Subrings and Ideals

Recall: (rings, commutative and unital)

A ring R is a set endowed with two binary operations "$+$" and "$\cdot$"

$$+: R \times R \to R$$
$$\cdot: R \times R \to R$$

such that

1) $(R, +)$ is an abelian group

2) "$\cdot$" is associative and distributes over "$+$".

R is said to be unital if $\exists$ an element $1_R \in R$ such that

$$1_R \cdot x = x \cdot 1_R = x \quad \forall\, x \in R.$$

R is said to be commutative if

$$x \cdot y = y \cdot x \quad \forall\, x, y \in R.$$

Main Examples of Rings

1) $\mathbb{Z}$ (prototype example of a commutative ring)

2) $K[x]$, polynomials with coefficients in a field K (commutative)

3) $M_n(K)$, the $n \times n$ matrices with entries in a field K. (non commutative if $n > 1$)

Definition: (Subring) Let R be a ring. A nonempty subset S of R is said to be a **subring** of R if S is a ring under the operations of R.

Theorem: (subring test) A nonempty subset S of a ring R is a subring if and only if $\forall\, x, y \in S$

1) $x + y \in S$

2) $-x \in S$ ($-x$ = additive inverse of x)

3) $x \cdot y \in S$.

proof: Just like the proof of the subgroup test.

$\Rightarrow$ trivial

$\Leftarrow$ associativity and distributivity of "$\cdot$" are inherited from R. $\square$

Example 1:

(polynomial subring)

For any field k, let S be the subset of $k[x]$ consisting of only even degree polynomials:

$$S = \left\{ \sum_{i=0}^{n} a_i x^{2i} \;\middle|\; n \in \mathbb{N} \cup \{0\} \right\}$$

Here, we include the zero polynomial.

Check that S is a subring!

Use the subring test

Let $p(x) = \sum_{i=0}^{n} a_i x^{2i} \in S$

$q(x) = \sum_{\ell=0}^{m} b_\ell x^{2\ell} \in S.$

Inverses: $-p(x) = \sum_{i=0}^{n} (-a_i) x^{2i} \in S$

Since the degree of every term is even

Sums: Without loss of generality, suppose $m \geq n$.

Then

$$p(x)+q(x) = \sum_{\ell=0}^{n} (a_\ell + b_\ell) x^{2\ell} + \sum_{\ell=n+1}^{m} b_\ell x^{2\ell}$$

$\in S$ since all powers are even.

products: $p(x) \cdot q(x)$

$$= \sum_{i=0}^{n} \sum_{\ell=0}^{m} (a_i b_\ell) x^{2i+2\ell}$$

$$= \sum_{i=0}^{n} \sum_{\ell=0}^{m} (a_i b_\ell) x^{2(i+\ell)} \in S$$

since all powers are even.

By the subring test, S is a subring!

Example 2: (direct sums) Let R_1 and R_2 be rings with operations abusively both denoted by "+" and "$\cdot$".

Then we define the **direct sum** $R_1 \oplus R_2$ to be the set $R_1 \times R_2$ with operations

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2, y_1 y_2).$$

Then under these operations, $R = R_1 \oplus R_2$ is a ring!

Observation: We have ring-isomorphic copies of R_1 and R_2 in R given by

$R_1 \times \{0_{R_2}\}$ and

$\{0_{R_1}\} \times R_2$, respectively.

We can see these are subrings using the subring test, but more is true!

Let $(x, 0_{R_2}) \in R_1 \times \{0_{R_2}\}$.

Then if $(y, z) \in R$,

$$(y, z) \cdot (x, 0_{R_2}) = \underbrace{(y \cdot x, 0_{R_2})}_{\in R_1 \times \{0_{R_2}\}}.$$

$$(x, 0_{R_2}) \cdot (y, z) = (x \cdot y, 0_{R_2})$$

$$\in R_1 \times \{0_{R_2}\}$$

Similarly,

$(0_{R_1}, x) \cdot (y, z)$ and

$(y, z) \cdot (0_{R_1}, x)$ are

elements of $\{0_{R_1}\} \times R_2$.

These subrings absorb other

elements of R under multiplication.

Note: the subring given in Example 1 does not have this property, since multiplication of an element of S by a monomial of odd degree kicks us out of S:

$$(x^2+1)\cdot x = x^3+x \notin S.$$

Definition: (Ideals, left and right)

A subring S of a ring R is called a **left ideal** if $x \cdot y \in S$ $\forall$ $x \in R$, $y \in S$.

Similarly, S is a **right ideal** if $y \cdot x \in S$ $\forall$ $x \in R$, $y \in S$.

If S is both a left and a right ideal, we say S is an **ideal**. We then usually denote ideals by I.

Example 3: (Ideals in $\mathbb{Z}$) If I is an ideal in $\mathbb{Z}$, then, in particular, $I \leq \mathbb{Z}$ under addition. Since $(\mathbb{Z}, +)$ is cyclic, we know that $(I, +)$ must be cyclic as well. Therefore,

$\boxed{I = \langle n \rangle}$ for some

$n \in \mathbb{N} \cup \{0\}$.

Example 4: (polynomial ideal) In $K[x]$, we can take an ideal

$$I = \left\{ \sum_{\boxed{i=1}}^{n} a_i x^i \;\middle|\; n \in \mathbb{N} \right\}$$

I is all polynomials without a constant coefficient. You can check, using the subring test, that I is a subring. Since $K[x]$ is commutative, we only need to show I is a left ideal.

Let $q(x) = \sum_{\ell=0}^{m} b_\ell x^\ell \in K[x]$.

Then if $p(x) = \sum_{i=1}^{n} a_i x^i \in I$,

$q(x) \cdot p(x)$

$$= \sum_{\ell=0}^{m} \sum_{i=1}^{n} (a_i b_\ell) x^{i+\ell} \in I$$

$\geq i \geq 1$

Therefore, I is an ideal.

Note: the zero polynomial is in I
by choosing $a_i = 0 \; \forall \; 1 \leq i \leq n$.

This assumes $p(x) \neq 0 \neq q(x)$.

But if either $p(x) = 0$ or $q(x) = 0$,

then $p(x) \cdot q(x) = 0 \in I$.

Theorem: (kernels are ideals) Let

R, S be rings,

$\varphi: R \to S$ a ring

homomorphism:

$$\varphi(x+y) = \varphi(x) + \varphi(y)$$
$$\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$$
$$\forall\ x, y \in R.$$

Then $\ker(\varphi) = \{x \in R \mid \varphi(x) = 0_S\}$

is an ideal of R.

proof: That $\ker(\varphi)$ is a subgroup follows immediately from the characterization for group homomorphisms. $\ker(\varphi) \neq \phi$ since $\varphi(0_R) = 0_S$. It only remains to check that if $x \in R$, $y \in \ker(\varphi)$, $x \cdot y \in \ker(\varphi)$ and $y \cdot x \in \ker(\varphi)$.

$$\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$$
$$= \varphi(x) \cdot 0_S$$
$$= 0_S$$

Similarly,

$$\varphi(y \cdot x) = 0_S.$$

So $\ker(\varphi)$ is an ideal of R.

$\square$

Definition: (simple ring) A ring R is said to be **simple** if R has no proper nontrivial ideals.

Theorem: ($M_n(K)$ is simple for $n>1$)

Let K be a field. Then $M_n(K)$ is a simple ring for all $n>1$.

proof: Extra credit in the case $K=\mathbb{R}$.

$\square$