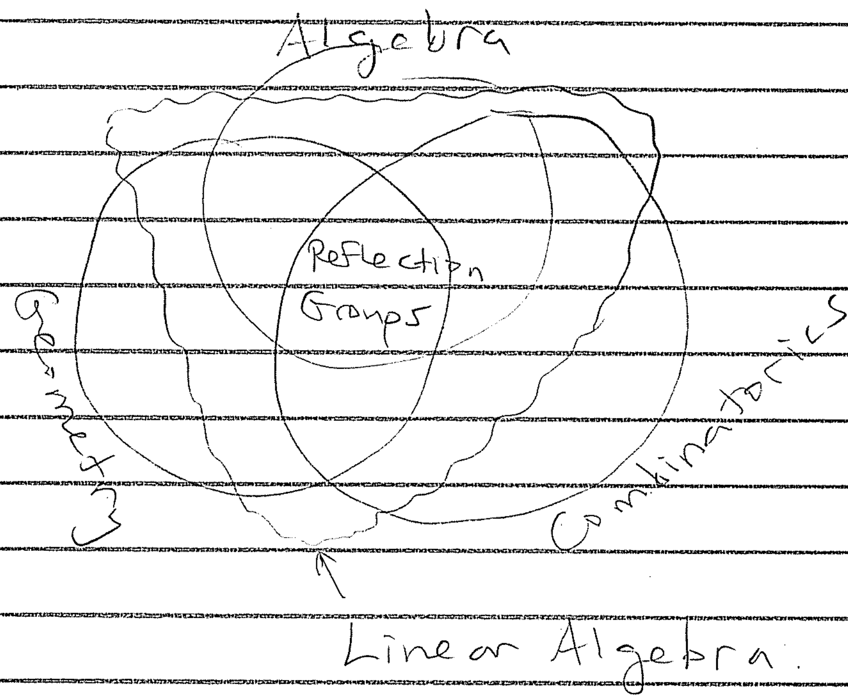
Tue, Aug 28

Recap: Sketch of MTH 592/685



Topic: - Linear Algebra

- Examples of "classification".

Nontrivial(!) Theorem: If $(V, \mathbb{F})$ is a finitely generated vector space then every <u>maximal</u> <u>independent</u> set

$$B \subseteq V$$

has the same (finite) size, called the "dimension" of $(V, \mathbb{F})$

$$|B| =: \dim_{\mathbb{F}}(V)$$

///

(Easy) Theorem: If $(V, \mathbb{F})$ has dimension $n < \infty$, then

$$(V, \mathbb{F}) \approx \mathbb{F}^n.$$

i.e.

"f.d. vector space" = "(field, pos. int.)"

and if the field is understood,

"f.d. vector space" = "positive integer"
(!)

Q: So can <u>fields</u> be classified?

A: Yes, to some extent.

Let $\mathbb{F}$ = a field. Then there is a unique ring map

$$\begin{aligned} \varphi : \mathbb{Z} &\longrightarrow \mathbb{F} \\ 1_{\mathbb{Z}} &\longmapsto 1_{\mathbb{F}} \end{aligned}$$

We know:

- $\ker \varphi = a\mathbb{Z}$ for some $a \in \mathbb{Z}$

- $\mathrm{im}\,\varphi$ is a domain
  (no zero divisors)
- 1st Iso. Thm.

$$\mathbb{Z}/a\mathbb{Z} \cong \mathrm{im}\,\varphi$$

$$\begin{aligned} \mathrm{im}\,\varphi \text{ domain} &\implies a\mathbb{Z} \text{ prime ideal} \\ &\implies a = 0 \text{ OR prime } p. \end{aligned}$$

Notation: "characteristic"

prime subfield.

$$\mathrm{char}(\mathbb{F}) = a = \begin{cases} 0 & \mathbb{Q} \\ \text{prime } p & \mathbb{Z}/p\mathbb{Z}. \end{cases}$$

① Finite fields.

Let $|\mathbb{F}| < \infty$ with characteristic p.

