21-237: Math Studies Algebra I October 26, 2022

Lecture 22 : Rings and their ideals

Lecturer: James Cummings

Scribe: Rajeev Godse

Recall from last lecture:

A **ring** is a set R equipped with 2 binary operations: $+$ and $\times$. The following axioms must hold:

1. $(R, +)$ is an abelian group. 0 is the identity of $(R, +)$, and $-r$ is the inverse of r.
2. $\times$ is associative.
3. $\times$ distributes over $+$ from either side. That is, $a \times (b + c) = (a \times b) + (a \times c)$ and $(a + b) \times c = (a \times c) + (b \times c)$. Equivalently, left and right application of $\times$ with a fixed element is a group homomorphism of $(R, +)$.

1 Examples of rings

(1) $n \times n$ real matrices, usual $+$ and $\times$.

(2) $\mathbb{R}^{\mathbb{R}}$, with pointwise $+$ and $\times$.

(3) $\mathbb{Z}$

(4) $\mathbb{Q}[x]$

2 Morphisms and subobjects

For rings R, S, $\phi : R \to S$ is a **ring homomorphism** if $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$ and $\phi(r_1 r_2) = \phi(r_1)\phi(r_2)$.

Note that if ϕ is a ring HM from $R \to S$, then ϕ is a group HM from $(R, +)$ to $(S, +)$.

If R is a ring, a **subring** of R is a subgroup of $(R, +)$ which is closed under $\times$.

If $\phi : R \to S$ is HM, $\ker(\phi) = \{r \in R : \phi(r) = 0\}$. $\operatorname{im}(\phi) = \phi[R] = \{s \in S : \exists r \in R, \phi(r) = s\}$.

3 Ideals

For ring R, a **left ideal** of R is a subgroup $I \leq (R, +)$ such that for all $a \in R$ and $b \in I$, $ab \in I$. *Not all subrings are ideals*: $\mathbb{Z}$ is a subring of $\mathbb{Z}[x]$, but *not an ideal* (consider $a = x$).

A **right ideal** is the same as a left ideal but instead closed under right multiplication.

A **two-sided ideal** is a left ideal and a right ideal.

Fact: If $\phi : R \to S$ is a ring HM, $\ker(\phi)$ is a 2-sided ideal of R. *Proof*: Let $b \in \ker(\phi), a \in R$. $\phi(ab) = \phi(a)\phi(b) = \phi(a)0 = 0$, so $ab \in \ker(\phi)$, and similarly for ba.

Fact: The ideals of $\mathbb{Z} \equiv$ subgroups of $(\mathbb{Z}, +) \equiv$ subsets of form $n\mathbb{Z}, n \geq 0$.

Proof: Let $G \leq (\mathbb{Z}, +)$, $G \neq 0$. Let n be the least positive number with $n \in G$. Let $a \in G$, $a = qn + r$ where $0 \leq r < n$. $r = a - qn \in G$, but since n is minimal, $r = 0$. So indeed, $a = qn$, and clearly $n\mathbb{Z}$ is contained in the subgroup by closure under group operations, so $G = n\mathbb{Z}$.

If J is a two-sided ideal in ring R, $a, b \in R$, then we say $a \equiv b \bmod J \iff a - b \in J \iff a + J = b + J$.

Quotient rings: Let J be a 2-sided ideal of R.

As $J \leq (R, +)$, form a quotient group $(R/J, +)$. Elements of R/J are cosets $a + J$, $(a + J) + (b + J) = (a + b) + J$.

We *attempt to define*: $(a+J)(b+J) = ab+J$. Why well-defined? Suppose $a+J = a'+J$, $b+J = b'+J$. Then, $a \equiv a' \bmod J$ and $b \equiv b' \bmod J$. $ab - a'b' = a(b - b') + (a - a')b' \in J$ since J is a two-sided ideal.

There are some things to verify:

(A) R/J is a ring.

(B) If $\phi_J : a \mapsto a + J$, ϕ_J is a ring HM.

(C) $\ker(\phi_J) = J$.

In fact, the kernel of any HM turns out to be a two-sided ideal. Easily following is the 1st IM theorem (rings): $\mathrm{im}(\phi) \simeq R/\ker(\phi)$.