Lecture XXXVII: More on Ideals. Quotient Rings

Recall: A left ideal I of a ring R is an abelian subgroup $I \leq (R,+,0)$ s.t. $R \cdot I \subseteq I$ where $R \cdot I = \{ r \cdot x \mid r \in R,\ x \in I \}$

For right ideal we need $I \cdot R = \{ xr \mid r \in R,\ x \in I \} \subseteq I$. A 2-sided ideal is both a left & a right ideal

§37.1 Some terminology on ideals:

We borrow some terminology from the "dictionary" provided in Proposition 3 §36.3

Definition: Fix R a commutative ring. Given two ideals I & J of R we define
$$I + J := \{ a+b \ : \ a \in I,\ b \in J \}$$

Lemma: Given 2 ideals I, J of a ring R, the set $I+J$ is an ideal of R. Furthermore, it is the smallest ideal containing both I & J.

Proof: $I+J$ is a subgroup of $(R,+)$ & it contains both I, J via

$a = a + 0 \quad a \in I,\ 0 \in J \quad$ & $\quad b = 0 + b \quad 0 \in I \ \ b \in J.$

For $r \in R$ $\quad x = a+b \in I+J \qquad r \cdot x = r\cdot(a+b) \overset{\text{Distributive}}{=} \underbrace{r \cdot a}_{\substack{\in I \\ (I \text{ ideal})}} + \underbrace{r \cdot b}_{\substack{\in J \\ (J \text{ ideal})}} \in I + J.$

So $I+J$ is an ideal.

Any $K \subseteq R$ ideal containing I & J must contain $I+J$ because K is closed under addition (it is a subgroup of $(R,+,0)$). $\square$

§37.2 Quotient Rings:

Let R be a ring and $I \subsetneq R$ be a proper two-sided ideal. Consider the group quotient $\overline{R} := R/I$ & give it the structure of a ring as follows:

- $(\overline{R}, +, \overline{0})$ is an abelian group $\quad \overline{a} + \overline{b} = \overline{a+b}$ where $\overline{a} = a + I$, $\overline{b} = b + I$
  $$-\overline{a} = \overline{-a} = -a + I$$
  $$\overline{0} = 0 + I$$

- Multiplication: $\quad \overline{a} \cdot \overline{b} = \overline{a \cdot b} \qquad 1_{\overline{R}} = \overline{1}$

Note: We write $\overline{a} = \overline{b}$ in R/I as $a \equiv b \mod I$ to highlight the ideal I.

Lemma: $(\overline{R}, +, \cdot, \overline{0}_R, \overline{1}_R)$ is a ring

Proof: (1) Need to check multiplication is well-defined (we know $+_{\overline{R}}$ is well-defined from Theorem §6.3)

$\bar{a} = \bar{c} \iff a-c \in I \iff c = a+f$ for some $f \in I$

$\bar{b} = \bar{d} \iff b-d \in I \iff d = b+g$ ______ $g \in I$

Then $ab - cd = ab - (a+f)(b+g) = ab - ab - \underbrace{a\underset{\in I}{g}}_{I} - \underbrace{\underset{\in I}{f}b}_{\in I} - \underbrace{\underset{\in I}{f}\underset{\in I}{g}}_{\in I}$

So $ab - cd \in I$, ie $\overline{ab} = \overline{cd}$

⚠ Multiplication in $\bar{R}$ is well-defined precisely because I is a two-sided ideal. It will not be well-defined for one-sided ideals (left or right).

(2) Next, we check the properties

- $(\bar{R}, +, \bar{0}_R)$ is an abelian group (group quotient ✓)
- Multiplication is associative because multiplication on R is.
- $\bar{a} \cdot \bar{1} = \overline{a \cdot 1} = \bar{a} = \overline{1 \cdot a} = \bar{1} \cdot \bar{a}$ so $\bar{1}$ is neutral element
- $\bar{1}_R \neq \bar{0}_R$ because $1 \notin I$ (I is a proper ideal of R!)
- Distribution Property on $\bar{R}$ is inherited from R. □

Remark: The quotient ring comes equipped with a natural ring homomorphism

$$\begin{aligned} \pi : R &\longrightarrow R/I \\ a &\longmapsto \bar{a} \quad (= a \bmod I) \end{aligned}$$

First Isomorphism Theorem for rings:

Let $f: R \to S$ be a ring homomorphism. Then:

(1) $I = \mathrm{Ker}(f) \subsetneq R$ is a two-sided proper ideal;

(2) f factors through π

$$\begin{tikzcd} R \arrow[rr, "f"] \arrow[dr, "\pi"'] & & S \\ & R/I \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

$f = \bar{f} \circ \pi$.

Furthermore $\bar{f} : R/I \longrightarrow \mathrm{Im}(f)$ is an isomorphism of rings.

Proof: (1) I is a 2-sided ideal by Lemma §36.2 It is proper because $f(1_R) = 1_S \neq 0_S$.

$\bar{f} : R/I \longrightarrow S$ is defined as $f(\bar{a}) = f(a)$

- It is well-defined since $\bar{a} = \bar{b} \iff a-b \in I \iff \exists g \in I$ with $b = a+g$.
So $f(b) = f(a+g) = f(a) + f(g) = f(a) + 0 = f(a)$.

