MATH 415

Modern Algebra I

Lecture 32: Factor rings. Homomorphisms of rings.

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:

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

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 $r_1, r_2, s_1, s_2 \in R$,

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

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 $a_1 b_1 \sim a_2 b_2$.

Homomorphism of rings

Definition. Let R and R' be rings. A function $f : R \to R'$ is called a **homomorphism of rings** if $f(r_1 + r_2) = f(r_1) + f(r_2)$ and $f(r_1 r_2) = f(r_1) f(r_2)$ for all $r_1, r_2 \in R$.

That is, f is a homomorphism of the binary structure $(R, +)$ to $(R', +)$ and, simultaneously, a homomorphism of the binary structure $(R, \cdot)$ to $(R', \cdot)$. In particular, f is a homomorphism of additive groups, which implies the following properties:

- $f(0) = 0$,
- $f(-r) = -f(r)$ for all $r \in R$,
- if H is an additive subgroup of R then $f(H)$ is an additive subgroup of R',
- if H' is an additive subgroup of R' then $f^{-1}(H')$ is an additive subgroup of R,
- $f^{-1}(0)$ is an additive subgroup of R, called the **kernel** of f and denoted $\mathrm{Ker}(f)$.

More properties of homomorphisms

Let $f : R \to R'$ be a homomorphism of rings.

- If H is a subring of R, then $f(H)$ is a subring of R'.

We already know that $f(H)$ is an additive subgroup of R'. It remains to show that it is closed under multiplication in R'. Let $r_1', r_2' \in f(H)$. Then $r_1' = f(r_1)$ and $r_2' = f(r_2)$ for some $r_1, r_2 \in H$. Hence $r_1' r_2' = f(r_1)f(r_2) = f(r_1 r_2)$, which is in $f(H)$ since H is closed under multiplication in R.

- If H' is a subring of R', then $f^{-1}(H')$ is a subring of R.

We already know that $f^{-1}(H')$ is an additive subgroup of R. It remains to show that it is closed under multiplication in R. Let $r_1, r_2 \in f^{-1}(H')$, that is, $f(r_1), f(r_2) \in H'$. Then $f(r_1 r_2) = f(r_1)f(r_2)$ is in H' since H' is closed under multiplication in R'. Hence $r_1 r_2 \in f^{-1}(H')$.

More properties of homomorphisms

- If H' is a left ideal in R', then $f^{-1}(H')$ is a left ideal in R.

We already know that $f^{-1}(H')$ is a subring of R. It remains to show that $r \in R$ and $a \in f^{-1}(H')$ imply $ra \in f^{-1}(H')$. We have $f(a) \in H'$. Then $f(ra) = f(r)f(a)$ is in H' since H' is a left ideal in R'. In other words, $ra \in f^{-1}(H')$.

- If H' is a right ideal in R', then $f^{-1}(H')$ is a right ideal in R.

- If H' is a two-sided ideal in R', then $f^{-1}(H')$ is a two-sided ideal in R.

- The kernel $\mathrm{Ker}(f)$ is a two-sided ideal in R.

Indeed, $\mathrm{Ker}(f)$ is the pre-image of the trivial ideal $\{0\}$ in R'.

More properties of homomorphisms

- If an element $a \in R$ is idempotent in R (that is, $a^2 = a$) then $f(a)$ is idempotent in R'.

Indeed, $(f(a))^2 = f(a^2) = f(a)$.

- If 1_R is the unity in R then $f(1_R)$ is the unity in $f(R)$.

Let $r' \in f(R)$. Then $r' = f(r)$ for some $r \in R$. We obtain $r'f(1_R) = f(r)f(1_R) = f(r \cdot 1_R) = f(r) = r'$ and $f(1_R)r' = f(1_R)f(r) = f(1_R \cdot r) = f(r) = r'$.

- If 1_R is the unity in R and R' is a domain with unity, then either $f(1_R)$ is the unity in R' or else the homomorphism f is identically zero.

If $f(1_R) = 0$ then f is identically zero: $f(r) = f(r \cdot 1_R) = f(r)f(1_R) = f(r) \cdot 0 = 0$ for all $r \in R$. Otherwise $f(1_R)$ is a nonzero idempotent element. We know that in a domain with unity, the only idempotent elements are the zero and the unity.