

1.

Math 501

Fall 2023

Algebraic Structures I

Tue / Thu 13:25 - 14:40

Physics 235

Office Hours: Tue 14:40 - 16:00
Thu 14:40 - 16:00right after class } Physics 209
outside sometimes
Zoom if necessary

Safety: • know where the exits are from the room and the building

- know the procedures for various emergencies, e.g.

- tornado
- fire
- active shooter

Policies • covered on Tue \Rightarrow fair game for HW due Thu

- collaboration / academic honesty
 - Yes on HW write your solutions yourself
 - No on exams

I have • brought numerous cases to the Office of Student Conduct
• never lost

Index cards

1. Ezra Miller

2. he / him

3. 44th grade

4. Major or potential major: Math, Music

5. What you hope to get out of this course

students who know basic abstract algebra and can write great proofs

6. The most important thing you've learned about how you learn

not to take notes!

7. Hobbies: frisbee, gardening, photography, ...

8. Something unique about yourself

X "I'm from MA"

✓ "I'm from HI —

but I'm allergic to pineapple!"

hold breath for 4 minutes
screws in right hand

told by doctor in hospital I was going to die of rabies
so radioactive I set off a Geiger counter from across room
remarkable bike accident without injury

Groups

Def: A group is a set G with a binary operation

$$G \times G \rightarrow G$$

$$(a, b) \mapsto ab$$

that

or $a * b$, or $a + b$, or $a \cdot b$, or $a \times b$, or $a \circ b$, or ...

semigroup

- is associative: $(ab)c = a(bc)$ for all $a, b, c \in G$

monoid

- has an identity e with $eg = ge = g$ for all $g \in G$

- has an inverse map $G \rightarrow G$ with $gg^{-1} = e$ for all $g \in G$.

Note: $ab = ba$ not required

Q. Must $g^{-1}g = e$?

Q. bijection?

A. Yes: $ab = e \Rightarrow abr = er$

$$\begin{aligned} br &= e \\ \Rightarrow ae &= er \\ \text{2-sided } e \\ \Rightarrow a &= r. \end{aligned}$$

G is abelian if $G \times G \rightarrow G$ is commutative: $ab = ba$ for all $a, b \in G$

E.g. $(\mathbb{R}, +)$

\mathbb{C}

\mathbb{Q}

\mathbb{Z}

$\left(\begin{array}{c} m \times n \text{ matrices} \\ \text{with any of these} \\ \text{coefficients} \end{array} \right), +$

$(\mathbb{R} \setminus \{0\}, \cdot)$

\mathbb{C}

\mathbb{Q}

\mathbb{Z}

$\left(\begin{array}{c} m \times n \text{ matrices} \\ \text{with any of these} \\ \text{coefficients} \\ \text{still no; why?} \end{array} \right), \cdot$

$C^0(\mathbb{R}^n \rightarrow \mathbb{R}, +)$

Fun $(S \rightarrow A, +)$ $A = \text{any abelian group!}$

non-abelian: $\{A \in \mathbb{R}^{2 \times 2} \mid \det A = 1\}$

$$\text{e.g. } \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

We'll see more non-abelian examples soon

Why groups?

Abstract the notion of symmetry:

"this operation leaves the figure looking the same as it did before" e.g. icosahedron ... colored and not!

⇒ a set of operations with composition: if f fixes figure
(symmetries)

G

$$G \times G \rightarrow G$$

$$\text{and } G \rightarrow G$$

$$f \mapsto f^{-1}$$

if f fixes figure

and g " "

then $f \circ g$ and $g \circ f$ do, too

and f^{-1} fixes figure

Combinatorics: discrete symmetries e.g. Platonic solids } linear transformations

Geometry: continuous symmetries e.g. rotations of sphere } given by matrices

⇒ matrix groups

Topology:



$$\text{circle} \times \text{circle} = \text{torus} \text{ has "homology group"} \quad \mathbb{Z} \times \mathbb{Z}$$

$$+ \quad 0 \quad = \quad \text{circle}$$

circle \times circle = torus has "homology group" $\mathbb{Z} \times \mathbb{Z}$ groups don't need to act on things

Computer Science: e.g., what's the fastest way to sort a list?

⇒ permutation groups, transpositions, ...

2. E.g. A field is an abelian group $(F, +)$ with additive identity $0 \in F$ such that

- $F^* = F \setminus \{0\}$ is an abelian group (F^*, \cdot) and
- multiplication \cdot distributes over addition $+$: $a \cdot (b+c) = a \cdot b + a \cdot c$.

E.g. $\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{F}_2 = \{0, 1\}, \mathbb{F}_3 = \{-1, 0, 1\}, \mathbb{F}_p = \{0, 1, \dots, p-1\}$ for $p \in \mathbb{Z}$ prime
 $\mathbb{R}(i), \mathbb{Q}(i) \quad \mathbb{Z}?$ What is $\mathbb{Z} \setminus \{0\}$? under \times ? monoid (commutative)

Note: Math 221 works verbatim with any F in place of \mathbb{R} , except for notions of length, angle, order ($a < b$)
 \downarrow
closeness (topology)

E.g. $\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Is it a field? Use:

Def: A subgroup of a group G is a subset $H \subseteq G$ that is

- closed under composition: $a, b \in H \Rightarrow ab \in H$
- closed under inversion: $a \in H \Rightarrow a^{-1} \in H$

notation: $H < G$

Lemma: $H < G$ is a group with same identity as G .

Pf: Associativity is for free: $(ab)c = a(bc)$ in H because it is so in G .

inversion $\Rightarrow a^{-1}a = e \in H$. \square

E.g. $\mathbb{Q}[\sqrt{2}] < \mathbb{C}$ closed under $+$ and $-$ because it is a \mathbb{Q} -vector subspace

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

$$(-)^{-1} \text{ because } \frac{1}{a+b\sqrt{2}} = \frac{1}{a+b\sqrt{2}} \cdot \frac{a-b\sqrt{2}}{a-b\sqrt{2}} = \frac{a}{a^2-2b^2} + \frac{-b}{a^2-2b^2}\sqrt{2}$$

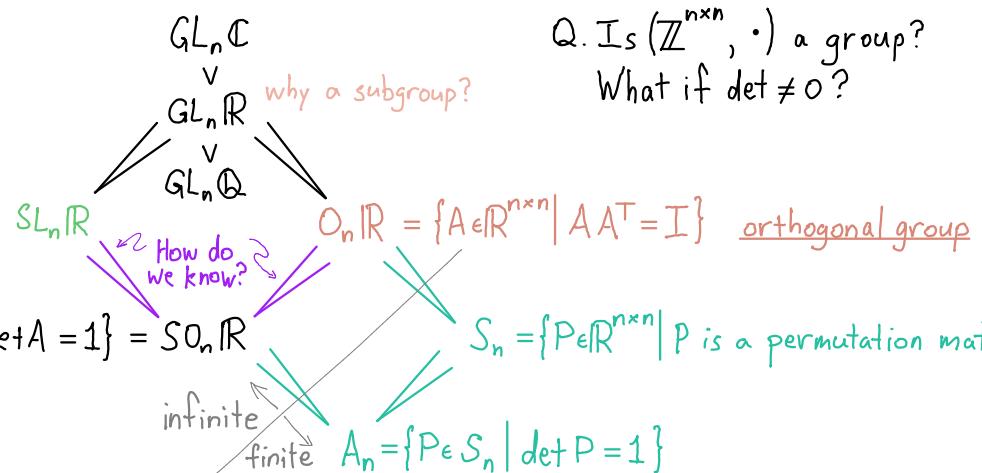
E.g. general linear group $GL_n F = \{A \in F^{n \times n} \mid \det A \neq 0\} = (F^{n \times n})^*$ $\stackrel{+}{\circ}$ since $a, b \in \mathbb{Q}$!

special linear group

$$SL_n F = \{A \in F^{n \times n} \mid \det A = 1\}$$

Exercise: $H_1, H_2 \leq G$
 $\Rightarrow H_1 \cap H_2 < G$.

