Today: More Algebra.

$A/I$ field $\iff$ $I$ maximal,
$A/I$ domain $\iff$ $I$ prime.

Commutative ring $(A, +, \cdot, 0, 1)$ is

- commutative group $(A, +, 0)$
- comm. semigroup $(A, \cdot, 1)$
  (monoid)
- $a(b+c) = ab + ac$.

Ring homomorphism $\varphi : A \to B$ is

- homomorphism of $(A, +, 0)$
  & of $(A, \cdot, 1)$
- require $\varphi(1_A) = 1_B$.

[Not automatic because
$\varphi(a) = \varphi(a1) = \varphi(a)\varphi(1)$,
but $\varphi(a)^{-1}$ might not exist.]

Given ring hom $\varphi : A \to B$, define
kernel & image:

$\ker\varphi = \{a \in A : \varphi(a) = 0\}$

$\operatorname{im}\varphi = \{b \in B : \exists a \in A, \varphi(a) = b\}.$

- $\operatorname{im}\varphi \subseteq B$ subring.
- $\ker\varphi \subseteq A$ not a subring.

  It's an ideal.

  [$a \in A$, $b \in \ker\varphi$ $(\varphi(b) = 0)$

  $\Rightarrow \varphi(ab) = \varphi(a)\varphi(b) = \varphi(a)0 = 0.$]

- Conversely, any ideal $I \subseteq A$ is the kernel of the "canonical surjection"

$$\begin{aligned} A &\longrightarrow A/I \\ a &\longmapsto a + I \end{aligned}$$

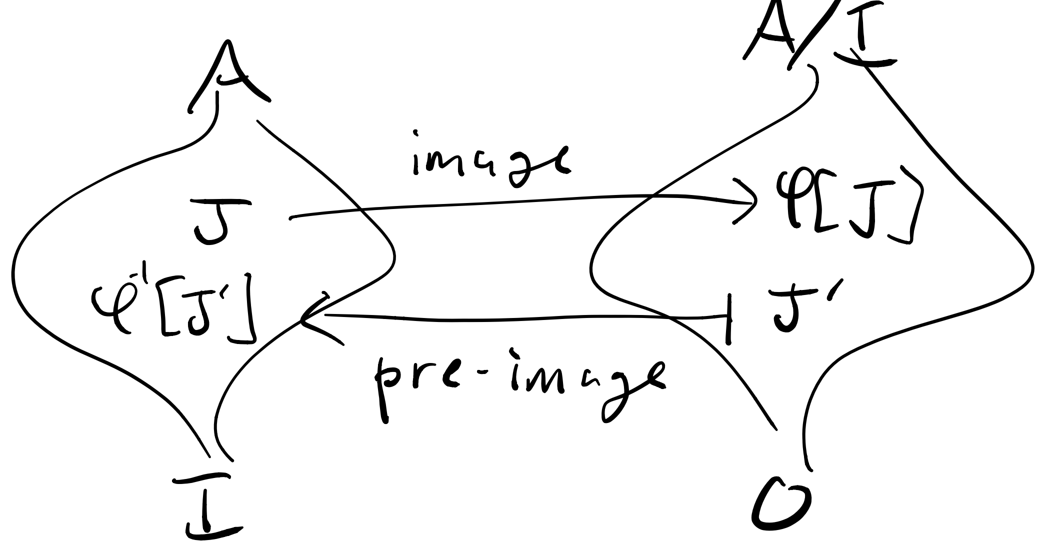
[kernel $\equiv$ ideal

image $\equiv$ subring.]

The "fundamental theorem" of ring homomorphisms is the so-called Correspondence Theorem:

Given an ideal $\varphi : A \to A/I$, we have an inclusion-preserving bijection

$$\left(\begin{array}{c}\text{ideals of } A \\ \text{containing } I\end{array}\right) \longleftrightarrow \left(\text{ideals of } A/I\right)$$




where $\varphi[J] := \{a + I : a \in J\}$

$\varphi^{-1}[J'] := \{a \in I : \varphi(a) \in J'\}$.

