof.</u> Exercise. $\square$

<u>Definition 1.6.</u> Let R be a ring.

(1) We say that R is an <u>integral domain</u> if for all $r, s \in R$ we have that $rs = 0$ implies $r = 0$ or $s = 0$.

(2) We say that R is a <u>division ring</u> if R is unital with $1 \neq 0$ and for all $r \in R \setminus \{0\}$ we have that r is a unit.

(3) We say that R is a <u>field</u> if R is a commutative division ring.

Note: Field $\Rightarrow$ division ring $\overset{\text{(Prop 2.20)}}{\Longrightarrow}$ integral domain.

Example 1.7 (1) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields. $\mathbb{Z}$ is not a division ring but is an integral domain.
(2) $\mathbb{Z}_n$ is a field if and only if n is a prime number (exercise).
Let R be a nonzero ring
(3) If $n>1$, then $M_n(R), U_n(R), L_n(R)$ are not integral domains.
(4) $R[X]$ is not a division ring. $R[X]$ is an integral domain if and only if R is.