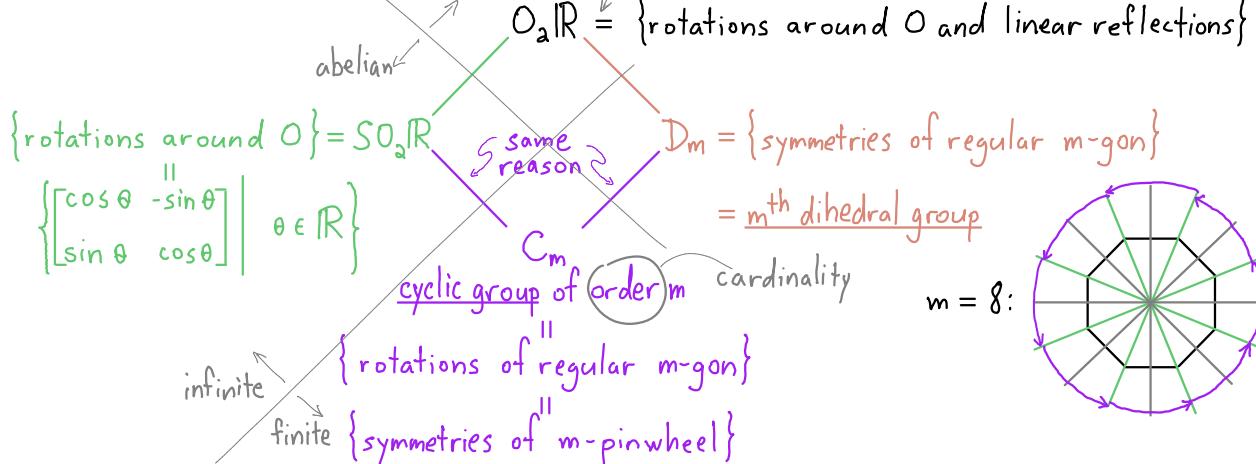
$$\{A \in \mathbb{R}^{n \times n} \mid A A^T = I \text{ and } \det A = 1\} = SO_n \mathbb{R}$$



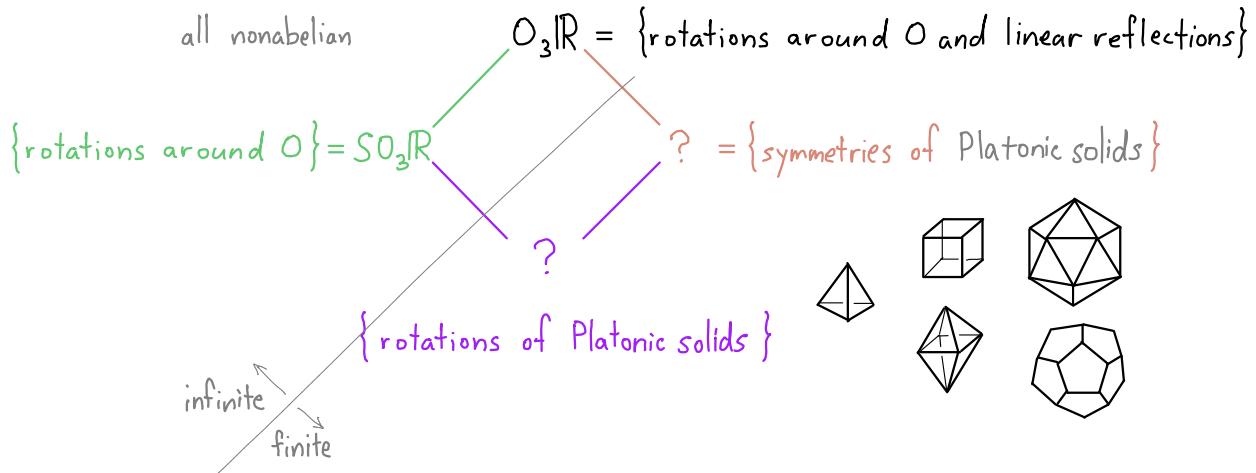
Def: A permutation of a set X is a bijection $\pi: X \rightarrow X$. The symmetric group is

E.g. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 1 & 4 & 2 \end{pmatrix}$ $3142 \leftrightarrow \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{bmatrix} \in S_4$ $S_n = \{\text{permutations of } \{1, \dots, n\}\}$

n = 2:



n = 3:



E.g. $(\mathbb{C}, +) > (\mathbb{R}, +) > (\mathbb{Q}, +) > (\mathbb{Z}, +) > (\mathbb{dZ}, +)$

e.g. $2\mathbb{Z} = \text{even integers}$

all abelian, all infinite

E.g. $\mathbb{C}^* > \mathbb{R}^* > \mathbb{Q}^* > \mathbb{Z}^*$ all abelian
 infinite | finite

3.

Uniqueness*" $\forall a$ " works in any monoid*

- identity: For $a \in G$ fixed, $ga = a \Rightarrow g = e$ because $(ga)a^{-1} = g(aa^{-1}) = ge = g$ and $aa^{-1} = e$.
- more generally: operation in G is cancellative: $ab = ac \Rightarrow b = c$
- inverses: $ab = e \Rightarrow b = a^{-1}$ already discussed
- bracketing: $a_1 \cdots a_n$ well defined, independent of bracketing

Pf: Induction on n . $n = 3$: $a(bc) = (ab)c$ by def.

$n \geq 4$: Show every bracketing equals $((\cdots((a_1 a_2) a_3) \cdots) a_{n-1}) a_n$.

$$a(bc) = \underbrace{(\cdots)}_{a} \underbrace{(\cdots)}_{k} \underbrace{(\cdots)}_{n-k} \text{ some internal bracketings}$$

b $\underbrace{(\cdots)}_{n-k+1} a_n$ c by induction

rewrite as desired, by induction. \square

Q. $(a_1 \cdots a_n)^{-1} = ?$

Def: $a^n = \underbrace{a \cdots a}_n$ for $n \in \mathbb{N}$ (so $a^0 = e$) and $a^{-n} = \underbrace{\bar{a} \cdots \bar{a}}_n$

Lemma: $a^{r+s} = a^r a^s$ for $r, s \in \mathbb{Z}$. \square

Warning: • Don't write $\frac{a}{b}$. Why? ab^{-1} vs. $b^{-1}a$

• $(ab)^m \neq a^m b^m$ in general

Subgroups of \mathbb{Z}

Q. $H \leq \mathbb{Z} \Rightarrow H = ?$

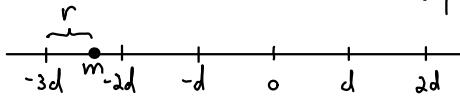
Prop: $H = d\mathbb{Z}$ for some $d \in \mathbb{Z}$.

Pf: $H = \{0\} \Rightarrow d = 0$. ✓ order of H

Assume $|H| > 1$. Pick $d \in H$ with $d \neq 0$ and $|d|$ minimal. WLOG $d > 0$ since $-d \in H$.

Claim: $H = d\mathbb{Z}$. Pf: • $d\mathbb{Z} \subseteq H$: $d \in H \Rightarrow \underbrace{d + d + \cdots + d}_{n \in \mathbb{Z}} \in H$ quotient remainder

• $H \subseteq d\mathbb{Z}$: Given $m \in H$, write $m = qd + r$ with $0 \leq r \leq d-1$.



Then $qd \in H \Rightarrow r = m - qd \in H$

$\Rightarrow r = 0$. \square

E.g. $4\mathbb{Z} + 6\mathbb{Z} = \langle 4, 6 \rangle \subseteq \mathbb{Z}$

= subgroup generated by 4 and 6

abelian = smallest subgroup containing 4 and 6
 $= \{\alpha \cdot 4 + \beta \cdot 6 \mid \alpha, \beta \in \mathbb{Z}\}.$

But $\langle 4, 6 \rangle \neq \langle 4 \rangle$ and $\langle 4, 6 \rangle \neq \langle 6 \rangle$; $\langle 4, 6 \rangle = ?$ <2>

Cor: For $a, b \in \mathbb{Z}$, $\langle a, b \rangle = \langle \gcd(a, b) \rangle$. check!

Pf: $\langle a, b \rangle = \{ \alpha a + \beta b \mid \alpha, \beta \in \mathbb{Z} \} = d\mathbb{Z}$ by Prop.

$\Rightarrow d \mid a$ and $d \mid b$. But $d = \alpha a + \beta b$ for some $\alpha, \beta \in \mathbb{Z}$,
so $d' \mid a$ and $d' \mid b \Rightarrow d' \mid (\alpha a + \beta b) = d$. \square

• find α, β } Euclid's
• compute d } algorithm

Def: In a group G , the cyclic subgroup generated by $a \in G$ is $\langle a \rangle = \{\text{powers of } a\}$

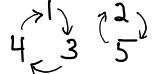
The order of a is $|a| = |\langle a \rangle|$.

$$= \{a^n \mid n \in \mathbb{Z}\}.$$

E.g. In $G = \mathbb{Q}^*$, $a = 3 \Rightarrow \langle a \rangle = \{ \dots, \frac{1}{9}, \frac{1}{3}, 1, 3, 9, \dots \}$

$$|a| = \infty.$$

E.g. In $G = S_5$, $a = (134)(25)$ is cycle notation for $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}$



$$|a| = ? \quad \begin{matrix} a^2 & a^{-1} & a^0 & a^1 & a^2 & a^3 & a^4 & a^5 & a^6 \\ 6 & a^4 & a^5 & e & a & (143) & (25) & (134) & (143)(25) & e \end{matrix}$$

E.g. $a = e \Rightarrow |a| = ?$ 1

Prop: $\{n \in \mathbb{Z} \mid a^n = e\} \leq \mathbb{Z}$, so it is $d\mathbb{Z}$ for some $d \in \mathbb{N}$.

$$\bullet d = 0 \Leftrightarrow |a| = \infty.$$

$$\bullet d > 0 \Leftrightarrow |a| = d \Leftrightarrow d \text{ is the smallest positive integer with } a^d = e.$$

Pf: S is a subgroup:

$$m, n \in S \Rightarrow a^{m+n} = a^m a^n = e e = e \Rightarrow m+n \in S.$$

$$m \in S \Rightarrow a^{-m} = (a^m)^{-1} = e^{-1} = e \Rightarrow m^{-1} \in S. \quad \checkmark$$

$$\text{Now } a^m = a^n \Leftrightarrow a^{m-n} = e$$

$$\Leftrightarrow m-n \in d\mathbb{Z}$$

$$\bullet d = 0: \Leftrightarrow m = n \quad \checkmark$$

$$\bullet d > 0: \Rightarrow \langle a \rangle = \underbrace{\{e, a, a^2, \dots, a^{d-1}\}}$$

all distinct

$$\text{and } a^d = e. \quad \square$$

4.