- It follows from the definition of R/I that $\bar{f}$ is a ring homomorphism and $f = \bar{f} \circ \pi$.
- Now, $\bar{f}$ is injective because
$\mathrm{Ker}(\bar{f}) \ni a \pmod{I} \iff f(a) = 0$ ie $a = 0 \mod I$.
- $\mathrm{Im}(\bar{f}) = \mathrm{Im}(f)$ by construction.

Hence, restricting the target space of $\bar{f}$ to $\mathrm{Im}(\bar{f}) = \mathrm{Im}(f) \subseteq S$ we get an isomorphism $R/\mathrm{Ker}(f) \xrightarrow[\bar{f}]{\sim} \mathrm{Im}\, f$ by Lemma §36.1.

§37.3 Some operations on left ideals:

1 Intersections:

We can take intersections of any set of ideals.
Let $I_\alpha \subseteq R$ be a left ideal, where α lies in a labeling set A.

$$I := \bigcap_{\alpha \in A} I_\alpha = \{a \in R \mid a \in I_\alpha \ \forall \alpha \in A\}$$

Lemma 1: I is a left ideal

Proof: I is clearly a subgroup (intersections of subgroups are subgroups)
Now, $\forall r \in R$ $\forall x \in I$, we have $r \cdot x \in I_\alpha$ $\forall \alpha \in A$ because $x \in I_\alpha$ and I_α is a left ideal). Thus, $r \cdot x \in I$, as we wanted. $\square$

2 Sum of left ideals:

Again, assume $I_\alpha \subseteq R$ is a left ideal $\forall \alpha \in A$

$$I := \sum_{\alpha \in A} I_\alpha = \text{smallest left ideal of } R \text{ containing all } I_\alpha\text{'s}.$$

just notation for now

Lemma 2:
$$I = \left\{ a_{\alpha_1} + a_{\alpha_2} + \dots + a_{\alpha_n} \;\middle|\; \begin{array}{l} n \in \mathbb{Z}_{\geq 0} \\ a_{\alpha_i} \in I_{\alpha_i} \\ \alpha_1, \dots, \alpha_n \in A \end{array} \right\}$$

So, I consists of all finite sums we can form using elements of I_α's.

Proof: If A is finite say $A=\{1,\dots,n\}$, then any ideal $\tilde{I}$ containing $I_1,\dots,I_n \subseteq R$ must contain the set $I_1+\dots+I_n := \{a_1+\dots+a_n \mid a_1\in I_1, a_2\in I_2,\dots,a_n\in I_n\}$

But this set itself is a left ideal $\left(r(a_1+\dots+a_n) = \underbrace{ra_1}_{\in I_1}+\dots+\underbrace{ra_n}_{\in I_n} \in I_1+\dots+I_n \right.$.

Hence, the statement is true if A is finite.

The general case follows by the same argument: any element of I involves finitely many indices, so I is a left ideal by construction. Any ideal J containing I_α $\forall\alpha$, will contain $I_{\alpha_1}+\dots+I_{\alpha_n}$ for each n. Thus, $I\subseteq J$. So, I is the smallest left ideal containing all I_α $(\alpha\in A)$ $\square$

③ Left ideals generated by subsets:

Let R be a ring and $X\subseteq R$ be a subset. Let

$I_X :=$ smallest left-ideal containing the set X

We call it the left-ideal generated by X & write it as $R\langle X\rangle$.

More precisely:

Lemma 3: $$I_X = \bigcap_{\substack{\tilde{I}\subseteq R \\ \text{left ideal} \\ X\subseteq\tilde{I}}} \tilde{I}$$

Proof: . (RHS) is a left ideal by Lemma 1 & it contains X.

- Any $\tilde{I}$ left ideal with $X\subseteq\tilde{I}$ contains the (RHS). Thus, equality holds.

Following the operation of sum, we get

Lemma 4: $I_X = \sum_{x\in X} R\cdot x$, ie I_X consists of all finite sums

$$\left\{ r_1x_1+\dots+r_Nx_N : \begin{array}{l} r_1,\dots,r_N\in R \\ x_1,\dots,x_N\in X \end{array} \right\}$$

Proof: $\sum_{x\in X} R\cdot x$ is the smallest left ideal containing $R\cdot x$ $\forall x\in X$ because

$R\cdot x$ = left ideal of R generated by x. That is, $R\cdot x$ the smallest left ideal containing x.

Reason: $x\subseteq I_X$ & $x\subseteq R\cdot x$ ideal gen by x $\Rightarrow$ $R\cdot x\subseteq I_X$

This is true $\forall x$ so $X\subseteq \sum_{x\in X} R\cdot x \subseteq I_X$.

Since $\sum_{x \in X} R \cdot x$ is a left-ideal, we get $I_X \subseteq \sum_{x \in X} R \cdot x$. $\square$

Notational Convenience: If $X = \{x_1, \dots, x_n\}$ (finite subset of R), we just write $R(x_1, x_2, \dots, x_n)$ for the left ideal generated by X.

Definition: Let R be a commutative ring and $I \subseteq R$ be an ideal. We say I is a principal ideal if $I = (a)$ for some $a \in I$

Example: Set of ideals of $\mathbb{Z} = \{ \underset{(n)}{\overset{\shortparallel}{n\mathbb{Z}}} : n = 0, 1, 2, \dots \}$ by Proposition 2 §36.3

Corollary: Every ideal of $\mathbb{Z}$ is principal.