Introduction to Rings and Modules

Lecture 2, Monday March 20 2023

Ari Feiglin

2.1 Ideals

Definition 2.1.1:

Suppose R is a ring, then a subset $\varnothing \neq I \subseteq R$ is a **left ideal** if:

(1) $(I, +)$ is a subgroup of $(R, +)$.

(2) For every $a \in I$ and every $r \in R$, $ra \in I$.

If I is closed on the right by multiplication of R then it is a **right ideal**. If I is both a left and right ideal, it is a **bidirectional ideal** (or simply an ideal) and is denoted $I \trianglelefteq R$.

Notice that:

(1) If R is commutative, left ideals, right ideals, and bidirectional ideals are all the same.

(2) Every left or right ideal is a subrng of R (since $(I, \cdot)$ is necessarily a semigroup since multiplication is associative and it is closed), but it may not contain an identity.

(3) If an ideal is also a subring, that is $1_R \in I$, then for every $r \in R$ $r \cdot 1_R = 1_R \cdot r = r \in I$, so $I = R$.

A trivial example of an ideal is the trivial ring $\{0\}$ since $r \cdot 0 = 0 \cdot r = 0$. And another trivial example of an ideal is just R itself.

Example 2.1.2:

If R is a ring and $a \in R$ then $Ra = \{ra \mid r \in R\}$ is the smallest left ideal containing a.

(1) $(Ra, +)$ is a group since $0_R \in Ra$ and if $r_1a, r_2a \in Ra$ then $r_1a + r_2a = (r_1 + r_2)a \in Ra$ and $r_1a + (-r_1)a = (r_1 - r_1)a = 0_R$.

(2) If $r \in R$ then for any $r'a \in R$, $rr'a \in Ra$ so Ra is a left ideal.

(3) If I is a left ideal containing a then for every $r \in R$ we have that $ra \in I$ by the definition of a left ideal, and so $Ra \subseteq I$.

We also called Ra the **left ideal generated by** a. We define aR in a similar fashion, it is also the smallest right ideal containing a and is the **right ideal generated by** a.

Example 2.1.3:

If R is a ring and $a \in R$ then any bidirectional ideal must contain elements of the form ras for $r, s \in R$. But it must also be a group under addition and so it must be closed under addition so it must contain all the elements of the form $\sum_{i=1}^{n} r_i a s_i$ for $r_i, s_i \in R$. This is the smallest group generated by $\{ras \mid r, s \in R\}$. This is a group under addition since $-\sum r_i a s_i = \sum(-r_i)as_i$ and it is by definition closed under addition and contains 0_R. And it is closed under both left and right multiplication so it is a bidirectional ideal.
This is obviously the smallest bidirectional ideal containing a since any bidirectional ideal containing a must contain all elements of the form ras and their sums.

Example 2.1.4:

Take $R = M_n(\mathbb{R})$ and $a = \operatorname{diag}(0, 1, 1, \ldots, 1)$. Then

$$Ra = \left\{ M \begin{pmatrix} 0 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} \;\middle|\; M \in M_n(\mathbb{R}) \right\}$$

If we let m_{ij} be the elements of M then

$$M \cdot a = \begin{pmatrix} 0 & m_{21} & \cdots & m_{n1} \\ \vdots & & \ddots & \vdots \\ 0 & m_{2n} & \cdots & m_{nn} \end{pmatrix}$$

So Ra is the set of all matrices whose first column is 0. Similarly aR is the set of all matrices whose first row is 0.

