Abstract Algebra III

This lecture will be recorded. If you do not want your face in the recording, please turn off your camera. If you do not want your voice in the recording, please participate using the chat.

This week: No HW.

Overview of field theory.

D&F Chapter 13 p.510 Qual: Chs 13-14

Group: One operation $\cdot$ which has an inverse, identity (associative)

We write it as $+$ if commutative

abelian group

Ring: Two operations $+$: associative, commutative, inverses, identity denoted 0

$(R,+)$ abelian gp

$\cdot$: associative, identity denoted 1.

note that $\cdot$ may not be commutative or have inverses

distributivity for how 2 operations interact

when $\cdot$ is commutative we say R is commutative,

everything but 0 has an inverse

$\cdot$ has inverses, we say R is a skew field or division ring

When $\cdot$ is commutative + has inverses we say that R is a field!

everything but 0 has a multiplicative inverse

F is a field

$(F,+)$ is a gp

$(F^\times, \cdot)$ is a gp $\quad F^\times = F - \{0\}$

distributivity

Examples: • $F = \mathbb{Q} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0 \right\} \Big/ \frac{a}{b} = \frac{c}{d}$ iff $bc = ad$

infinitely many elements

• p prime $\quad \mathbb{Z}/p\mathbb{Z}$ is a field

$$\mathbb{Z}/p\mathbb{Z} \overset{..}{=} \mathbb{F}_p$$

finite fields, p elements

new notation

Definition

Let F be a field, let 1 be its multiplicative identity. If there is $n \in \mathbb{N}$ with

$$\underbrace{1+1+1+\ldots+1}_{n \text{ times}} = 0$$

additive identity

then we say that char$(F) = n$

characteristic

If there is no such n, we say char$(F) = 0$.

Note that $\text{char}(\mathbb{Q}) = 0$

$\text{char}(\mathbb{F}_p) = p$ $\qquad$ $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

Proposition: If F is a field with $\text{char}(F) = n$ then $n = 0$ or n is prime.

Definition: Let F be a field. Then the subfield of F generated by 1 is called the prime subfield of F.

Definition: Let F be a field. Then the subfield of F generated by 1 is called the prime subfield of F.

$1 \in F$: field generated by 1 is the smallest subfield of F that contains 1.

$+, \cdot,$ inverses

$$\text{prime subfield} \supseteq \left\{ \begin{array}{l} 1,\ \underbrace{1+1}_{=2},\ \underbrace{1+1+1+1}_{=4}, \ldots \\ \frac{1}{2}, \frac{1}{4}, \frac{1}{5}, 2 \cdot \frac{1}{5}, \ldots \end{array} \right\}$$

The prime subfield of F is (isomorphic to)

$$\begin{cases} \mathbb{Q} & \text{if } \operatorname{char}(F)=0 \\ \mathbb{F}_p & \text{if } \operatorname{char}(F)=p \end{cases}$$

prime subfield contains

$$\left\{ \begin{matrix} 1,2,3,4,\ldots\ldots -1,-2,\ldots \\ \frac{1}{2},\frac{1}{3},\ldots \quad -\frac{1}{2},\ldots \end{matrix} \right\}$$

$\leftarrow +, \cdot$ inverse already in

$\mathbb{F}_p \cong \{0,1,2,3,\ldots p-1\}$

$M_2(\mathbb{Q})$

$$\left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} : a \in \mathbb{Q} \right\}$$

$\{1,\sigma,\sigma^2\}$

$\{0,1,2\}$ $\mathbb{Z}/3\mathbb{Z}$

$\mathbb{F}_3$

$\{1,g,g^2\} = C_3$

Definition Let K be a field and $F \subseteq K$ be a subfield.

Then we say that K is a (field) extension of F, we write it K/F, and we call F the base field of this extension.

this is not a quotient!!

Proposition 2 (Section 13.1 of D&F)

Let F, F' be fields, $\varphi: F \to F'$ be a field homomorphism.

it means $\varphi(a+b) = \varphi(a) + \varphi(b)$
$\varphi(ab) = \varphi(a)\varphi(b)$

Then φ is either 0 ($\varphi(a)=0 \ \forall a \in F$) or φ is injective. then $\underset{\cong F}{\varphi(F)} \subseteq F'$ we can say $F \subseteq F'$

Groups

1. subgps (Sylow e.g.)
2. Homomorphisms (1st, 2nd, 3rd, 4th isom)
3. Group actions

fields + field extension (subfields, fields)

~~X~~

(but there is lin. alg.)

we won't cover this this semester

when a field acts on a set, this set is called a vector space "linear algebra"

Definition

Let $F \subseteq F'$, F, F' fields. (So F' is a field extension of F). Then F' is an F-vector space

and $[F':F] = \dim_F F'$ ← dimension of F' as an F-V.S.

degree of F' over F

Vector space
- $\vec{v}_1 + \vec{v}_2$
vector +

associative
identity $\vec{0}$
inverse $-\vec{v}_1$

scalar mul
- $k \cdot \vec{v}$

"associative" $k_1(k\vec{v}) = (k_1 k)\vec{v}$
$1 \cdot \vec{v} = \vec{v}$
distributivity $k(\vec{v}_1 + \vec{v}_2) = k\vec{v}_1 + k\vec{v}_2$

That’s all for today!