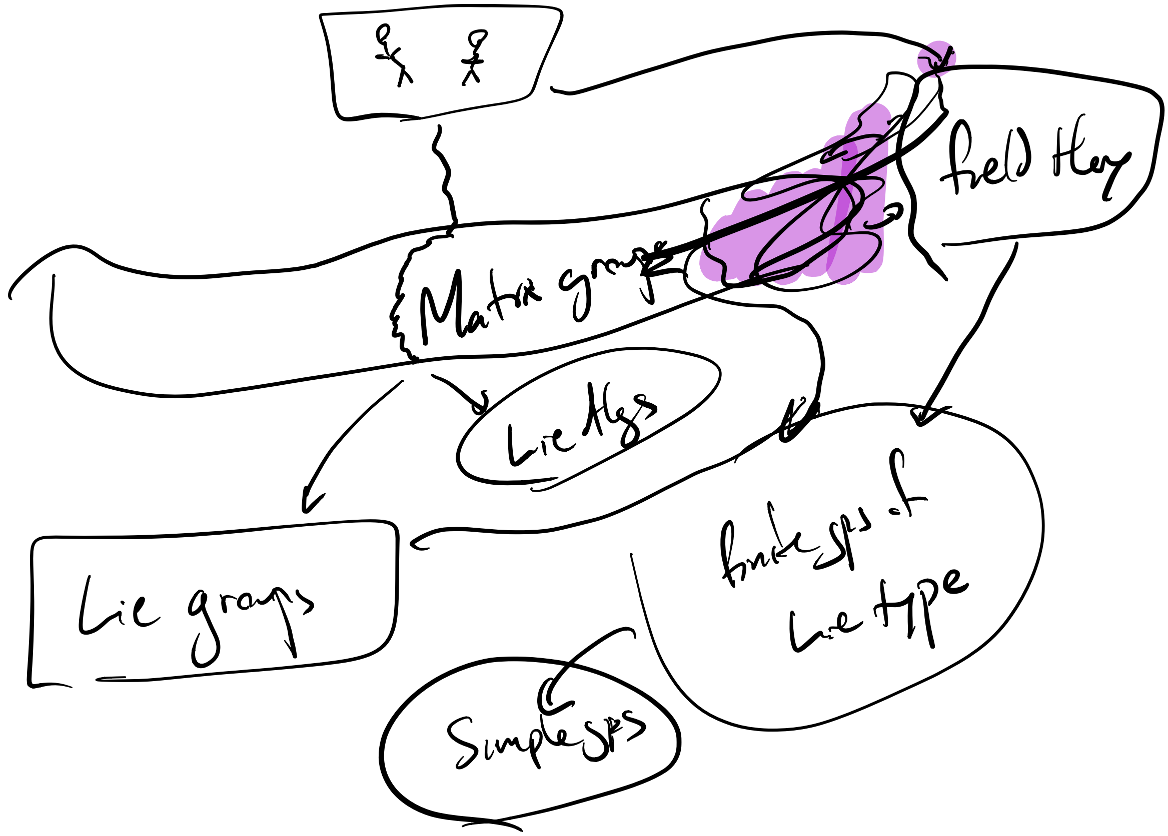

Today: fields & vector spaces & forms

3.2 (main topic at end of bk ch 15, 16)

Ch 3, 4

Ch 8

Reminder

A field F is a set with two binary operations

$$+, \cdot : F \times F \longrightarrow F$$

s.t. $(F,+)$ is an Abelian group
write 0 for the identity element.

$(F \setminus \{0\}, \cdot)$ is an Abelian group
write 1 for the identity element

and such that

$$a(b+c) = ab + ac.$$

$$\left[\underline{\text{Note:}} \quad \begin{aligned} a \cdot 0 &= a(0+0) = a \cdot 0 + a \cdot 0 \\ 0 &= a \cdot 0 + a \cdot 0 - a \cdot 0 = a \cdot 0 \end{aligned} \right]$$

Examples $\quad \mathbb{C}, \mathbb{R}, \quad \mathbb{Q} = \{ z \in \mathbb{C} \mid z = \frac{a}{b}, a, b \in \mathbb{Z} \}$

$$\mathbb{Q}(i) = \{ a + bi \mid a, b \in \mathbb{Q} \} \subset \mathbb{C}$$

subfield

$$(a+bi)(c+di) = (ac - bd) + (ad + bc)i$$

$$\mathbb{Q}(\sqrt{2}) = \{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \} \subset \mathbb{C} \quad \text{subfield}$$

$$(a+b\sqrt{2})(c+d\sqrt{2}) = (ac + 2bd) + (ad+bc)\sqrt{2}$$

$$(a+b\sqrt{2})(a-b\sqrt{2}) = a^2-2b^2 \neq 0$$ if $a,b \neq 0$!

$$(a+b\sqrt{2})\left(\frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}\right)$$

"

$$\underbrace{(a+b\sqrt{2})(a-b\sqrt{2})}_{a^2-2b^2}\left(\frac{1}{a^2-2b^2}\right) = 1$$

$a^2 = 2b^2$ either $b=0$ ($\Rightarrow a=0$)

or

$\frac{a^2}{b^2} = \left(\frac{a}{b}\right)^2 = 2 \Rightarrow \sqrt{2} \in \mathbb{Q}$ no!