Example 2.1.5:

If R is a group and $J \trianglelefteq R$ is a bidirectional ideal then $M_n(J) \trianglelefteq M_n(R)$. The ideality of $M_n(J)$ follows simply from the ideality of J. And as it turns out, the converse is true as well: for every bidirectional ideal $I \trianglelefteq M_n(R)$ there exists $J \trianglelefteq R$ such that $M_n(J) = I$. Let J be the set of all $a \in R$ such that a is an element of a matrix in I. Then $I \subseteq M_n(J)$. If $x \in J$ then there exists an $M \in I$ where $x = m_{ij}$. Take A to be the matrix of 0s except for $a_{jj} = 1$ and B the same but $b_{ii} = 1$. Then

$$[BMA]_{ts} = R_t(BM) \cdot C_s(A) = R_t(B) \cdot M \cdot C_s(A)$$

And so if $t \neq i$ or $s \neq j$ then $R_t(B) = 0$ or $C_s(A) = 0$ and this is 0. If $t, s = i, j$ then this is equal to $m_{ij} = x$ and since I is an ideal $BMA \in I$ and BMA is the matrix of 0s except for at index i, j which is x. And so for any

Notice that if $\mathbb{F}$ is a field, and $\{0\} \neq I \trianglelefteq \mathbb{F}$ is an ideal then $a \in I$ and so $a^{-1} \in \mathbb{F}$ so $aa^{-1} = 1 \in I$ and therefore $I = \mathbb{F}$. So fields only have trivial ideals.
An important insight to have with rings is that prime decomposition need not be unique ($p \neq 0, 1$ is prime in R if $p \mid ab$ means $p \mid a$ or $p \mid b$). For example the ring $\left\{a + b\sqrt{-5} \;\middle|\; a, b \in \mathbb{Z}\right\}$ has two decompositions for 6, $2 \cdot 3$ and $(1+\sqrt{-5})(1-\sqrt{-5})$. We will define later what a prime ideal is, and prime ideals do have a notion of unique decompositions.

Definition 2.1.6:

If R is a ring and $a, b \in R$ then:

$$Ra + Rb = \{r_1 a + r_2 b \mid r_1, r_2 \in R\}$$

This is still an ideal since the product of subgroups (sum of abelian subgroups) is itself a subgroup, and this is obviously closed under left multiplication by R. And if $S \subseteq R$ is a subset, then

$$RS = \left\{ \sum_{i=1}^{n} r_i s_i \;\middle|\; n \in \mathbb{N}, r_i \in R, s_i \in S \right\}$$

So if $S = \{a\}$ then $RS = Ra$ and if $S = \{a, b\}$ then $RS = Ra + Rb$. And we similarly define this for right ideals.

Definition 2.1.7:

If R is a commutative ring and $I \trianglelefteq R$ an ideal, then we define

$$\sqrt{I} = \{a \in R \mid \exists n \in \mathbb{N} \colon a^n \in I\}$$

This is called the **radical ideal** of I.

Notice that $I \subseteq \sqrt{I}$, and that this is indeed an ideal:

(1) If $a \in \sqrt{I}$ and $r \in R$ then since $a^n \in I$ we have that $(ra)^n = r^n a^n$ since R is commutative and $r^n \in R$ and $a \in I$ so $(ra)^n \in I$so $ra \in \sqrt{I}$.

(2) If $a \in \sqrt{I}$ then $-a \in \sqrt{I}$ since $-a = (-1)a$ and $\sqrt{I}$ is closed under left multiplication by above.

(3) Suppose $a, b \in \sqrt{I}$ where $a^n, b^m \in I$. Then by the binomial theorem (since it is simple why this holds in commutative rings):

$$(a+b)^{n+m} = \sum_{k=0}^{n} \binom{n+m}{k} a^k \cdot b^{n+m-k}$$

where for $n \in \mathbb{N}$, $na = a + \cdots + a$ (n summands). If $k \geq n$ then $a^k = a^n a^{k-n}$ where $a^n \in I$ and $a^{k-n} \in R$ so $a^k \in I$ and so $a^k b^{n+m-k} \in I$ (and so is $\binom{n+m}{k} a^k b^{n+m-k}$ since I is a group under addition). And if $k < n$ then $m < n + m - k$

and so as before $b^{n+m-k} \in I$ and so $\binom{n+m}{k} a^k b^{n+m-k} \in I$ and so our sum is in I. So $\sqrt{I}$ is closed under addition and therefore is an ideal.

