MATH 415

Modern Algebra I

Lecture 31:
Subrings and ideals.

Subrings

Definition. Suppose R and R_0 are rings. We say that R_0 is a **subring** (or **sub-ring**) of R if R_0 is a subset of R and the operations on R_0 (addition and multiplication) agree with those on R.

Let R be a ring. Given a subset $S \subset R$, we can define addition and multiplication on S by restricting the corresponding operations from R to S. Then S is a subring of R as soon as it is a ring.

Proposition 1 The subset S is a subring if and only if it
(i) contains the zero: $0 \in S$,
(ii) is closed under addition: $x, y \in S \implies x + y \in S$,
(iii) is closed under taking the negative: $x \in S \implies -x \in S$,
(iv) is closed under multiplication: $x, y \in S \implies xy \in S$.

Proposition 2 A subset S of a ring is a subring with respect to the induced operations if and only if it is
(i) nonempty, and
(ii) closed under addition, subtraction and multiplication: $x, y \in S \implies x + y, x - y, xy \in S$.

Proposition 3 A subset S of a ring R is a subring with respect to the induced operations if and only if it is
(i) a subgroup of the additive group R, and
(ii) closed under multiplication: $x, y \in S \implies xy \in S$.

Proposition 4 A subset S of a ring R is a subring with respect to the induced operations if and only if it is
(i) a subgroup of the additive group R, and
(ii) a subsemigroup of the multiplicative semigroup R.

Examples. • $R = \mathbb{Z}$.

Since the additive group $\mathbb{Z}$ is cyclic, any subgroup is also cyclic. The subgroups are the trivial group $\{0\}$ and groups of the form $m\mathbb{Z} = \{mx \mid x \in \mathbb{Z}\}$, where m is a positive integer. All these subgroups are also subrings.

- $R = \mathbb{Z}_n$.

Since the additive group $\mathbb{Z}_n$ is cyclic, any subgroup is also cyclic. The subgroups are the trivial group $\{0\}$ and groups of the form $m\mathbb{Z}_n = \{mx \mid x \in \mathbb{Z}_n\}$, where m is a proper divisor of n. All these subgroups are also subrings.

Remark. If R_0 is a subring of R, then the zero element in R_0 is the same as in R. On the other hand, if R and R_0 are both rings with unity, then the unity in R_0 may not be the same as in R. Indeed, in the ring $\mathbb{Z}_{10}$, the unity is 1, while in its subring $2\mathbb{Z}_{10} = \{0, 2, 4, 6, 8\}$, the unity is 6.

Ideals

Definition. Suppose R is a ring. We say that a subset $S \subset R$ is a **left ideal** of R if

- S is a subgroup of the additive group R,
- S is closed under left multiplication by any elements of R:

$s \in S,\ x \in R \implies xs \in S$.

We say that a subset $S \subset R$ is a **right ideal** of R if

- S is a subgroup of the additive group R,
- S is closed under right multiplication by any elements of R:

$s \in S,\ x \in R \implies sx \in S$.

All left ideals and right ideals of the ring R are also called **one-sided ideals**. A **two-sided ideal** (or simply an **ideal**) of the ring R is a subset $S \subset R$ that is both a left ideal and a right ideal. That is,

- S is a subgroup of the additive group R,
- S is closed under multiplication by any elements of R:

$s \in S,\ x \in R \implies xs,\ sx \in S$.

Basic facts on the ideals

- Any left, right or two-sided ideal is a subring (with respect to the induced operations).

- In a commutative ring, the notions of a left ideal, a right ideal, and a two-sided ideal are equivalent.

- The trivial subring $\{0\}$ is a two-sided ideal (all other ideals are called **nonzero**).

- Any ring is a two-sided ideal of itself (all other ideals are called **proper**).

- In a ring with unity, a one-sided ideal is proper if and only if it does not contain the unity.

- For any element a of a ring R, the set $Ra = \{xa \mid x \in R\}$ is a left ideal (called **principal**).

- For any element a of a ring R, the set $aR = \{ax \mid x \in R\}$ is a right ideal (called **principal**).

Examples of ideals

- $R = \mathbb{Z}$.

The subrings are $\{0\}$ and $m\mathbb{Z} = \{mx \mid x \in \mathbb{Z}\}$, where m is a positive integer. Each of them is a principal ideal.

- $R = \mathbb{Z}_n$.

The subrings are $\{0\}$ and $m\mathbb{Z}_n = \{mx \mid x \in \mathbb{Z}_n\}$, where m is a proper divisor of n. Each of them is a principal ideal.

- $R = \mathbb{Z} \times \mathbb{Z}$.

A subset $\{(m, m) \mid m \in \mathbb{Z}\}$ is a subring but not an ideal. One can show that all ideals are principal.

- $R = R_1 \times R_2$, a direct product of rings.

If I_1 is a left ideal in R_1 and I_2 is a left ideal in R_2, then $I_1 \times I_2$ is a left ideal in $R_1 \times R_2$. In the case R_1 and R_2 are rings with unity, any left ideal is of that form (the same for right ideals).

Examples of ideals

- $R = \mathbb{F}[x]$, polynomials in one variable over a field.

For any polynomial $p(x)$ there is a principal ideal $I_p = p(x)\mathbb{F}[x]$. If $p = 0$ then $I_p = \{0\}$. Otherwise I_p consists of all polynomials divisible by $p(x)$. Conversely, suppose I is a nonzero ideal in $\mathbb{F}[x]$ and let p be a nonzero polynomial with the least degree in I. For any $f \in \mathbb{F}[x]$ we have $f = pq + r$, where $q, r \in \mathbb{F}[x]$ and either $r = 0$ or $\deg(r) < \deg(p)$. If the polynomial f belongs to the ideal I, so does $r = f - pq$. By the choice of p, this implies $r = 0$. It follows that $I = I_p$.

- $R = \mathbb{F}[x, y]$, polynomials in two variables over a field.

Let R_0 be the set of all polynomials in R with no constant term. Elements of R_0 can be written as $xf(x, y) + yg(x, y)$, where $f, g \in \mathbb{F}[x, y]$. It follows that R_0 is an ideal. This ideal is not principal. Indeed, R_0 contains x and y but does not contain 1.