To check K is a subfield $K \subset F$ F a field

need:

$(K,+) < (F,+)$ is a subgrp

$(K\setminus\{0\},\cdot) < (F\setminus\{0\},\cdot)$ is a subgp.

$a(b+c) = ab+ac$

for $a,b,c \in K \subset F$

K closed under $+$, has inverses (negatives)

$K\setminus\{0\}$ closed under $\cdot$, has inverses (reciprocal)

enough to show K closed under $\cdot$

$ab \in K$ for all $a,b \in K$

if $a,b \in K \setminus \{0\} \subset F \setminus \{0\}$ $\quad ab \in K \cap (F \setminus \{0\}) = K \setminus \{0\}$

$$\mathbb{F}_2 = \{T, F\} = \{0, 1\} = \{\text{even}, \text{odd}\} = \mathbb{Z}/2\mathbb{Z}$$

$$\{\bar{0}, \bar{1}\}$$

$$\boxed{\begin{aligned} 0+0 &= 0 \\ 0+1 &= 1 \\ 1+0 &= 1 \\ 1+1 &= 0 \end{aligned}}$$

$\mathbb{Z}/2\mathbb{Z}$

$0 \cdot 0 = 0$

$0 \cdot 1 = 0$

$1 \cdot 0 = 0$

$\boxed{1 \cdot 1 = 1}$ (e)

$\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z} = \{$mult of 3, 1 more than mult 3, 2m...

$\{0 \bmod 3,\ 1 \bmod 3,\ 2 \bmod 3\}$

$\quad \bar{0} \qquad \bar{1} \qquad \bar{2}$

$\bar{1} \cdot \bar{2} = \bar{2}$

$\bar{1} + \bar{2} = \bar{0}$

$(3n+1)(3m+2)$

$\bar{1} + \bar{1} = \bar{2}$ $\qquad \bar{1} + \bar{0} = 1$

$3(\ ) + 2$

$\bar{2} \cdot \bar{2} = \bar{1}$

$\mathbb{F}_3 \setminus \{0\} = \{\bar{1}, \bar{2}\}$ $\quad C_2$

$\mathbb{Z}/pq\mathbb{Z}$

more generally: $\mathbb{F}_p$ $\quad p$ prime.

$\bar{p} \cdot \bar{q} = \bar{0}$

Linear algebra "works" over fields

eg: notion of vector space

<u>Def</u>: A vector space V over a field F is a set w/ a binary op $+: V \times V \to V$ and a operation $\cdot: F \times V \longrightarrow V$

s.t. $(V,+)$ is a group

$$(F \setminus \{0\}) \times V \longrightarrow V$$

is an action of the group $(F\setminus\{0\}, \cdot)$

and $a(v+w) = av + aw$.

and $(a+b)v = av + bv$

just as before

- dimension, bases, linear transformations $\leftrightarrow$ matrices, determinants, invertibility, Gaussian elimination, rank, nullity

---

Characteristic of a field

$1 \in F$ $\qquad 2 = 1+1 \qquad 3 = 1+1+1$

$$-5 = -(1+1+1+1+1)$$

in general, have a homomorphism of additive groups

$$\begin{aligned}(\mathbb{Z},+) &\xrightarrow{\varphi} (F,+)\\ n &\longmapsto \underbrace{1+1+\cdots+1}\\ -n &\longmapsto -(\text{" } n \text{ times})\end{aligned}$$

1st Iso $\Rightarrow$ $\mathbb{Z}/\underbrace{\ker\varphi} \simeq \operatorname{im}\varphi < (F,+)$

Show: $\ker\varphi = \begin{cases} 0 & \text{or} \\ p\mathbb{Z} & \text{for } p \text{ a prime number}\end{cases}$

n = smallest pos # in $\ker\varphi$

$n = pq$ then $\varphi(p), \varphi(q) \neq 0$

but $\underset{\underset{(1+\cdots+1)}{\underbrace{}_{p\neq 0}}}{\varphi(p)}\ \varphi(q)$ ... $(\underbrace{1+\cdots+1}_{p\neq 0})(\underbrace{1+\cdots+1}_{q\neq 0}) = \underbrace{1+\cdots+1}_{pq} = \varphi(pq) = 0$

Def if $\ker = p\mathbb{Z}$ we say F has characteristic p

if $\ker = 0$ — — — — — 0.

ex: $\mathbb{Q}, \mathbb{R}, \mathbb{Q}(i)$ char 0 $\qquad$ $\mathbb{F}_2$ char 2

$\mathbb{F}_p$ char p

ex: $\mathbb{F}_p((t)) = \left\{ \sum_{n=n_0}^{\infty} a_i t^i \;\middle|\; \begin{array}{l} a_i \in \mathbb{F}_p \\ n_0 \in \mathbb{Z} \end{array} \right\}$

field of char p (very infinite)