Homomorphisms

Def: A map $\varphi: G \rightarrow G'$ of groups is a \cdot homomorphism if $\varphi(ab) = \varphi(a)\varphi(b)$ $\forall a, b \in G$
 \cdot isomorphism if also φ is bijective; write $G \xrightarrow{\varphi} G'$ or $G \cong G'$ φ^{-1} also isom.

Examples

1. $GL_n F \xrightarrow{\det} F^*$ $\det(AB) = \det A \det B$ | Are these isomorphisms? No, but
 $O_n \mathbb{R} \xrightarrow{\det} \{\pm 1\}$ ($= \mathbb{Z}^*$)
- $S_n \rightarrow \{\pm 1\}$ $S_n = \{\text{permutations of } \{1, \dots, n\}\} \cong \{\text{permutation matrices}\} < O_n \mathbb{R}$
2. Fix $P \in GL_n F$. Then $GL_n F \cong GL_n F$ conjugation by P change of basis
 $A \mapsto PAP^{-1}$ (similarity) $P(AB)P^{-1} = (PAP^{-1})(PBP^{-1})$

3. $C_\infty = \text{infinite cyclic group } \langle a \rangle = \{ \dots, a^{-2}, a^{-1}, e, a, a^2, \dots \} \quad |a| = \infty$
 $\Rightarrow \mathbb{Z} \xrightarrow{\cong} C_\infty \quad \begin{matrix} \varphi(m+n) = a^{m+n} = a^m a^n = \varphi(m)\varphi(n) \\ 1 \mapsto a \end{matrix}$ composition in \mathbb{Z} composition in C_∞
- $C_d = \langle a \rangle = \{e, a, \dots, a^{d-1}\}$ cyclic of order $d \Rightarrow \mathbb{Z} \xrightarrow{\cong} C_d \quad \begin{matrix} \text{surjective homomorphism} \\ 1 \mapsto a \end{matrix}$ later: $C_d \cong \mathbb{Z}/d\mathbb{Z}$
4. $\varphi: F^+ \rightarrow GL_2 F$
 $a \mapsto \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \quad \varphi(a+b) = ? \quad F = \text{field} \checkmark$
 $F = \mathbb{Z} ? \checkmark$
5. $\mathbb{Q}^n \xrightarrow{\varphi} \mathbb{Q}^m$ homomorphism \Leftrightarrow linear

Exercise: Prove there is a group homomorphism $\mathbb{R}^n \rightarrow \mathbb{R}^m$ that isn't linear!

Lemma: $G \cong G' \Rightarrow |G| = |G'|$.

If $\varphi: G \cong G'$ then $|a| = |\varphi(a)| \quad \forall a \in G$. \square

Def: An isomorphism $G \cong G$ is an automorphism of G .

E.g. conjugation by $g \in G$ is an automorphism: $a \mapsto gag^{-1}$ inverse?
 $gbg^{-1} \leftarrow b$

E.g. $\text{Aut } C_8 = ?$

$$C_8 = \langle a \rangle = \{e, a, a^2, a^3, a^4, a^5, a^6, a^7\}$$

orders: 1 8 4 8 2 8 4 8

$\varphi: C_8 \rightarrow \text{Aut } G$ determined by $\varphi(a)$ since $\varphi(a^n) = \varphi(a)^n \quad \forall n \in \mathbb{Z}$

$$|a| = 8 \Rightarrow |\varphi(a)| \in \{1, a^3, a^5, a^7\}.$$

Lemma: G abelian \Rightarrow $\varphi_n: G \rightarrow G$ is a homomorphism.
 $g \mapsto g^n$

$$\text{Pf: } \varphi_n(gh) = (gh)^n = g^n h^n = \varphi(g)\varphi(h). \quad \square$$

Lemma $\Rightarrow \Psi(a) = a^n$ homomorphism $\forall n \in \{1, 3, 5, 7\}$.
 \Rightarrow isomorphism, since bijective

Prop: If $G \xrightarrow{\Psi} G'$ is a homomorphism then

- $$(i) \quad \varphi(e) = e' \quad \text{and} \quad \varphi(a^{-1}) = \varphi(a)^{-1} \quad \forall a \in G.$$

- $$(ii) \quad \text{im } \varphi = \{\varphi(a) \mid a \in G\} \text{ and}$$

$\ker \varphi = \{a \in G \mid \varphi(a) = e'\}$ are subgroups.

- (iii) $\ker \psi$ is a normal subgroup: $a \in \ker \psi$ and $g \in G \Rightarrow gag^{-1} \in \ker \psi$.

closed under conjugation by G

- (iv) φ surjective $\Leftrightarrow \text{im } \varphi = G'$.

φ injective $\Leftrightarrow \ker \varphi = \{e\}$.

$$\underline{\text{Pf:}} \quad (\text{i}) \quad \varphi(a a^{-1}) = \varphi(a) \varphi(a^{-1}) \quad a = e \Rightarrow \varphi(e) = \varphi(e)^{-1} \Rightarrow e' = \varphi(e)$$

$$\varphi(e) = e' \Rightarrow \varphi(a^{-1}) = \varphi(a)^{-1}$$

- $$(ii) \quad a' = \varphi(a) \quad \text{and} \quad b' = \varphi(b) \quad \Rightarrow \quad a'b' = \varphi(a)\varphi(b) = \varphi(ab) \quad \checkmark$$

↓

$$(\alpha')^{-1} = \varphi(\alpha)^{-1} = \varphi(\alpha^{-1}). \quad \checkmark$$

$$\varphi(a) = e' \quad \text{and} \quad \varphi(b) = e' \quad \Rightarrow \quad \varphi(ab) = \varphi(a)\varphi(b) = e'e' = e'. \quad \checkmark$$

↓

$$\varphi(a^{-1}) = \varphi(a)^{-1} = (e')^{-1} = e'. \quad \checkmark$$

- $$(iii) \quad a \in \ker \varphi \Rightarrow \varphi(a) = e' \Rightarrow \varphi(gag^{-1}) = \varphi(g)e'\varphi(g^{-1}) \\ = \varphi(g)\varphi(g^{-1})^{\text{green circle}} = e'. \quad \checkmark$$

(iv) surj. ✓

$$\varphi(a) \neq \varphi(b) \Leftrightarrow \varphi(a)\varphi(b)^{-1} \neq e'$$

$$\Leftrightarrow \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1}) \neq e'.$$

This is true $\wedge a \neq b$ precisely when

$$\varphi(ab^{-1}) = e' \Leftrightarrow ab^{-1} = e \quad \forall a, b \in G$$

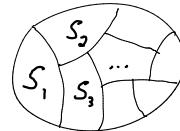
$$\text{i.e. } \varphi(c) = e' \Leftrightarrow c = e \quad \forall c \in G. \quad \square$$

5.

Equivalence relations

3 ways to say same thing Fix a set S . block

1. partition of S : $S = \bigcup_{i \in I} S_i$ with $S_i \neq \emptyset$ and $S_i \cap S_j = \emptyset \quad \forall i \neq j$ disjoint union
index set (could be infinite)



E.g. 1. $\{1, 2, 3, 4, 5\} = \{1, 3\} \cup \{2, 5\} \cup \{4\}$ 2. $1 \sim 3 \quad 2 \sim 5$ 3. $\{1, 2, 3, 4, 5\} \rightarrow \{[3], [2], [4]\}$

• $\mathbb{Z} = \{\text{evens}\} \cup \{\text{odds}\}$

$a \sim b \Leftrightarrow 2 | a - b$

$\mathbb{Z} \rightarrow \{\bar{0}, \bar{1}\}$

evens $\mapsto \bar{0}$
odds $\mapsto \bar{1}$

2. equivalence relation \sim on S : for some pairs $a, b \in S$, $a \sim b$.

Must be • reflexive: $a \sim a$

Formally, $\sim \subseteq S \times S$

• symmetric: $a \sim b \Rightarrow b \sim a$

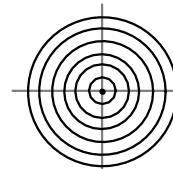
$\{(a, b) \mid a \sim b\}$

• transitive: $a \sim b$ and $b \sim c \Rightarrow a \sim c$ E.g. 1. + 2.

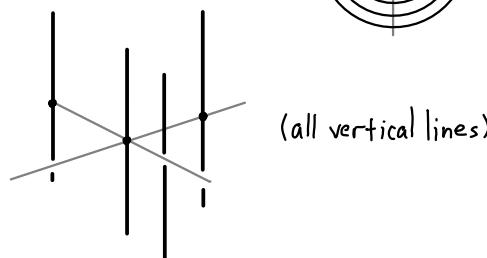
equivalence class of $a = [a] = \{x \in S \mid x \sim a\}$

3. fibers of a map $S \xrightarrow{\varphi} T$: the fiber over $t \in T$ is $\varphi^{-1}(t) = \{s \in S \mid \varphi(s) = t\}$.

