Lecture XXXIX: Properties of ideals; Examples

§39.1 Some more general properties of an ideal:

Let R_1, R_2 be two rings. Let $f: R_1 \longrightarrow R_2$ be a ring homomorphism.

Lemma 1: If $I_2 \subseteq R_2$ is a left / right / two-sided ideal, then so is

$$I_1 = f^{-1}(I_2) = \{a_1 \in R_1 \mid f(a_1) \in I_2\} \subseteq R_1$$

Proof: I_1 is an additive subgroup of R_1 because f is a group homomorphism.

($0_{R_1} \in I_1$ because $f(0_{R_1}) = 0_{R_2} \in I_2$.

$a, b \in I_1 \Rightarrow f(a), f(b) \in I_2 \Rightarrow f(a \pm b) = f(a) \pm f(b) \in I_2$, so $a \pm b \in I_1$)

- Now, assume I_2 is a left ideal

  if $x \in I_1$ and $r \in R_1$ then $f(r \cdot x) = \underbrace{f(r)}_{\in R_2} \underbrace{f(x)}_{\in I_2} \in I_2 \Rightarrow r \cdot x \in I_1$

  Thus, I_1 is also a left ideal

- Similarly, assume I_2 is a right ideal.

  If $x \in I_1$ and $r \in R_1$, then $f(x \cdot r) = \underbrace{f(x)}_{\in I_2} \cdot \underbrace{f(r)}_{\in R_2} \in I_2 \Rightarrow x \cdot r \in I_2$

  Thus, I_1 is also a right ideal.

Combining these 2 cases we get the statement for two-sided ideals. □

⚠ Image of an ideal, need NOT be an ideal.

Example: $f: \mathbb{Z} \longrightarrow \mathbb{Q}$, $n \longmapsto \frac{n}{1}$ $\qquad 2\mathbb{Z} \subseteq \mathbb{Z}$ is an ideal.

But $\{\frac{2n}{1} : n \in \mathbb{Z}\} \subsetneq \mathbb{Q}$ is not an ideal (it's only an additive subgroup)

Reason: Only ideals of $\mathbb{Q}$ (a field) are $\{0\}$ & $\mathbb{Q}$.

Lemma 2: If $f: R_1 \longrightarrow R_2$ is a surjective ring homomorphism, then, if $I_1 \subseteq R_1$ is a left / right / two-sided ideal, then so is $f(I_1) \subseteq R_2$.

Proof: Write $I_2 = f(I_1) \subseteq R_2$.

As image of a subgroup is a subgroup, we know that I_2 is an additive subgroup.

Fix $x_2 \in I_2$ & $r_2 \in R_2$. Since f is surjective, $\exists\, x_1 \in I_1$ & $r_1 \in R_1$ with $f(x_1) = x_2$, $f(r_1) = r_2$

- Assume I_1 is a left-ideal, then $r_1 x_1 \in I_1$ because $f(r_1 x_1) = f(r_1) f(x_1) = r_2 \cdot x_2 \in I_2$
- Similarly, if I_1 is a right-ideal, then $x_1 r_1 \in I_1$ because $f(x_1 \cdot r_1) = f(x_1) f(r_1) = x_2 r_2 \in I_2$
- From these two cases, the statement for 2-sided ideals holds. $\square$

- Similarly to the case of groups, we have the following statement:

Second Isomorphism Theorem:

Let $f: R_1 \longrightarrow R_2$ be a surjective ring homomorphism and let $J = \mathrm{Ker}(f) \subseteq R_1$ (it is a proper 2-sided ideal). We have a bijection:

$$\left\{\begin{array}{c}\text{Left/right/2-sided} \\ \text{ideals of } R_1 \text{ containing } J\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{Left/right/2-sided} \\ \text{ideals of } R_2\end{array}\right\}$$

$$\begin{array}{ccc} \Psi & & \Psi \\ I_1 & \longmapsto & f(I_1) \\ f^{-1}(I_2) = \{a \in R_1 : f(a) \in I_2\} & \longleftarrow\!\shortmid & I_2 \end{array}$$

