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":

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

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

- $\forall f(x), g(x) \in \mathbb{F}[x]$, $g(x) \not\equiv 0$,
  $\exists q(x), r(x) \in \mathbb{F}[x]$,

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

[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

$$ab - ac = 0$$
$$a(b-c) = 0 \quad \& \quad a \neq 0.$$
$$b - c = 0$$
$$b = c.$$

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 $a^{-1} \in \mathbb{F}$, 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 $\mathrm{Frac}(A)$ and injective ring hom $\iota : A \hookrightarrow \mathrm{Frac}(A)$ such that

$$\begin{tikzcd} A \arrow[rr, hook, "\forall \varphi"] \arrow[dr, hook, "\iota"'] & & \mathbb{F} \\ & \mathrm{Frac}(A) \arrow[ur, dotted, "\exists ! \hat{\varphi}"'] & \end{tikzcd}$$

given

input

output

For any injective hom into a field $\varphi : A \hookrightarrow \mathbb{F}$, $\exists$ unique (injective) hom $\hat{\varphi} : \mathrm{Frac}(A) \hookrightarrow \mathbb{F}$ such that

$\varphi = \hat{\varphi} \circ \iota$.

Remark: If $\iota : A \hookrightarrow \mathrm{Frac}(A)$ exists then it is unique. Problem 2(a): Prove that it actually does exist.

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

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

Fundamental Example:

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

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 <u>ideal</u> $I \subseteq A$ is an additive subgroup $(I,+,0) \leq (A,+,0)$ 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 <u>ring</u> with multiplication

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

Well-Defined ?

So $a+I = a'+I$ & $b+I = b'+I$ 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 $\Longleftrightarrow$ A/I field
- $I \subseteq A$ prime $\Longleftrightarrow$ A/I domain.

Next Time!