E.g. $\mathbb{C} \rightarrow \mathbb{R}$
 $z \mapsto |z|$ \Rightarrow fibers:



E.g. $\mathbb{R}^3 \rightarrow \mathbb{R}^2$
 $(x, y, z) \mapsto (x, y)$ \Rightarrow fibers:



E.g. 3.

3 \Rightarrow 1: $S = \bigcup_{t \in T} \varphi^{-1}(t)$ $\varphi^{-1}(t) \neq \emptyset$ because φ is surjective

$t \neq t' \Rightarrow \varphi^{-1}(t) \cap \varphi^{-1}(t') = \emptyset$

1 \Rightarrow 2: partition $S = \bigcup_{i \in I} S_i \iff a \sim b \Leftrightarrow a, b \in \text{same block}$

2 \Rightarrow 3: given \sim on S , let $T = \{\text{equivalence classes}\}$

$\psi: S \rightarrow T$

$s \mapsto [s]$ other notations: \bar{s} , C_s

General e.g. G group $a \sim b$ if $gag^{-1} = b$ for some $g \in G$ conjugacy classes

check $a \sim a: a = eae^{-1}$

compare: similar matrices

$a \sim b \Rightarrow b \sim a: a = g^{-1}bg$

$a \sim b$ and $b \sim c \Rightarrow a \sim c: hbh^{-1} = c \Rightarrow (hg)a(hg)^{-1} = h(gag^{-1})h^{-1} = hbh^{-1} = c$. ✓

E.g. $G = S_3 = \{e, (12), (13), (23), (123), (132)\}$

$$(12)(123)(12) = (132)$$

partition of S_3 by cycle type!

conjugacy classes		
(1)(2)(3)	(12)	(123)
	(23)	(132)
	(13)	

$$(13)(12)(13) = (1)(23)$$

$$(23)(12)(23) = (13)(2)$$

$$(123)(12)(123)^{-1} = (1)(23)$$

$$(132)(12)(132)^{-1} = (13)(2)$$

Remark: Can use $S \rightarrow T$ not surjective, but must omit empty fibers from partition and \sim

General e.g. $\Psi: G \rightarrow G'$ $N = \ker \Psi$ $\Psi(a) = \Psi(b) \Leftrightarrow aN = bN$

Nonempty fibers all have form aN for some $a \in G$ $\Leftrightarrow b \in aN \stackrel{\text{def}}{=} \{an \mid n \in N\}$

Cosets

Fix subgroup $H \leq G$

Def: A left coset of H (in G) is a subset of G having the form aH for some $a \in G$.

Write $b \equiv a$ (b is congruent to a) if $b \in aH$ (i.e. $b = ah$ for some $h \in H$).

Prop: The left cosets of H partition G .

Pf: $a = ae$ and $e \in H$ ($a \equiv a$)

$$b = ah \Rightarrow a = b\underbrace{h^{-1}}_{\in H} \quad (a \equiv b \Rightarrow b \equiv a)$$

$$b = ah \text{ and } c = bh' \Rightarrow c = a\underbrace{h h'}_{\in H}. \quad \square$$

Cor: $aH \cap bH \neq \emptyset \Leftrightarrow aH = bH. \quad \square$

Def: $G/H = \{\text{cosets of } H \text{ in } G\}$, so

$G \rightarrow G/H$ has fibers aH for $a \in G$.

E.g. Another way to see S_3

$$e \quad (12) \quad (23) \quad (13) \quad (123) \quad (132)$$

$$1 \quad x \quad y \quad \begin{matrix} xyx^{-1} \\ yxy \end{matrix} \quad xy \quad yx$$

$$S_3 = \langle x, y \mid x^2 = 1, y^2 = 1, xyx = yxy \rangle$$

$$\begin{array}{c} \parallel \\ \text{generators} \end{array} \quad \begin{array}{c} \nwarrow \\ \text{relations} \end{array}$$

$$H = \langle x \rangle = \{1, x\}$$

$$yH = \{y, yx\}$$

$$xyH = \{xy, xxy\}$$

$$\left. \begin{array}{c} \\ \end{array} \right\} S_3/H$$

E.g. $G = \mathbb{Z}$ $H = 2\mathbb{Z}$ $G/H = \mathbb{Z}/2\mathbb{Z} = \{2\mathbb{Z}, 1+2\mathbb{Z}\} = \{\bar{0}, \bar{1}\}$
 even odds

$H = 3\mathbb{Z}$ $G/H = \mathbb{Z}/3\mathbb{Z} = \{3\mathbb{Z}, 1+3\mathbb{Z}, 2+3\mathbb{Z}\} = \{\bar{0}, \bar{1}, \bar{2}\}$

6.

Def: The index of a subgroup $H \leq G$ is $[G:H] = |G/H|$.

Prop: All cosets of H have the same size. 1

Consequently, $|G| = |H|[G:H]$. 2

Pf: $aH \rightarrow bH$ }
 $g \mapsto ba^{-1}g$ } bijection

$$ba^{-1}g' \leftrightarrow g' \quad 1 \checkmark$$

2: Both sides are ∞ unless $[G:H] = r < \infty$, in which case

$$|G| = |a_1H| + \dots + |a_rH| = r|H|. \quad \square$$

Cor [Lagrange's Thm]: $H \leq G$ and G finite $\Rightarrow |G| \mid |H|$. now you've really seen some group theory

Cor: $a \in G \Rightarrow |a| \mid |G|$.

Pf: $|a| = |\langle a \rangle| \leq G. \quad \square$

Cor: $|G| = p$ prime $\Rightarrow G \cong C_p$ is cyclic of order p .

Pf: Pick $g \in G$ with $g \neq e$. Then $|g| = 1$ or p .

$$g \neq e \Rightarrow |g| = p \Rightarrow G = \langle g \rangle. \quad \square$$

Prop: $\varphi: G \rightarrow G'$ homomorphism \Rightarrow

$$|G| = |\ker \varphi| \cdot |\text{im } \varphi|.$$

Pf: $|\text{im } \varphi| \leftrightarrow \{\text{nonempty fibers of } \varphi\}$

$$[G:H] = |G/H| \text{ for } H = \ker \varphi. \quad \square$$

$$|\ker \varphi| \mid |G|$$

$$\Rightarrow |\text{im } \varphi| \mid |G|$$

$$|\text{im } \varphi| \mid |G'|$$

Modular arithmetic

Def: For $a, b, n \in \mathbb{Z}$, $a \equiv b \pmod{n}$ if $a - b \in n\mathbb{Z}$

" a is congruent to b modulo n "

$$a + n\mathbb{Z} = b + n\mathbb{Z}$$

$$\bar{a} = \bar{b} \text{ in } \mathbb{Z}/n\mathbb{Z}$$

G/H

Lemma: $[\mathbb{Z}:n\mathbb{Z}] = n = |\mathbb{Z}/n\mathbb{Z}|$

Pf: Division with remainder: $m = qn + r$ with $0 \leq r < n-1$.

Q. \mathbb{Z} has $+$, \times ; what about $\mathbb{Z}/n\mathbb{Z}$?

Prop: $a, b, n \in \mathbb{Z} \Rightarrow \overline{a+b} = \bar{a} + \bar{b}$

and $\overline{ab} = \bar{a}\bar{b}$ are well defined in $\mathbb{Z}/n\mathbb{Z}$.

E.g. $n = 2 \quad \mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$
 even odds

familiar rules:	even + even = even	even · even = even
	odd + odd = even	odd · odd = odd
	even + odd = odd	even · odd = even

E.g. $n = 10$: last digit of $2179 + 836 = ? \quad \bar{9} + \bar{6} = \bar{5}$
 $2179 \times 836 = ? \quad \bar{9} \times \bar{6} = \bar{4}$

E.g. "clock arithmetic"

E.g. weekdays: What day of the week will September 14, 2024 be?

$$\text{Thu} \equiv 5 \pmod{7} \quad 365 \equiv \cancel{?} \cancel{1} \pmod{7} \quad 7 \mid 350 \Rightarrow 15 \equiv 1 \pmod{7}$$

$$\text{Thu} + \cancel{365} \equiv \cancel{5} + \cancel{1} \equiv \cancel{6} \equiv \begin{matrix} \text{Fri} \\ \text{Sat} \end{matrix} \quad \text{Is that right? No! Why? Leap year!}$$

Pf: Need $a - a' \in n\mathbb{Z}$
 $b - b' \in n\mathbb{Z}$

$$\left. \begin{array}{l} \Rightarrow \overline{a+b} = \overline{a'+b'} \\ \text{But } (a+b) - (a'+b') = (a-a') - (b-b') \in n\mathbb{Z}. \quad \checkmark \end{array} \right\} \begin{array}{l} \text{ring} \\ \text{ring homomorphism} \end{array}$$

$$\downarrow \quad \overline{ab} = \overline{a'b'}. \quad \text{But } ab - a'b' = ab - ab' + a'b - a'b'$$

$$= \underset{n\mathbb{Z}}{a}(\underset{n\mathbb{Z}}{b-b'}) + \underset{n\mathbb{Z}}{(a-a')b} \in n\mathbb{Z}. \quad \square$$

Note: \mathbb{Z} has + associative commutative with inverses
 × associative (commutative) distributive over +

Q. $\mathbb{Z}/n\mathbb{Z}^* = ?$ When is \overline{m} invertible? $\Leftrightarrow am \equiv 1 \pmod{n}$ for some $a \in \mathbb{Z}$

A.

$$\begin{aligned} &\Leftrightarrow am \in 1 + n\mathbb{Z} \quad " \\ &\Leftrightarrow am = 1 - bn \quad " \quad \text{and } b \in \mathbb{Z} \\ &\Leftrightarrow am + bn = 1 \quad " \\ &\Leftrightarrow \gcd(m, n) = 1. \end{aligned}$$

E.g. music theory = ? clock arithmetic!

$$\mathbb{Z}/12\mathbb{Z} = \{C, C^\#, D, D^\#, \dots, B^\flat, B\} \quad \# = +1, \flat = -1, \text{ so } A^\# = B^\flat \text{ on notes}$$

octave \equiv unison, octave + 3rd \equiv 3rd : \equiv means "sounds like"

circle of fifths: $\mathbb{Z}/12\mathbb{Z} = \langle 7 \rangle$ since $\gcd(7, 12) = 1$.

on key signatures: up one fifth = $+7 = \#$, down one fifth = $-7 = \flat$

$\dots, B^\flat, F, C, G, D, \dots$

cf.