Definition 2.1.8:

$a \in R$ is **nilpotent** if there exists an $n \geq 1$ such that $a^n = 0_R$.

So if R is commutative then $\{a \in R \mid a \text{ is nilpotent}\} = \{a \in R \mid \exists n \in \mathbb{N} \colon a^n = 0_R\} = \sqrt{\{0_R\}}$. And since $\{0_R\}$ is an ideal, so is its radical and therefore the set of nilpotent elements in R is also an ideal.
Suppose R is a ring and $\varnothing \neq J \subseteq R$ is a subset such that $(J, +) \leq (R, +)$. Since $(R, +)$ is abelian, J is normal, and so R/J is a quotient *group*, where $(a + J) + (b + J) = (a + b) + J$. Now we'd like to define

$$(a + J) \cdot (b + J) = (ab) + J$$

When is this well-defined? Suppose $a_1 + J = a_2 + J$ and $b_1 + J = b_2 + J$ then $a_2 = a_1 + j$ for $j \in J$ and $b_2 = b_1 + j'$ for $j' \in J$. We want to satisfy

$$(a_1 b_1) + J = (a_2 b_2) + J \iff a_2 b_2 - a_1 b_1 \in J$$

And since

$$a_2 b_2 - a_1 b_1 = (a_1 + j)(b_1 + j') - a_1 b_1 = a_1 b_1 + a_1 j' + j b_1 + j j'$$

In order for this to be in J we must have that $a_1 j' + j b_1 \in J$ for every $a_1, b_1 \in R$ and $j \in J$. And this is equivalent to having $aj \in J$ and $ja \in J$ for every $a, j \in J$, which is equivalent to J being a bidirectional ideal. So in order for R/J to have a ring structure (or at least for multiplication to be well-defined) it is necessary and sufficient for J to be a bidirectional ideal.
This leads us to the following definition of the quotient ring:

Definition 2.1.9:

Suppose R is a ring and $I \trianglelefteq R$ is a bidirectional ideal, then we define the **quotient ring** $\left(R/I, +, \cdot\right)$ where R/I is the set of cosets of I under addition, addition is defined as normal, and multiplication of cosets as defined above.

We showed that this is indeed well-defined, and is a ring since $-(aI) = (-a)I$ and I is the identity.

Proposition 2.1.10:

Suppose $f \colon R \longrightarrow S$ is a ring homomorphism, then we define

$$\operatorname{Ker}(f) = \{a \in R \mid f(a) = 0_S\} = f^{-1}(0), \qquad \operatorname{Im}(f) = \{s \in S \mid \exists r \in R \colon f(r) = s\} = f(R)$$

and $\operatorname{Ker}(f)$ is a bidirectional ideal of R and $\operatorname{Im}(f)$ is a subring of S.

Proof:

We know that since f is also a group homomorphism from $(R, +)$ to $(S, +)$, $\operatorname{Ker}(f)$ is a subgroup of $(R, +)$ by group theory. Suppose $r \in R$ and $a \in \operatorname{Ker}(f)$ then $f(ra) = f(r)f(a) = f(r)0_S = 0_S$ so $ra \in \operatorname{Ker}(f)$ and $f(ar) = f(a)f(r) = 0_S f(r) = 0_S$ so $ar \in \operatorname{Ker}(f)$ and so $\operatorname{Ker}(f)$ is a bidirectional ideal of R.
And $\operatorname{Im}(f)$ is a subgroup of $(R, +)$. Since $f(1_R) = 1_S$, this means that $1_S \in \operatorname{Im}(f)$ and since $f(a)f(b) = f(ab)$, $\operatorname{Im}(f)$ is closed under multiplication so it is a subring of S.

■

Theorem 2.1.11 (The First Isomorphism Theorem):

Suppose $f \colon R \longrightarrow S$ is a ring homomorphism, then there is a natural isomorphism

$$R/\operatorname{Ker}(f) \cong \operatorname{Im}(f)$$

(in other words, $R/\operatorname{Ker}(f)$ and $\operatorname{Im}(f)$ are ring-isomorphic.)