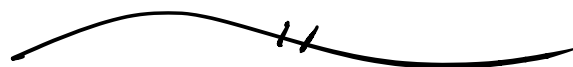


How to balance the historical vs. logical approaches to the material?

Idea: Develop both in parallel, with logical development attached to the HW assignments.



HW1 Discussion:

Commutative ring \mathbb{F} is called "field"

if $\forall 0 \neq a \in \mathbb{F} \exists a^{-1} \in \mathbb{F}$ such that

$$a^{-1}a = 1.$$

In this case, $\mathbb{F}[x]$ has many structural similarities to \mathbb{Z} .

In particular, each has a

"Euclidean Algorithm":

$$\bullet \forall a, b \in \mathbb{Z}, b \neq 0, \exists q, r \in \mathbb{Z},$$

$$\begin{cases} a = qb + r, \\ |r| < |b|. \end{cases}$$

• $\forall f(x), g(x) \in \mathbb{F}[x], g(x) \neq 0,$
 $\exists q(x), r(x) \in \mathbb{F}[x],$

$$\begin{cases} f(x) = q(x)g(x) + r(x), \\ \deg(r) < \deg(g) \text{ or } r(x) \equiv 0. \end{cases}$$

[Fundamental Analogy:

\mathbb{Z} vs. $\mathbb{F}[x]$

]

Problem 1: A nonzero polynomial $f(x) \in \mathbb{F}[x]$ of degree d has at most d roots in \mathbb{F} , counted with multiplicity.

A comm ring A is called an integral domain (or just a domain) if for all $a, b \neq 0$ in A we have $ab \neq 0$. Important property:

If $ab = ac$ & $a \neq 0$, then

$$ab - ac = 0$$

$$a(b - c) = 0 \quad \Rightarrow \quad a \neq 0.$$

$$b - c = 0$$

$$b = c.$$

Every subring $A \subseteq \mathbb{F}$ in a field is a domain. Indeed, given $a, b \in A$ with $ab = 0$ and $a \neq 0$ we have

$$a^{-1} \in \mathbb{F}, \text{ so } b = a^{-1}ab = a^{-1}0 = 0$$

in \mathbb{F} , hence also in A .

Conversely, I claim that every domain is a subring of a field.

Problem 2 (a): Prove this. (b):

It follows that nonzero $f(x) \in A[x]$ where A is a domain, has at most finitely many roots in A .

Problem 3: If A is an infinite

domain & $f(x), g(x) \in A[x]$ have
 $f(\alpha) = g(\alpha)$ for infinitely many $\alpha \in A$
 then $f(x) = g(x)$ as polynomials,
 i.e. they have the same coefficients.

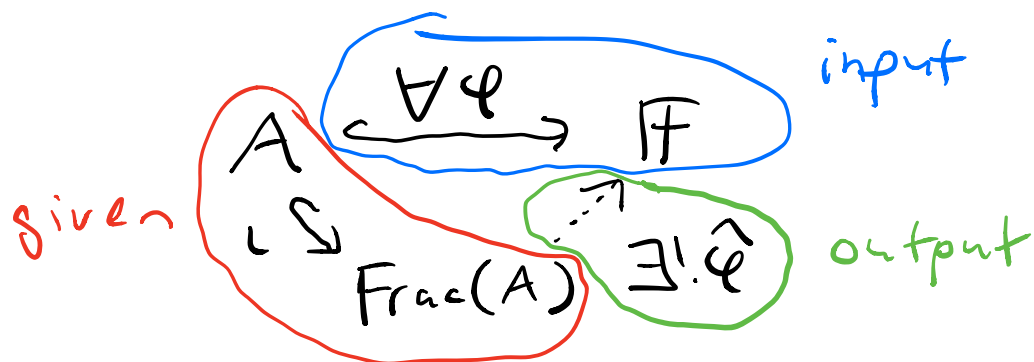
[Follows from Z(b).]

Moral: Many properties of domains
 are inherited from properties of fields.

Universal Property of Fractions.

Given domain A , \exists unique field
 $\text{Frac}(A)$ and injective ring hom

$\iota: A \hookrightarrow \text{Frac}(A)$ such that



For any injective hom into a field
 $\varphi: A \hookrightarrow F$, \exists unique (injective)

hom $\hat{\varphi}: \text{Frac}(A) \hookrightarrow \mathbb{F}$ such that
 $\varphi = \hat{\varphi} \circ \iota$.

Remark: If $\iota: A \hookrightarrow \text{Frac}(A)$ exists
then it is unique. Problem 2(a):

Prove that it actually does exist.

Hint: Let $\text{Frac}(A) = \{ \frac{a}{b}, b \neq 0 \} / \sim$

$$\frac{a}{b} = \frac{a'}{b'} \iff ab' = a'b.$$

Fundamental Example:

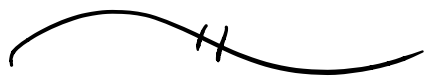
$$\mathbb{Q} = \text{Frac}(\mathbb{Z})$$

Universal Property: If a field

$\mathbb{F} \supseteq \mathbb{Z}$ contains the integers, then

it also contains the rational

numbers: $\mathbb{F} \supseteq \mathbb{Q} \supseteq \mathbb{Z}$.



Maximal & Prime Ideals :

An ideal $I \subseteq A$ is an additive subgroup $(I, +, 0) \subseteq (A, +, 0)$ satisfying

$$a \in A, b \in I \implies ab \in I.$$

In this case the additive quotient group $A/I = \{a+I : a \in A\}$ is also a ring with multiplication

$$(a+I)(b+I) := ab+I$$

Well-Defined ?

$$\text{Sp } a+I = a'+I \text{ \& } b+I = b'+I$$

so that $a-a' \in I, b-b' \in I$.

Then want to show $ab+I = a'b'+I$,
i.e. that $ab-a'b' \in I$.

Proof :

$$\begin{aligned} ab-a'b' &= ab-a'b+a'b-a'b' \\ &= (a-a')b+a'(b-b') \end{aligned}$$

$\in I$

because $a-a', b-b' \in I$. \square

Definition:

Let $I \subseteq A$ be ideal.

- Say I is maximal if $I \subseteq J \subseteq A$
for ideal $J \Rightarrow I=J$ or $J=A$
- Say I is prime if
 $A \setminus I$ closed under multiplication.

Exercise:

- $I \subseteq A$ maximal $\Leftrightarrow A/I$ field
- $I \subseteq A$ prime $\Leftrightarrow A/I$ domain.

Next Time!