7. Groups of small order

G

$ G $	abelian	nonabelian
1	$\{e\}$	
2	$\mathbb{Z}/2\mathbb{Z}$	
3	$\mathbb{Z}/3\mathbb{Z}$	
4	$\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$a, b \in G \setminus \{e\}$ with $a^2 = e$ and $b^2 = e$ $\Rightarrow ab = ba$ since $\neq a, b, \text{ or } e$
5	$\mathbb{Z}/5\mathbb{Z}$	
6	$\mathbb{Z}/6\mathbb{Z}, \cancel{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}}$	S_3
7	$\mathbb{Z}/7\mathbb{Z}$	
8	$\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, (\mathbb{Z}/2\mathbb{Z})^3$	 D_4, Q_8 ("quaternions")
:		

→ Def: The product $G \times G' = \{(g, g') \mid g \in G \text{ and } g' \in G'\}$ is a group under componentwise composition

$$(g_1, g'_1)(g_2, g'_2) = (g_1 g_2, g'_1 g'_2). \quad \text{Homomorphisms: } G \times G' \xrightarrow{\quad} G'$$

$\downarrow \quad \swarrow$
 $G \quad \text{projections}$

$$\begin{array}{ccc} G' & & g' \\ \downarrow & & \downarrow \\ G & \xrightarrow{\quad} & G \times G' \\ g & \mapsto & (g, e') \end{array}$$

E.g. $|G|=6$ nonabelian: $a, b \in G \quad ab \neq ba \quad |g| \in \{2, 3\} \quad \text{if } g \neq e$

$$G = \{1, x, x^2, y, y^2, z\} \Rightarrow |z| = 2, \text{ so } G \text{ has an element of order 2.}$$

But $a^2 = b^2 = (ab)^2 = e \Rightarrow abab = e \Rightarrow ab = ba, \text{ so } G \text{ has an element of order 3.}$

May as well assume $|a| = 2$ and $|b| = 3$, since then $ab = ba \Rightarrow G \cong \mathbb{Z}/6\mathbb{Z}$.

Then $G = \{1, a, b, b^2, ab, ba\} \cong S_3$ via $a \mapsto (12)$ and $b \mapsto (123)$.

Ex: $aba = ? \neq e, ab, ba, a$ (since $ab \neq e$), b (since $ab \neq ba$); check ↗

Quotient groups

Q. When is G/H a group? ... with $G \rightarrow G/H$ a homomorphism?

Thm: $\Leftrightarrow H$ is a normal subgroup, written $H \trianglelefteq G$.

Pf: \Rightarrow : Prop, p. ⑧: $G \xrightarrow{\varphi} G/H \Rightarrow H = \ker \varphi \trianglelefteq G$.

\Leftarrow : $(aH)(bH)$ is supposed to be a left coset of H , where

$$A, B \subseteq G \Rightarrow AB = \{ab \mid a \in A \text{ and } b \in B\}.$$

"Every left coset is a right coset if H is normal":

 OMIT:
done
in
HW2

Lemma: $H \trianglelefteq G \Leftrightarrow gH = Hg \quad \forall g \in G.$

$$\begin{aligned} \text{Pf: } gH &= \{gh \mid h \in H\} \\ &= \{g(g^{-1}hg) \mid h \in H\} \quad \text{since } g^{-1}Hg = H \\ &= \{hg \mid h \in H\} \\ &= Hg. \quad \square \end{aligned}$$

\Leftarrow also holds

$$\text{Now compute } (aH)(bH) = (a(Hb)H) = (a(bH)H) = abHH = abH.$$

$\frac{||}{ab} \quad \frac{||}{ab}$

Exercise: Let G be a group and S a set with a map $S \times S \rightarrow S$.
 $(s, t) \mapsto st$

If $\varphi: G \rightarrow S$ with $\varphi(ab) = \varphi(a)\varphi(b) \quad \forall a, b \in G$

then S is a group.

Ex $\Rightarrow S = G/H$ proves Thm. \square

Cor: $N \trianglelefteq G \Leftrightarrow \exists$ homomorphism $\varphi: G \rightarrow G'$ with $\ker \varphi = N$.

Pf: \Rightarrow : Prop, p. 8

$\Leftarrow: G' = G/N. \quad \square$

$$\text{E.g. } n\mathbb{Z} \triangleleft \mathbb{Z} \quad n\mathbb{Z} = \ker(\mathbb{Z} \rightarrow C_n) \quad \mathbb{Z}/n\mathbb{Z} \cong C_n$$

General: What if $G \xrightarrow{\varphi} G'$ with $N = \ker \varphi$?

Is there a relation between G' and G/N ?

First Isomorphism Theorem: $G \xrightarrow{\varphi} G' \Rightarrow G/N \xrightarrow{\sim} G'$.

Pf: Essentially the Ex. \square

$$\text{E.g. } G = \mathbb{C}^*$$

$$N = S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$$

$$G/N = ? \quad \text{cosets}$$

$$\begin{array}{ccc} \text{Diagram of concentric circles} & \cong & \mathbb{R}_+^* \\ |z|=4/3 & |z|=1/2 & |z|=2/3 \end{array}$$

How it's used: 1. $G/\ker \varphi \xrightarrow{\sim} \text{im } \varphi$

2. If $G \xrightarrow{\varphi} G'$ is any homomorphism and $N \trianglelefteq G$ with $N \leq \ker \varphi$, then φ induces a homomorphism $G/N \rightarrow G'$.

8.

Group actions

General principle: $\text{Aut}(\text{anything}) \cap \text{symmetries}(\text{anything}) = G$ is a group

$\begin{cases} g: X \xrightarrow{\sim} X \\ g': X \rightarrow X \\ \text{id}: X \rightarrow X \end{cases} \Rightarrow g' \circ g: X \rightarrow X$

$g^{-1}: X \rightarrow X$ $x \in X \Rightarrow gx \in X$

$g'gx \in X$ $1x \in X$

often algebraic, in this class
but there's no real difference

Def: A group action (or operation) of G on a set S is a map

$$\begin{aligned} G \times S &\rightarrow S & \text{satisfying} && (i) 1s = s \\ (g, s) &\mapsto gs & && (ii) g'(gs) = (g'g)s \quad \forall g, g' \in G \text{ and } s \in S \end{aligned}$$

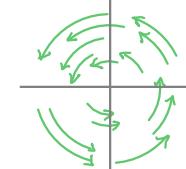
Terminology: S is a G -set with a left action (right action $S \times G \rightarrow S$)

E.g. 1. $S = F^n$ $G = GL_n F$ algebraic? geometric?

point
lines
planes
 \vdots

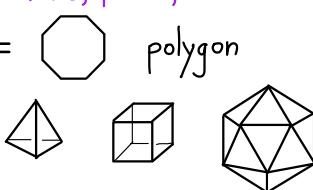
$$\begin{array}{c} GL_n F \\ \swarrow \quad \searrow \\ SL_n F \quad O_n F \\ \searrow \quad \swarrow \\ SO_n F \end{array}$$

$$\text{e.g. } SO_2 \mathbb{R}^2 \times \mathbb{R}^2 \rightarrow \mathbb{R}^2$$



2. $G = S_n$ $S = \{1, \dots, n\}$ neither: preserves no algebraic or geometric structure

3. $S = \text{points in } \mathbb{R}^n$ $G = \text{rigid motions or translations}$ geometric



$$\begin{array}{ccc} A_4 & S_4 & A_5 \\ S_4 & S_4 \times C_2 & H_3 \end{array}$$

geometric

4. $S = \text{polygon}$ $G = \text{cyclic, dihedral,}$

$$\begin{array}{ccc} \triangle & \square & \text{dodecahedron} \\ & & \end{array}$$

geometric

5. $S = \mathbb{C}$ $G = C_2 = \{1, r\}$ $r \cdot \alpha = \bar{\alpha}$ algebraic? geometric?