Then $\mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}/p\mathbb{Z} \underset{\text{subfield.}}{\leq} \mathbb{F}$

Then $\mathbb{F}$ is a f.d. vector space over $\mathbb{Z}/p\mathbb{Z}$.
(say dim $= k$), hence

$$|\mathbb{F}| = |(\mathbb{Z}/p\mathbb{Z})^k| = p^k.$$

(finite fields have size p^k)

Conversely, let $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ and consider the ring of polynomials

$$\mathbb{F}_p[x] = \{a_0 + a_1 x + \cdots + a_d x^d : a_1, \ldots, a_d \in \mathbb{F}_p,\ d \geq 0\}$$

If $f(x) \in \mathbb{F}_p[x]$ is irreducible of degree k then $(f(x))$ is a max. ideal

$\Longrightarrow$ $\mathbb{F}_p[x]/(f(x))$ is a field.

and "we know" that it's a k-dim vector space over $\mathbb{F}_p$, hence

$$\mathbb{F}_p[x]/(f(x)) \cong \mathbb{F}_p^k$$

$$|\mathbb{F}_p[x]/(f(x))| = |\mathbb{F}_p^k| = p^k$$

($\exists$ field of every size p^k)

Finally, the hard part

↓

Theorem (Galois, ~1830): Given p prime, $\exists$ irreducible $f(x) \in \mathbb{F}_p[x]$ of all degrees. Furthermore, if irred $f(x)$, $g(x)$ have the <u>same degree</u> k, then

$$\frac{\mathbb{F}_p[x]}{(f(x))} \simeq \frac{\mathbb{F}_p[x]}{(g(x))} =: \underset{\underline{\text{unique}}}{\mathbb{F}_{p^k}} = \mathbb{F}_q$$

☆ Exercise: Put everything together to prove

Classification Theorem: There is a unique field of size p^k for all $(p,k) =$ (prime, pos. int.), and every finite field has this form.

($\mathbb{F}_q = GF(q)$, "Galois field") ///

Hence

"finite field" = "(prime, pos. int.)"

"FINITE vector space" = "(prime, pos. int., pos. int.)"

pretty simple!

② Topological Fields.

Let $\mathbb{F}$ be a field. We say $\|\cdot\| : \mathbb{F} \to \mathbb{R}_{\geq 0}$ is an <u>absolute</u> <u>value</u> if

$$\left.\begin{array}{l} \bullet\ \|x\| = 0 \iff x = 0 \\ \bullet\ \|xy\| = \|x\|\,\|y\|. \\ \bullet\ \|x+y\| \leq \|x\| + \|y\|. \end{array}\right\} \begin{array}{c} \text{or} \\ \text{“valuation”} \\ \text{or} \\ \text{“norm”} \end{array}$$

IF $|\mathbb{F}| < \infty$ the $\mathbb{F}$ has <u>only</u> the <u>trivial</u> abs. value

$$\|x\|_0 = \begin{cases} 0 & x = 0 \\ 1 & x \neq 0 \end{cases}$$

Q: So what about char 0? (i.e. $\mathbb{Q}$).

Theorem (Ostrowski, 1916).

The only abs. values on $\mathbb{Q}$ are.

- $\|x\|_0 = \begin{cases} 0 & x = 0 \\ 1 & x \neq 1, \end{cases}$ “trivial”

- $\|x\|_\infty = \begin{cases} x & x \geq 0 \\ -x & x < 0 \end{cases}$ “real”.

- Let p be prime and suppose $x = p^n \frac{a}{b}$ with a, b, p coprime. and $n \in \mathbb{Z}$. Then

$$\|x\|_p := \begin{cases} 0 & x = 0 \\ p^{-n} & x \neq 0 \end{cases}$$ "p-adic norm"

///

Given a normed field $\|\cdot\| : \mathbb{F} \to \mathbb{R}_{\geq 0}$, we define its (topological) completion:

$\hat{\mathbb{F}}$ = limits of Cauchy sequences with respect to $\|\cdot\|$.

Then we get:

p-adic numbers real numbers.

$$\begin{tikzcd}
\mathbb{Q}_p & & \mathbb{Q}_\infty = \mathbb{R} \\
& \mathbb{Q} \arrow[ul, "\|\cdot\|_p"] \arrow[ur, "\|\cdot\|_\infty"'] &
\end{tikzcd}$$

Furthermore, we have

Theorem (Frobenius, 1877)
The only "reasonable extensions" of $\mathbb{R}$ are

$$\mathbb{R} \subseteq \underset{\substack{\uparrow \\ \text{not} \\ \text{ordered}}}{\mathbb{C}} \subseteq \underset{\substack{\uparrow \\ \text{not} \\ \text{commutative}}}{\mathbb{H}} \subseteq \underset{\substack{\nwarrow \\ \text{not} \\ \text{associative}}}{\mathbb{O}}$$

Today's Moral:
These are the reasonable f.d. vector spaces

$$\boxed{\mathbb{F}_q^n, \quad \mathbb{Q}^n, \quad \mathbb{R}^n, \quad \mathbb{C}^n}$$

That's all.

[Side Remark: I have swept "function fields" and hence Algebraic Geometry under the rug. Sorry.]