18. Ideals

Q. What does $\ker(f: A \to B)$ look like?

Def: $I \leq A$ is a left ideal (right / 2-sided) in the ring A if $AI \subseteq I$ (both: AI and IA).

no adjective → default: "ideal" means 2-sided

E.g.
- any $A \Rightarrow I = \{0\}$ is 2-sided
- $\mathbb{Z} \geq n\mathbb{Z}$ 2-sided
- $M_2(\Bbbk) \geq \begin{bmatrix} 0 & * \\ 0 & * \end{bmatrix}$ left, but not right

Def: $a \in A \Rightarrow Aa =$ principal left ideal

$AaA =$ principal ideal

general: $Aa_1 + \cdots + Aa_n =$ left ideal generated by $a_1, \ldots, a_n \in A$

$Aa_1A + \cdots + Aa_nA =$ ideal " " $= \langle a_1, \ldots, a_n \rangle$

E.g. {polynomials with even constant term} $= \langle 2, x \rangle \subseteq \mathbb{Z}[x]$

Q. Why ideals?

Prop: $f: A \to B$ ring homomorphism $\Rightarrow \ker f$ is an ideal.

Pf: $f(a) = 0 \Rightarrow f(bab') = 0 \ \forall\, b, b' \in A$. □

In fact:

Thm: $I \subseteq A$ is an ideal $\Leftrightarrow \exists$ ring homomorphism $f: A \to B$ with $I = \ker f$.

Pf: $\Leftarrow$: Prop.

$\Rightarrow$: $I \subseteq A$ ideal $\Rightarrow A/I$ is a ring with $(x+I)(y+I) = xy + I$

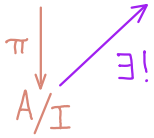
↑ quotient ring = quotient abelian group

i.e. $a \in x+I$ and $b \in y+I \Rightarrow ab \in xy+I$

Why? Because $xI + Iy + I^2 \subseteq I$! □

Thm (Universal property): $A \xrightarrow{\varphi} B$ ring homomorphism with $\ker \varphi \supseteq I$

$\Rightarrow \exists!\, \varphi_*: A/I \to B$ with $\varphi = \overline{\varphi} \circ \pi$.



Pf: True for $(A, +) \to (B, +)$. The claim: φ_* is already a ring homomorphism:

$$\varphi_*(\pi(x)\,\pi(y)) = \varphi_*(\pi(xy)) = \varphi(xy)$$

$$= \varphi(x)\varphi(y) = \varphi_*(\pi(x))\varphi_*(\pi(y)). \quad \square$$

Commutative rings Fix commutative ring R.

Def: An ideal $\mathfrak{p} \subseteq R$ is
- **prime** if $R/\mathfrak{p}$ is entire (an integral domain)
- **maximal** if $\mathfrak{p} \neq R$ and $I \supseteq \mathfrak{p} \Rightarrow I \in \{\mathfrak{p}, R\}$

R entire $\Leftrightarrow$ 0 is prime

Prop: R is a field $\Leftrightarrow$ 0 is maximal.

Pf: $\Rightarrow$: $x \notin \langle 0 \rangle \Rightarrow \langle x \rangle = R$ $\quad \langle x \rangle = \langle 1 \rangle$ $\Updownarrow$

$\Leftarrow$: $x \neq 0 \Rightarrow \langle x \rangle = R$ since $\langle 0 \rangle$ is maximal $\Rightarrow 1 = xy$ for some $y \in R^* \Rightarrow x \in R^*$. $\square$

Cor: maximal $\Rightarrow$ prime.

Pf: Every field is entire. $\square$

Generally: Let $a, b \in R$ entire. Then $\langle a \rangle = \langle b \rangle \Leftrightarrow b = ua$ for some $u \in R^*$.

Pf: $b \in \langle a \rangle \Rightarrow b = xa$. $a \in \langle b \rangle \Rightarrow a = yb = yxa \Rightarrow a(1-xy) = 0 \Rightarrow a = 0$ or $xy = 1$. $\square$

$b = 0 = 1 \cdot 0$

E.g. $p \in \mathbb{Z}$ prime $\Leftrightarrow \langle p \rangle \subseteq \mathbb{Z}$ prime

$\Leftrightarrow \langle p \rangle \subseteq \mathbb{Z}$ maximal, since $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ is a field.

Thm: If $I_1, \dots, I_n \subseteq R$ are ideals with $I_i + I_j = R \ \forall\ i \neq j$

then $f: R \to R/I_1 \times \cdots \times R/I_n$ is surjective.

$x \mapsto (x + I_1, \dots, x + I_n) \Rightarrow \ker f = ?$

$0 \qquad 0 \quad \Rightarrow x \in I_1, \dots, x \in I_n \Leftrightarrow x \in I_1 \cap \cdots \cap I_n$

Pf: Suffices: $\exists\ y_1, \dots, y_n \in R$ with $y_i \mapsto (0, \dots, 0, \underset{\uparrow}{1}, 0, \dots, 0)$ (1 in the i^{th} slot)

analogue: map of vector spaces

surjective $\Leftrightarrow$ image $\supseteq$ basis

$I_1 + I_j = R \Rightarrow \exists\ a_j \in I_1$ with $a_j + b_j = 1$.

and $b_j \in I_j$

$\Rightarrow 1 = (a_2 + b_2) \cdots (a_n + b_n) \in I_1 + b_2 \cdots b_n$,

so take $y_1 = b_2 \cdots b_n$, and similarly for $i = 2, \dots, n$. $\square$

E.g. $R = \mathbb{Z}$ $\quad I_1 = 4\mathbb{Z}$

$I_1 = 6\mathbb{Z}$

$\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$

$x \mapsto (x \pmod 4, x \pmod 6)$

$0 \quad 0$
$1 \quad 1$
$2 \quad 2$
$3 \quad 3$
$\quad\ 4$
$\quad\ 5$

$? \mapsto (\ 0\ ,\ 1\ )$

Cor (Chinese Remainder Theorem):

If $I_1, \dots, I_n \subseteq R$ are ideals with $I_i + I_j = R \ \forall\ i \neq j$,

then $x_1, \dots, x_n \in R \Rightarrow \exists\ x \in R$ with $x \equiv x_i \pmod{I_i} \ \forall\ i$. $\square$

E.g. $m_1, \dots, m_n \in \mathbb{Z}$ with $\gcd(m_i, m_j) = 1 \ \forall\ i \neq j$.

In particular, $m = p_1^{e_1} \cdots p_n^{e_n}$ factorization into distinct primes

$\Rightarrow |(\mathbb{Z}/m\mathbb{Z})^*| \cong |(\prod_{i=1}^{n} \mathbb{Z}/p_i^{e_i}\mathbb{Z})^*|$

Euler φ function $\Rightarrow \varphi(m) = \prod_{i=1}^{n} \varphi(p_i^{e_i}) = \prod_{i=1}^{n} (p_i - 1) p_i^{e_i - 1}$. $\square$