Proof: Many small things to check.

Key steps: $\forall$ ideals $J \leq A$ and $J' \leq A/I$,

- $\varphi[J] \leq A/I$ & $\varphi^{-1}[J] \leq A$ are ideals.

- $\varphi[J] \subseteq J' \iff J \subseteq \varphi^{-1}[J']$.
  ("adjunction of posets")

- $\varphi^{-1}[\varphi[J]] = I + J$

- $\varphi[\varphi^{-1}[J']] = J'$.

First two properties give inclusion preserving bijection between

$$\left\{ \begin{array}{l} \text{ideals } J: \\ \varphi^{-1}[\varphi[J]] = J \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{ideals } J': \\ \varphi[\varphi^{-1}[J']] = J' \end{array} \right\}$$

Next two properties tell us exactly which ideals these are.

On the left side: $J = I + J \iff I \subseteq J$.

///

Background: Any function of sets $\varphi: S \to T$ gives an image/preimage adjunction

$$\varphi : 2^S \rightleftarrows 2^T : \varphi^{-1}$$

$$\varphi[X] \subseteq Y \iff X \subseteq \varphi^{-1}[Y]$$

If $(S,+,0)$, $(T,+,0)$ are comm groups, then we get adjunction of subgroup lattices. If $S$ & $T$ are rings then we get adjunction of ideal lattices.

---

Let's translate fields & domains into language of ideals.

Field $\equiv$ Ring $A$ with no ideals other than $0$ & $A$. $(0 \neq A)$

Proof: Let $I \subseteq A$ be ideal. If $u \in I$ for some unit then $1 = uu^{-1} \in I$, hence $a = a1 \in A$ $\forall$ $a \in A$, hence $I = A$. Hence a field has no ideals. Conversely if $A$ has no ideals then any nonzero $u \in A$ is a unit because $0 \subsetneq uA \leq A$ implies $uA = A \Rightarrow ua = 1$ for some $a \in A$. ///

Apply correspondence:

$A/I$ field $\Leftrightarrow$ $A/I$ has no nontrivial ideals

$\Leftrightarrow$ no ideals between $A$ & $I$ (i.e., $I$ is maximal). ///

Domain $\equiv$ Ring in which $0$ is a prime ideal.

[ $P$ prime $\Leftrightarrow$ $A \setminus P$ closed under mult.

$0$ prime $\Leftrightarrow$ $A \setminus 0$ closed under mult.

$\Leftrightarrow$ domain. ]

One can show that "primeness" of ideals is preserved under correspondence.

(Proof postponed.) Hence

$$A/I \text{ domain} \iff 0 \subseteq A/I \text{ prime}$$

$$\underset{?}{\iff} \underset{\substack{\ker\varphi \\ I}}{\varphi^{-1}[0]} \subseteq A \text{ prime}$$

///

Finish the proof:

Say $P' \subseteq A/I$ prime.

To show $\varphi^{-1}[P']$ prime, let

$a, b \notin \varphi^{-1}[P']$, hence $\varphi(a), \varphi(b) \notin P'$,

hence $\varphi(ab) = \varphi(a)\varphi(b) \notin P'$,

hence $ab \notin \varphi^{-1}[P']$. ✓

Say $I \subseteq P \subseteq A$ prime.

To show $\varphi[P] \subseteq A/I$ prime, let

$a+I, b+I \notin \varphi[P]$, hence

$a, b \notin P$ (recall $\varphi[P] = \{p+I : p \in P\}$),

hence $ab \notin P$. To conclude,

we will show this implies

$$(a+I)(b+I) \notin \varphi[P].$$

Indeed, if $(a+I)(b+I) = ab + I$ <u>is</u> in $\varphi[P]$ then we have

$$ab + I = p + I \in \varphi[P]$$

for some $p \in P$, hence

$$ab - p \in I \subseteq P$$

$$ab - p \in P$$

$$ab \in P.$$ Contradiction.

///