

Definition. A subring of a commutative ring R is a subset S of R that is a ring in its own right, with the addition and multiplication on S being the same as the addition and multiplication on R and with the multiplicative identity element in S being the same as the multiplicative identity element in R .

Note. If S is a subring of a commutative ring R , then the additive identity in S is the same as the additive identity in R . This fact is proven along the way, in the proof of the following proposition.

Proposition. A subset S of a commutative ring R is a subring of R if and only if all of the following conditions are met:

- (i) $1_R \in S$, where 1_R denotes the multiplicative identity in R .
- (ii) For all $a, b \in S$, $a - b \in S$.
- (iii) For all $a, b \in S$, $ab \in S$.

Proof. Let R be a commutative ring, and let S be a subset of R .

First we show that if S is a subring of R then the three conditions are met.

Suppose S is a subring of R . Then it has a multiplicative identity, 1_S , and by the definition of a subring, $1_S = 1_R$, where 1_R denotes the multiplicative identity in R . Thus $1_R \in S$, proving (i).

Now let $a, b \in S$. Since S is a commutative ring there is a binary operation $+: S \times S \rightarrow S$, and since S is a subring of R , this addition agrees with the addition defined on R . In particular, this means that S is closed under addition. Further, there is an additive inverse for b in S , since S is a ring, and since additive inverses are unique in R , it is the same as $-b$ in R . Thus $a - b = a + (-b) \in S$, proving (ii).

Similarly, there is a binary operation $\times: S \times S \rightarrow S$ that agrees with the multiplication defined on R . Thus S is closed under multiplication, proving (iii).

Next we show that if S satisfies the three enumerated conditions, then it is a subring of R .

To show that S is a subring of R , we need to show that S is a commutative ring in its own right, with the addition and multiplication on S being defined as the addition and multiplication on R .

By (i), S is nonempty, since $1_R \in S$. We need to show that the addition and multiplication from R give rise to binary operations on S . Certainly addition and multiplication are functions on $S \times S$; we only need to show that the target for each is S , i.e. that S is closed under the addition and multiplication coming from R . Condition (iii) is closure under multiplication. We will prove closure under addition after proving the two existence axioms for addition.

Existence of additive identity: Since S is nonempty, we may take $a \in S$. By (ii), $a - a \in S$. Thus $0_R \in S$, since $a - a = 0_R$. We claim that 0_R is an additive identity for S . For any $s \in S$, $0_R + s = s$, since $s \in R$ and since 0_R is the additive identity in R . Thus 0_R is an additive identity for S . Since the additive identity for a ring is *unique*, 0_R is *the* additive identity for S . Since 0_R is the additive identity for S as well as R , we now denote it simply as 0.

Existence of additive inverses: Take any $a \in S$. Then, by (ii) $0 - a \in S$. But $0 - a = 0 + (-a)$, where $-a$ is the additive inverse of a in R . Thus we have shown $-a \in S$. Clearly, $a + (-a) = 0$, so $-a$ is an additive identity for a in S .

Closure under addition: Take any $a, b \in S$. Then $-b \in S$, and $-(-b) = b$, since if $-b$ is an additive inverse for b , then b is an additive inverse for $-b$. Thus, $a + b = a - (-b) \in S$ by (ii).

Commutativity of addition: Take any $a, b \in S$. Then $a + b \in S$ (by closure under addition) and, since $a, b \in R$, we have $a + b = b + a$, by commutativity of addition in R .

Associativity of addition: Take any $a, b, c \in S$. Then, since $a, b, c \in R$, $a + (b + c) = (a + b) + c$, and closure ensures that these sums are in S .

Existence of multiplicative identity: Take any $a \in S$. Since $1_R \in S$, $1_R \cdot a \in S$ by (iii) and $1_R \cdot a = a$, since multiplication in S is the same as multiplication in R . Thus 1_R is a multiplicative identity in S as well as R . We now denote it simply as 1.

Commutativity of multiplication: Take any $a, b \in S$. Then $ab \in S$, since S is closed under multiplication, and, since $a, b \in R$, $ab = ba$, by commutativity of multiplication in R .

Associativity of multiplication: Take any $a, b, c \in S$. Since $a, b, c \in R$, $a(bc) = (ab)c$ in R , and since S is closed under multiplication $a(bc) = (ab)c$ in S .

Distributivity: Take any $a, b, c \in S$. Since $a, b, c \in R$, $a(b + c) = ab + ac$ in R , and since S is closed under addition and multiplication, $a(b + c) = ab + ac$ in S . □

Note. We say that distributivity and commutativity and associativity of addition and multiplication are *inherited* from R , because they follow readily from the fact that $S \subset R$.