MATH 415

Modern Algebra I

Lecture 21: Subrings and ideals. Factor rings.

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.

Factor space

Let X be a nonempty set and $\sim$ be an equivalence relation on X. Given an element $x \in X$, the **equivalence class** of x, denoted $[x]_\sim$ or simply $[x]$, is the set of all elements of X that are **equivalent** (i.e., related by $\sim$) to x:

$$[x]_\sim = \{y \in X \mid y \sim x\}.$$

Theorem Equivalence classes of the relation $\sim$ form a partition of the set X.

The set of all equivalence classes of $\sim$ is denoted $X/{\sim}$ and called the **factor space** (or **quotient space**) of X by the relation $\sim$.

In the case when the set X carries some structure (algebraic, geometric, analytic, etc.), this structure may (or may not) induce an analogous structure on the factor space $X/{\sim}$.

Factor ring

Let R be a ring. Given an equivalence relation $\sim$ on R, we say that the relation $\sim$ is **compatible** with the operations (addition and multiplication) in R if for any $r_1, r_2, s_1, s_2 \in R$,

$$r_1 \sim r_2 \text{ and } s_1 \sim s_2 \implies r_1+s_1 \sim r_2+s_2 \text{ and } r_1s_1 \sim r_2s_2.$$

If this is the case, we can define operations on the factor space $R/\sim$ by $[r] + [s] = [r + s]$ and $[r][s] = [rs]$ for all $r, s \in R$ (compatibility is required so that the operations are defined uniquely).

Then $R/\sim$ is also a ring called the **factor ring** (or **quotient ring**) of R.

If the ring R is commutative, then so is the factor ring $R/\sim$. If R has the unity 1, then $R/\sim$ has the unity [1].

Question. When is an equivalence relation $\sim$ on a ring R compatible with the operations?

Let R be a ring and assume that an equivalence relation $\sim$ on R is compatible with the operations (so that the factor space $R/\sim$ is also the factor ring).

Since R is an additive group and the relation $\sim$ is compatible with addition, the factor ring $R/\sim$ is a factor group in the first place. As shown in group theory, it follows that

- $I = [0]_\sim$, the equivalence class of the zero, is a normal subgroup of R, and
- $R/\sim = R/I$, which means that every equivalence class is a coset of I, $[r]_\sim = r + I$ for all $r \in R$.

The fact that the subgroup I is normal is redundant here. Indeed, the additive group R is abelian and hence all subgroups are normal.

Lemma The subgroup I is a two-sided ideal in R.

Proof: Let $a \in I$ and $x \in R$. We need to show that $xa, ax \in I$. Since $I = [0]_\sim$, we have $a \sim 0$. By reflexivity, $x \sim x$. By compatibility with multiplication, $xa \sim x0 = 0$ and $ax \sim 0x = 0$. Thus $xa, ax \in I$.

Theorem If I is a two-sided ideal of a ring R, then the factor group R/I is, indeed, a factor ring.

Proof: Let $\sim$ be a relation on R such that $a_1 \sim a_2$ if and only if $a_1 \in a_2 + I$. Then $\sim$ is an equivalence relation compatible with addition, and the factor space $R/\sim$ coincides with the factor group R/I. To prove that R/I is a factor ring, we only need to show that the relation $\sim$ is compatible with multiplication. Suppose $a_1 \sim a_2$ and $b_1 \sim b_2$. Then $a_1 = a_2 + h$ and $b_1 = b_2 + h'$ for some $h, h' \in I$. We obtain $a_1 b_1 = (a_2 + h)(b_2 + h') = a_2 b_2 + (a_2 h' + h b_2 + h h')$. Since I is a two-sided ideal, the products $a_2 h'$, $h b_2$ and $h h'$ are contained in I, and so is their sum. Thus $a_1 b_1 \sim a_2 b_2$.