6. $S = \mathbb{Z}/10\mathbb{Z}$ $G = C_4 = \text{Aut}(\mathbb{Z}/10\mathbb{Z})$ algebraic

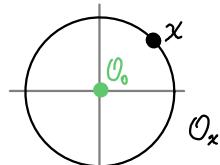
Notation: $\lambda_g: S \rightarrow S$ left multiplication by g Q. $\lambda_g \circ \lambda_{g'} = ?$ A. $\lambda_1 = \text{id}_S$

7. $S = F^{n \times}$ $G = GL_n F$ left actions $\lambda_g(s) = gs$ $\lambda'_g(s) = sg^{-1}$

right actions $\rho_g(s) = sg$ $\rho'_g(s) = g^{-1}s$

Def: Let G act on S . The orbit of $s \in S$ is $\mathcal{O}_s = \{gs \mid g \in G\} = Gs$.

E.g. 1. $G = SO_2 \mathbb{R}$ $S = \mathbb{R}^2$



$$G_0 = SO_2 \mathbb{R}$$

$$G_x = \text{id}_{\mathbb{R}^2} \quad \forall x \neq 0$$

2. $\mathcal{O}_i = \{1, \dots, n\}$ only one orbit: transitive action

	$G = \text{rigid motions}$	$G = \text{translations}$
points	transitive	transitive
lines	transitive	$\mathcal{O}_l = \{l' \subseteq \mathbb{R}^n \mid l' \parallel l\}$ parallel class of l
planes	transitive $G_s = \{e\} \forall s$	" $G_l = \{\text{translations parallel to } l\}$

4. skip fixes l as a set but maybe not pointwise

$$5. \mathcal{O}_\alpha = \{\alpha, \bar{\alpha}\} \text{ if } \alpha \notin \mathbb{R} \quad G_\alpha = \{1\}$$

$$\mathcal{O}_\alpha = \{\alpha\} \text{ if } \alpha \in \mathbb{R} \quad G_\alpha = \{1, \alpha\}$$

Lemma: The orbits of G on S partition S .

Pf: Write $s \sim s'$ if $s' = gs$ for some $g \in G$. Show it's an equivalence relation. \square

Note: G acts transitively on each orbit.

Def: The stabilizer of $s \in S$ is $G_s = \{g \in G \mid gs = s\} \leqslant G$.

Lemma: $gs = hs \Leftrightarrow g^{-1}hs = s \Leftrightarrow g^{-1}h \in G_s$. \square

E.g. 1. $G_0 = \text{Sp}_{\mathbb{R}^2}$ 5. $G_\alpha = \{1\}$ 3. $G_s = \{e\} \forall s$
 $G_x = \text{id}_{\mathbb{R}^2} \forall x \neq 0$ 5. $G_\alpha = \{1, \alpha\}$ 3. $G_l = \{\text{translations parallel to } l\}$

General: bigger orbit \Leftrightarrow smaller stabilizer

Lemma: $H \leqslant G \Rightarrow G$ acts transitively on G/H via $g \cdot aH = gaH$

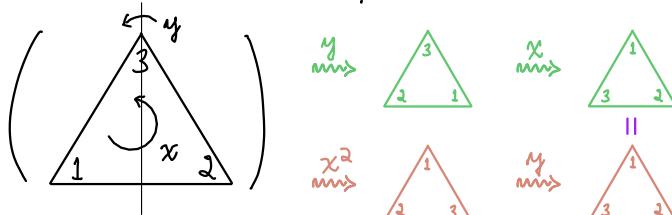
Pf: $(ba^{-1})aH = bH$. \square

$$C \in G/H \Rightarrow gC = \{gc \mid c \in C\}$$

Q. $G_{1+H} = ?$ $H!$

Note: $hH \Rightarrow hH = H$, but h doesn't act trivially on H .

E.g. $G = D_3 = \text{symmetries}$



$$= \langle x, y \mid x^3 = 1, y^2 = 1, xy = yx^2 \rangle$$

$$H = \{1, y\}$$

$$G/H = \left\{ \begin{array}{l} \{1, y\} = C_1 \\ \{x, xy\} = C_2 \\ \{x^2, x^2y\} = C_3 \end{array} \right\}$$

$$x: \begin{array}{c} C_3 \\ \curvearrowright \\ C_1 \\ \curvearrowright \\ C_2 \end{array} \quad (1 \ 2 \ 3)$$

$$y: \begin{array}{c} C_1 \\ \curvearrowright \\ C_2 \\ \curvearrowright \\ C_3 \end{array} \quad (2 \ 3)$$

$$\begin{aligned} &yx^2 = xy \\ &yxy = x^2 \end{aligned}$$

9. Prop: G acts on $X \Leftrightarrow G \rightarrow S_X$ is a homomorphism,
 $g \mapsto \lambda_g$

where $\lambda_g: X \rightarrow X$
 $x \mapsto gx.$ \square

E.g. $D_3 \rightarrow S_3 = \text{permutations}(D_3/H)$

kernel = ? image = ?

$$\begin{aligned} & \cap \\ H \text{ since } g \cdot C_i = C_i \quad \forall i = 1, 2, 3 \Rightarrow gH = H \\ & \Rightarrow g \in H; \end{aligned}$$

but $[y \cdot C_2 = C_3, \text{ so } y \notin \ker(D_3 \rightarrow S_3).]$ Thus $\ker = \{1\}.$

or: $H \not\cong D_3$ since $xyx^{-1} = yx^2 \notin H,$ so $\ker \neq H$

$$\Rightarrow D_3 \cong S_3.$$

Prop: Fix a G -set X and $x \in X$ with stabilizer G_x and orbit $O_x.$

There is a natural bijection $G/H \xrightarrow{\Psi} O_x$ Every transitive group action
 $aH \mapsto ax$ is an action on cosets.

It satisfies $\Psi(gC) = g\Psi(C)$ for $g \in G$ and $C \in G/H.$

$$\begin{aligned} \text{Pf: Need } aH = bH \Rightarrow ax = bx. \text{ But } aH = bH &\Leftrightarrow a^{-1}b \in H \\ &\Leftrightarrow a^{-1}bx = x \end{aligned}$$

Ψ is surjective by construction.

injective by \square

Loose ends 1. $G \leqslant \text{Isom}(\mathbb{R}^2)$ finite $\Rightarrow G \cong C_n$ or $D_n.$

$$\begin{aligned} \text{Need } r \in G \text{ reflection} \Rightarrow G \cong D_n. \text{ Pf: } H = \{\text{rotations in } G\} \leqslant G \\ \Rightarrow H \cong C_n \text{ for some } n \\ \Rightarrow G \supseteq H \cup rH = D_n. \end{aligned}$$

But $g \in G$ reflection $\Rightarrow r^{-1}g$ rotation
 $\text{act on } \Rightarrow g \in rH. \quad \square$

2. Prop: Let $G \subseteq X.$ Fix $x \in X$ and $x' \in O_x,$ say $x' = ax.$

Then $\{g \in G \mid gx = x'\} = aG_x$ and $G_{x'} = aG_xa^{-1}.$

$$\begin{array}{ccc} \text{Pf:} & | & | \\ x \mapsto x' & x \mapsto x & x' \mapsto x. \end{array} \quad \square$$

Counting

Recall: $|G| = |H| \cdot |G/H|$. Let $G \trianglelefteq X$.

Cor: $|G| = |\mathcal{O}_x| \cdot |\mathcal{O}_x|$ for $x \in X$.

Pf: $|G| = |H| [G:H]$ with $H = G_x$ plus bijection $G/H \rightarrow \mathcal{O}_x$. \square

Lemma: $|X| = \sum_{\text{orbits } O} |\mathcal{O}|$.

Pf: X is partitioned by its orbits. \square

E.g. G = orientation-preserving isometries of icosahedron I .

1. Q. $|G| = ?$

A. Every $g \in G$ is a rotation about centroid of I .

- G acts on $F = \{\text{faces of } I\}$. Let $f \in F$.

$$|\mathcal{O}_f| = |F| = ? \quad 20 \quad \text{because } G \text{ acts transitively}$$

$$|G_f| = ? \quad 3 \text{ rotations of } f = \triangle \Rightarrow |G| = 3 \cdot 20 = 60.$$

- G acts on $V = \{\text{vertices of } I\}$. Let $v \in V$.

$$|\mathcal{O}_v| = |V| = ? \quad 12 \quad \text{because } G \text{ acts transitively}$$

$$|G_v| = ? \quad 5 \text{ rotations fixing edges emanating from } v \Rightarrow |G| = 5 \cdot 12 = 60.$$

2. Q. How many edges does I have?

A. G acts on $E = \{\text{edges of } I\}$. Let $e \in E$.

$$|\mathcal{O}_e| = |E| = ? \quad 30 \quad \text{because } G \text{ acts transitively}$$

$$|G_e| = ? \quad 2 \text{ rotations fixing edge } e \Rightarrow |G| = 2 \cdot ? = 60.$$

$$3. V \Rightarrow |V| = 12 = 1 + 1 + 5 + 5$$

\nearrow \nwarrow \nearrow \nwarrow vertex figures of v and $-v$

$H = G_v = \text{stabilizer of } v \text{ for some (any) } v \in V$

$\overset{||}{G}_f = \text{stabilizer of } f \text{ for some (any) } f \in F \Rightarrow 12 = 3 + 3 + 3 + 3$

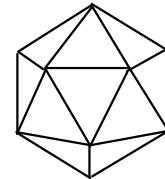
\uparrow
 $H \text{ fixes no vertex}$

Prop: $H, K \leqslant G \Rightarrow [H : H \cap K] \leqslant [G : K]$.