Moreover, this bijection preserves our usual operations on ideals. For instance, if $I_2 \subseteq R_2$ is a 2-sided ideal, $I_1 = f^{-1}(I_2) \subseteq R_1$ is a 2-sided ideal and $R_1/I_1 \simeq R_2/I_2$

Proof: The correspondence holds by Lemma 2 § 38.4.

$$\begin{tikzcd} R_1 \arrow[r, "f"] \arrow[rr, bend right, "g"'] & R_2 \arrow[r, "\pi"] & R_2/I_2 \end{tikzcd}$$

$g = \pi \circ f$ is a surjective ring homomorphism

$\mathrm{Ker}\, g = \{ a \in R_1 \mid f(a) \in I_2 \} = I_1 \subset R_1$

Then, by the 1st Iso Theorem, we have $R_1/I_1 \simeq R_2/I_2$ $\square$

$a \,(\mathrm{mod}\, I_1) \longmapsto f(a) \bmod I_2$

§ 39.2 Examples of rings, ideals and their interpretation:

1. $R = K[x]$ polynomial ring in 1-variable with coefficients from a field K (say $\mathbb{C}$, $\mathbb{R}$ or $\mathbb{Q}$)

Definition: A polynomial $g \in K[x]$ is monic if the leading coefficient of $g(x)$ is 1 (ie, $g(x) = 1 \cdot x^d + (\text{lower order terms})$)

Proposition: The Euclidean Algorithm works in $K[x]$. Meaning, given $g(x) \neq 0$ and $f(x)$ we have $f(x) = q(x)\, g(x) + r(x)$ where $q(x), r(x) \in K[x]$ and either $r(x) = 0$ or degree $r(x) <$ degree $g(x)$

Proof: Without loss of generality we assume $g(x)$ is monic, ie $g(x) = x^d + a_{d-1}x^{d-1} + \dots + a_0$
Otherwise, $g(x) = \text{leading coeff} \cdot \tilde{g}(x)$ with $\tilde{g}$ is monic & $q(x) = \dfrac{\tilde{q}(x)}{\text{lead coeff}}$ if $f = \tilde{q}\tilde{g} + \tilde{r}$.

We proceed by complete induction on degree of $f(x)$.

Base Case: $\deg(f) = 0$

- If $\deg(g) = 0$ $\Rightarrow$ $f = \frac{f}{g} g(x) + 0$ & $q = \frac{f}{g} \in K$
- If $\deg(g) > 0$, then set $q(x) = 0$ & $r(x) = f(x)$

Inductive Step: Assume the statement is true for all f of degree $< n$. Pick $f(x)$ of degree $= n$
We treat 2 cases, depending on the order relation with respect to $\deg(g)$.

- If $0 \leq \deg(f) < \deg(g)$, then set $q(x) = 0$, $r(x) = f(x)$.
- If $\deg(f) \geq \deg(g)$, let $b :=$ leading coefficient of f, $b \in K^{\times}$.
  (ie $f(x) = b\,x^n + b_{n-1}x^{n-1} + \dots + b_0$)

Replace f by $\tilde{f}(x) = f(x) - b\,x^{n-d} g(x)$

Then either $\tilde{f} = 0$ or $\deg \tilde{f} < \deg f$.

- If $\tilde{f} = 0$, then $q = b\,x^{n-d}$ & $r(x) = 0$
- If $\tilde{f} \neq 0$, by inductive hypothesis applied to $\tilde{f}$, we can find $\tilde{q}(x)$ & $r(x)$ with $\tilde{f} = \tilde{q}(x) g(x) + r(x)$ with $r(x) = 0$ or $\deg(r) < \deg \tilde{f} < \deg f$. □

$$\Rightarrow f(x) = \underbrace{(b\,x^{n-d} + \tilde{q}(x))}_{=: q(x)} g(x) + r(x)$$

Corollary: Every ideal of $K[x]$ is principal.

