Subrings

Definition

Let R be a ring. To say that R' is a *subring* of R, denoted $R' \leq R$, means:

1). $R' \subseteq R$

2). R' is a ring under the induced operations

$R' < R$ means R' is a subring of R but $R' \neq R$.

Theorem: Subring Test

Let R be a (commutative) ring and let S be a non-empty subset of R. S is a (commutative) subring of R iff the following are true:

1). $\forall\, a, b \in S, a - b \in S$

2). $\forall\, a, b \in S, ab \in S$

Proof

$\Longrightarrow$ Assume $S \leq R$
$\langle S, + \rangle \leq \langle R, + \rangle$
Assume $a, b \in S$
$\langle S, + \rangle$ is a group so $-b \in S$
$a - b \in S$ (closure)
$ab \in S$ (closure)
$\therefore$ 1 and 2 hold.

$\Longleftarrow$ Assume 1 and 2 hold
By the subgroup test, $\langle S, + \rangle \leq \langle R, + \rangle$
$\langle S, \cdot \rangle$ is closed
Associativity is inherited from R
The distributive laws are inherited from R
$\therefore S \leq R$.

Note that proving subrings with unity is more complicated because unity for a subring may differ from unity of its parent ring:

$\mathbb{Z} \times \mathbb{Z}$ is a ring with unity $(1, 1)$
$\mathbb{Z} \times \{0\}$ is a ring with unity $(1, 0)$
$\mathbb{Z} \times \{0\} < \mathbb{Z} \times \mathbb{Z}$, but $(1, 0) \neq (1, 1)$

Theorem

Let R be a ring and let $S = \bigcap_{i \in I} R_i$ where $R_i \leq R$:

$$S \leq R$$

Proof

$\langle S, + \rangle \leq \langle R, + \rangle$
Assume $a, b \in S$
$\forall\, i \in I, a, b \in R_i$
Assume $i \in I$

$a, b \in R_i$
By closure, $ab \in R_i$
$\forall 1 \in I, ab \in R_i$
$ab \in S$

$\therefore S$ is closed under multiplication.

Multiplicative associativity is inherited from R
The distributive laws are inherited from R

$\therefore S \leq R$