Pf: Let $X = G/K$. Then $G \trianglelefteq X$. Set $x = 1K \in X$.

$$H_x = ? \quad H \cap K$$

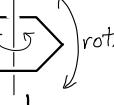
$$[H : H \cap K] = |\mathcal{O}_x| \leqslant |X| = |G/K| = [G : K]. \quad \square$$



10.

Finite rotation groups

Thm: Every finite $G \leq SO_3$ is one of

- C_k cyclic group of rotations by $2\pi m/k$ about a fixed line for $m \in \mathbb{Z}$
- D_k dihedral = symmetries of  rot.
- T symmetries of tetrahedral group $|T| = 12$
- O symmetries of octahedral group $|O| = 24$
- I symmetries of icosahedral group $|I| = 60$

Pf: Set $n = |G|$. $1 \neq g \in G \Rightarrow g$ fixes unique line l

\Rightarrow " " " pair of points in unit sphere S^2
poles in S^2 of g 

G acts on $P = \bigcup_{1 \neq g \in G} \text{poles}(g)$: p is a pole of g and $a \in G$
 $\Rightarrow ap$ is a pole of aga^{-1}

$|P| = ?$ Dunno. Don't care, exactly.

Consider the multiset $M = \{ \text{poles}(g) \mid g \in G \text{ and } g \neq 1 \}$.

$$|M| = 2(n-1) = 2n-2$$

How many times does $p \in P$ appear in M ?

By def, $|G_p| - 1$. Set $r_p = |G_p|$. Then

$$|M| = 2n-2 = \sum_{p \in P} (r_p - 1).$$

Note: $G_p \cong C_{r_p}$ is generated by $\frac{2\pi}{r_p}$ rotation about $l = \text{span}(p)$.

$r_p \geq 2$ since $1 \neq g \in G_p$ if $p \in \text{poles}(g)$.

Let $\mathcal{O}_1, \mathcal{O}_2, \dots$ be the orbits of G in P .

Set $m_i = |\mathcal{O}_i|$.

Observe: $r_p = r_{p'} = \frac{n}{m_i}$ whenever $p, p' \in \mathcal{O}_i$ since $|G_p| \cdot |\mathcal{O}_p| = |G|$

$$\boxed{\quad} \Rightarrow 2n-2 = \sum_i m_i (r_i - 1)$$

$$\Rightarrow 2 - \frac{2}{n} = \sum_i \left(1 - \frac{1}{r_i}\right)$$

$\nearrow < 2 \qquad \searrow \geq \frac{1}{2}$

famous formula

$$\Rightarrow \# \text{ orbits} \leq 3$$

$$\# \text{ orbits} = 1 : \underbrace{2 - \frac{2}{n}}_{\geq 1} = \underbrace{1 - \frac{1}{r}}_{< 1} \rightarrow *$$

$$\# \text{ orbits} = 2 : 2 - \frac{2}{n} = \left(1 - \frac{1}{r_1}\right) + \left(1 - \frac{1}{r_2}\right)$$

$$\frac{2}{n} = \left(\frac{1}{r_1}\right) + \left(\frac{1}{r_2}\right). \quad \text{But } r_i \leq n \text{ since } r_i | n$$

$$\geq \frac{1}{n} \geq \frac{1}{n}$$

$$\Rightarrow r_1 = r_2 = n$$

$$\Rightarrow |\mathcal{O}_1| = |\mathcal{O}_2| = 1$$

$$\Rightarrow P = \{\pm p\} \Rightarrow G = G_p \cong C_n.$$

$$\# \text{ orbits} = 3 : \frac{2}{n} = \frac{1}{r_1} + \frac{1}{r_2} + \frac{1}{r_3} - 1. \quad \text{Assume } r_1 \leq r_2 \leq r_3.$$

$$\text{Then } r_1 = 2, \text{ else } \sum_{i=1}^3 \frac{1}{r_i} \leq 1.$$

Case 1: $r_1 = r_2 = 2$ and $r_3 = r \geq 2$

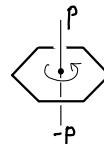
Case 2: $r_3 \geq 3$

$$1. \frac{2}{n} = \frac{1}{r_3} \Rightarrow n = 2r_3 \text{ and } |\mathcal{O}_3| = 2$$

$$\Rightarrow \mathcal{O}_3 = \{\pm p\} \text{ and } G_p = C_{r_3} \text{ about } l = \text{span}(p).$$

Every $g \in G$ fixes r -gon in l^\perp .

$$|G| = 2r \Rightarrow G = D_r$$



$$2. r = (2, r_2, r_3) \quad r_2 \geq 4 \Rightarrow \frac{1}{2} + \frac{1}{r_2} + \frac{1}{r_3} - 1 \leq 0 \rightarrow$$

$$r_2 \geq 3 \quad r_2 = 3 \text{ and } r_3 \geq 6 \Rightarrow \frac{1}{2} + \frac{1}{3} + \frac{1}{r_3} - 1 \leq 0 \rightarrow$$

$$\Rightarrow r \in \begin{cases} (2, 3, 3) \\ (2, 3, 4) \\ (2, 3, 5) \end{cases} \quad \frac{2}{n} = \frac{1}{2} + \frac{1}{3} + \frac{1}{3} - 1 = \frac{7}{6} - 1 = \frac{1}{6} \Rightarrow n = 12$$

$$n = 24$$

$$n = 60$$

$$\text{E.g. } (2, 3, 5) : |\mathcal{O}_3| = \frac{60}{5} = 12.$$

Let $p \in \mathcal{O}_3$ and $q \in \mathcal{O}_2$ a pole nearest to p .

$G_p \cap \mathcal{O}_2$ and $|G_p| = 5 \Rightarrow G_p \cdot q = \text{vertices of a regular pentagon}$

$\Rightarrow \#\{\text{poles nearest to } p\} = 5k$ for some k

Show $k = 1$ and conclude that the $|\mathcal{O}_3| = 12$ pentagons form dodecahedron

$\Rightarrow \mathcal{O}_3 = \text{vertices of icosahedron. } \square$

11.

Cayley's Thm: Every finite group is isomorphic to a subgroup of S_n for some n .

Pf: Let $n = |G|$. $G \subseteq S_n$ by left multiplication.

$$\begin{aligned} G \times G &\rightarrow G \Rightarrow G \xrightarrow{\varphi} S_n \\ (g, x) &\mapsto gx \quad g \mapsto (\lambda_g : x \mapsto gx) \end{aligned}$$

$$gx = x \Rightarrow g = 1$$

\Rightarrow action is faithful: $\ker \varphi = \{1\}$. \square

Pretty, but pretty useless. Other general actions of G on G ?

E.g. conjugation: $G \times G \rightarrow G$

$$(g, x) \mapsto gxg^{-1}$$

$$\text{stabilizer } G_x = \{g \in G \mid gxg^{-1} = x\}$$

$$= \{g \in G \mid gx = xg\}$$

= centralizer $Z(x)$ of $x \in G$.

$$\ker(G \rightarrow S_G) = ?$$

Def: the center $Z(G)$

$$= \{x \in G \mid x \text{ commutes with all } g \in G\}$$

Note: $x \in Z(x)$.

Class Equation: $|G| = \sum_{\substack{\text{conjugacy} \\ \text{classes } C}} |C|$.

• each divides $|G|$ since $|G| = |G_x| \cdot |\mathcal{O}_x|$ for $x \in X$ by Cor, p. 18

• at least one is 1 (why?)

E.g. $G = S_4$: $C_1 \quad C_{(12)} \quad C_{(123)} \quad C_{(12)(34)} \quad C_{(1234)}$

$$1 \quad \binom{4}{2} = 6 \quad 2 \binom{4}{3} = 8 \quad \frac{1}{2} \binom{4}{2} = 3 \quad ? \quad 24 - (\text{the rest})$$

why?

why?

$$(1 \underbrace{\quad}_{3!})$$

$$24 = 1 + 6 + 8 + 3 + 6$$

Observation: $x \in Z(G) \Leftrightarrow Z(x) = G \Leftrightarrow |\text{conjugacy class of } x| \text{ is } |\{x\}| = 1$

Def: G is a p-group for prime p if $|G| = p^e$ for some $e \geq 1$

Prop: G a p-group $\Rightarrow Z(G) \neq \{1\}$.

Pf: $p \mid |C| \forall$ conjugacy classes C except those of size 1. Thus

$$\begin{aligned} p^e = |G| &= 1 + \sum_{\substack{\text{classes} \\ C \neq C_1}} |C| \\ p \text{ divides } &\uparrow \quad \uparrow \quad \uparrow \quad \uparrow \\ \text{but not } &\Rightarrow p \nmid \sum_{C \neq C_1} |C| \Rightarrow |C| = 1 \end{aligned}$$

for some $C \neq C_1$. \square

Cor: p prime \Rightarrow every group of order p^2 is abelian.