Proof: Let $I \subseteq K[x]$ be an ideal. If $I = (0)$, then I is principal.
On the contrary, if $I \neq (0)$, choose $g(x) \in I \setminus \{0\}$ of smallest degree

Claim: $I = (g)$

Pf/ ($\supseteq$) is true by construction. For the other inclusion, we use the Euclidean Algorithm. If $f(x) \in I$, we write $f(x) = q(x)\, g(x) + r(x)$ with $q(x), r(x) \in K[x]$ and either $r(x)$ or $\deg r < \deg g$. Now, $r(x) = f(x) - q(x)\, g(x) \in I$ & so $\deg r \not< \deg g$ by the minimality of $\deg g$. Thus $r = 0$, so $f \in (g)$. This shows ($\subseteq$). □

As a consequence, we get a one to one correspondence:

$$\text{Set of ideals of } K[x] \longleftrightarrow \{ g(x) \text{ where } g(x) \in K[x] \text{ is monic} \}$$

Over $K = \mathbb{C}$, by the fundamental theorem of algebra,

$$g(x) \in \mathbb{C}[x] \text{ monic of degree } d \longleftrightarrow g(x) = (x - z_1) \cdots (x - z_d)$$
$$z_1, \ldots, z_d \in \mathbb{C}$$

② $R = \mathbb{Z}[i] = \{ a + bi : a, b \in \mathbb{Z} \}$

Name: R = Gaussian Integers.

- Addition (component-wise): $(a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + (b_1 + b_2) i$
- Multiplication: $(a + bi)(c + di) = (ac - bd) + (ad + bc) i$

(Using Distribution + $i^2 = -1$)

$\Rightarrow$ $R = \mathbb{Z}[i]$ consists of complex numbers $z \in \mathbb{C}$ s.t. $\text{Real Part}(z) \in \mathbb{Z}$
$\text{Imaginary Part}(z) \in \mathbb{Z}$

$\rightsquigarrow$ we get Norm: $\mathbb{Z}[i] \longrightarrow \mathbb{Z}_{\geq 0}$

$$z = a + bi \longmapsto a^2 + b^2 = |z|^2$$

(1) $R^\times = \{ \pm 1, \pm i \}$

Proof: ($\supseteq$) $(\pm 1)^{-1} = \pm 1$ & $(\pm i)^{-1} = \mp i$.

($\subseteq$) $z \in R^\times \Longrightarrow zw = 1$ for some $w \in R^\times$

$\Rightarrow$ $\text{Norm}(zw) = \text{Norm}(1) = 1$

But $\text{Norm}(zw) = \text{Norm}(z)\,\text{Norm}(w) \Longrightarrow \text{Norm}(z) \in \mathbb{Z}^\times$

Conclude: $z = \pm 1, \pm i$ (only elements in R of norm one)

(2) The Euclidean Algorithm works:

Let $z \in R \setminus \{0\}$ and $w \in R$. Then, $\frac{w}{z} = s + it \in \mathbb{C}$

Up to shifts by integers, we can make sure $-\frac{1}{2} \leq s, t \leq \frac{1}{2}$, i.e. $\exists\, a, b \in \mathbb{Z}$ st $-\frac{1}{2} \leq s-a, t-b \leq \frac{1}{2}$

$$\Rightarrow \text{Norm}\left(\frac{w}{z} - (a+bi)\right) \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2}$$

So $w = (a+bi)z + r$ where $r \in R$ has norm $\leq \frac{1}{2}|z| < |z|$.

<u>Proposition 2:</u> Given $w \in R$, $z \in R \setminus \{0\}$ we can find $!\, q, r \in R$ s.t.

$$w = q \cdot z + r \quad \text{and} \quad \text{Norm}(r) = |r|^2 < |z|^2 = \text{Norm}(z).$$

<u>Corollary 2:</u> Every ideal in $\mathbb{Z}[i]$ is principal.

<u>Proof:</u> A generator of a non-zero ideal $I \subseteq \mathbb{Z}[i]$ is any $z \in I \setminus \{0\}$ of minimal norm. $\square$