Pf: $|Z(G)| \geq p$. $x \notin Z(G) \Rightarrow Z(x) \supseteq \{x\} \cup Z(G)$ Better pf: Midterm 1, #3
 $\Rightarrow |Z(x)| \geq p+1$
 $\Rightarrow |Z(x)| = p^2$
 $\Rightarrow x \text{ commutes with everything}$
 $\Rightarrow x \in Z(G) \rightarrow \star. \quad \square$

Cor: $|G| = p^2 \Rightarrow G \cong \underbrace{C_p}_{} \text{ or } \underbrace{C_p \times C_p}_{}.$

Pf: $|x|=p^2$ for some $x \in G$ $|x|=p \forall x \in G. \quad \square$

Note: $|G|=8 \Rightarrow 5$ possibilities
 $|G|=16 \Rightarrow 14$ possibilities

not all abelian

The icosahedral group \mathbb{I}

Def: G is simple if its only normal subgroups are $\{1\} \neq G$.

E.g. C_p is simple.

Thm: \mathbb{I} is simple.

Pf: Lemma: $N \trianglelefteq G \Rightarrow N$ is a (disjoint) union of conjugacy classes.

Pf: $x \in N \Rightarrow gxg^{-1} \in N \quad \forall g \in G. \quad \square$

Lemma $\Rightarrow |N| = \sum_{\substack{\text{classes } C \\ \text{of } G \text{ contained} \\ \text{in } N}} |C|$. Class eqn. for \mathbb{I} : $60 = 1 + 15 + 20 + 12 + 12$
will prove later

and no subsum containing 1 divides 60. \square

Cor: $A_5 \cong \mathbb{I}$ is simple.

Pf: \mathbb{I} acts on 5 cubes [demonstrate]

$\Rightarrow \mathbb{I} \xrightarrow{\varphi} S_5$. $\underbrace{\ker \varphi \neq \mathbb{I}}$ since moves at least one cube.

$\Rightarrow \ker \varphi = \{1\}$ by Thm since $\ker \varphi \trianglelefteq \mathbb{I}$

$\Rightarrow \mathbb{I} \hookrightarrow S_5$.

$[S_5 : \mathbb{I}] = 2$. sign: $S_5 \rightarrow \{\pm 1\}$ $\ker \text{sign}|_{\mathbb{I}} \trianglelefteq \mathbb{I}$

induces $\mathbb{I} \rightarrow \{\pm 1\}$.

$\Downarrow = \mathbb{I}$ by Thm, since index is 1 or 2

$\Rightarrow \mathbb{I} \trianglelefteq \ker(\text{sign}) \Rightarrow \mathbb{I} = \ker(\text{sign}) = A_5$ by def. \square

12.

Class eqn for $I: 60 = 1+15+20+12+12$

$ g $	#
1	1

(1)

x	$ I_x $	# copies $\leq I$
face f	3	$20/2 = 10 \leftarrow$ all conjugate, since
edge e	2	$30/2 = 15 \leftarrow I$ acts transitively on
vertex v	5	$12/2 = 6 \leftarrow$ faces, edges, and vertices antipodal pairs

 $2 \geq 15 \quad \text{all } I_e \text{ conjugate} \Rightarrow 15$ $3 \geq 10 \cdot 2 = 20 \quad "I_f" \Rightarrow 20 = 20 \text{ or } 10 + 10. \text{ But } I_f = \{1, h, h^2\} \Rightarrow h = \frac{2\pi}{3} \text{ rotation around pole}(f)$
 $5 \geq 6 \cdot 4 = 24 \quad \text{similarly, } I_v = \{1, g, g^2, g^3, g^4\} \Rightarrow 24 = 12 + 12. \quad \square \Rightarrow h^2 = " \quad \text{pole}(-f)$
 $\Rightarrow h \sim h^2.$ But $1+15+20+24=60$, so that's all.

Q. Why isn't this the class eqn?

A. $24 \nmid 60$ Actions on subsets

$G \curvearrowright X \Rightarrow G \curvearrowright 2^X = \{\text{subsets of } X\}$

 $U \subseteq X \Rightarrow gU = \{gu \mid u \in U\} \text{ same size as } U$

$\Rightarrow G \curvearrowright \binom{X}{d} = \{U \subseteq X \mid |U|=d\}$

E.g. $G = \text{octahedral group} \curvearrowright \boxed{\text{cube}} \Rightarrow G \curvearrowright X = \{\text{vertices of } \boxed{\text{cube}}\}$

$\binom{|X|}{2} = \binom{8}{2} = 28 \text{ pairs of vertices}$

3 orbits: $\bullet O_1 = \text{pairs of vertices on an edge} \quad \# = 12$ $\bullet O_2 = \text{" a face diagonal} \quad \# = 6 \cdot 2 = 12$ $\bullet O_3 = \text{" body diagonal} \quad \# = 8/2 = 4 \quad 28 = 12+12+4$ Note again: $gU = U \Rightarrow g \text{ permutes } U: \text{not } gu = u \text{ but } gue \in u$ Lemma: If $H \curvearrowright X$ and $U \subseteq X$ then H stabilizes U ($H_U = H$) $\Leftrightarrow U$ is a union of H -orbits.Pf: H stabilizes $U \Leftrightarrow O_u = Hu \subseteq U \quad \forall u \in U. \quad \square$ Prop: Let $G \curvearrowright G$ by left multiplication. Then $|G_U| \mid |U|$ Pf: Set $H = G_U$. Lemma $\Rightarrow U = \bigcup_{\substack{\text{H-orbits} \\ \text{right cosets } Hu}}$ right cosets Hu

$\Rightarrow |U| = \sum_{\text{H-orbits } O} |O| = k|H|. \quad \square$

Cor: $\gcd(|U|, |G|) = 1 \Rightarrow G_U = \{1\}$.Pf: $|G_U| \mid |G|$ and $|G_U| \mid |U|.$ \square

E.g. $G \trianglelefteq G$ by conjugation. $H \leq G \Rightarrow G_H$ is the normalizer

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}.$$

$$\# \text{subgroups conjugate to } H = ? \quad |G| / |N(H)| \quad |O_H| \cdot |G_H| = |G| \\ = [G : N(H)].$$

Notes: • $H \trianglelefteq N_G(H)$ and $N(H)$ maximal with this property.

$$\cdot N_G(H) = G \Leftrightarrow H \trianglelefteq G.$$

The Sylow theorems

Fix group G and prime p with $|G| = p^e m$ and $p \nmid m$. Assume $e \geq 1$.

First Sylow Thm: G has a subgroup of order p^e . Sylow p -subgroup

proofs next time

Cor: G has an element of order p .

Pf: Let H be a Sylow p -subgroup and $1 \neq g \in H$.

$$|g| = p^r \text{ for some } r \leq e \Rightarrow |g^{p^{r-1}}| = p. \quad \square$$

Second Sylow thm: Let $K \leq G$ with $p \mid |K|$ and $H \leq G$ a Sylow p -subgroup.

Then $(gHg^{-1}) \cap K$ is a Sylow p -subgroup of K for some $g \in G$.

Cor: 1. $K \leq G$ is a p -group $\Rightarrow K \leq$ some Sylow p -subgroup of G .

2. All Sylow p -subgroups of G are conjugate.

Pf: 1. Pick H as in Sylow 2. Then $K \leq gHg^{-1}$ by def.

But gHg^{-1} is a Sylow p -subgroup of G .

2. Part 1 + $K = gHg^{-1}$ if $|K| = |gHg^{-1}|$. \square

Third Sylow Thm: Let $s = \#\text{Sylow } p\text{-subgroups of } G$, where $|G| = p^e m$.

Then $s \mid m$ and $s \equiv 1 \pmod{p}$.

E.g. $|G| = 15 \Rightarrow G \cong C_{15}$ $n = 15 = 3 \cdot 5$

$p = 3$, $m = 5$: $s \mid 5$ and $s \equiv 1 \pmod{3}$.

$$s \in \{1, 5\} \quad \Rightarrow s = 1 \Rightarrow \text{Sylow 3-subgroup } H \trianglelefteq G$$

$$p = 5, m = 3: s \mid 3 \text{ and } s \equiv 1 \pmod{5}. \Rightarrow s = 1 \Rightarrow \text{Sylow 5-subgroup } K \trianglelefteq G$$

HW2 #21 $\Rightarrow G$ abelian

$$\Rightarrow G \cong C_3 \times C_5 \cong C_{15}.$$

13.

Semidirect products

Note: $\forall k \in K \leq G$ and $H \trianglelefteq G \Rightarrow khk^{-1} \in H$

$h \mapsto khk^{-1}$ is an automorphism $\varphi_h: H \rightarrow H$

Def: Fix a homomorphism $K \rightarrow \text{Aut } H$. The semidirect product of H and K is
 $k \mapsto \varphi_k$

$H \rtimes K = (H \times K, \cdot)$ with $(h, k) \cdot (h', k') = (h\varphi_k(h'), kk')$

The point: $khk^{-1} = \varphi_k(h) \Rightarrow h(kh)k' = h\underbrace{k\varphi_k(h)k'}_{\varphi_k(h')}k'$.

Lemma: $H \trianglelefteq H \rtimes K$ and $khk^{-1} = \varphi_k(h) \quad \forall k \in K \text{ and } h \in H$. \square

E.g. $|G| = 21 \quad p = 7, \quad m = 3 \Rightarrow s \mid 3 \text{ and } s \equiv 1 \pmod{7} \Rightarrow s = 1$

\Rightarrow Sylow 7-subgroup $H \triangleleft G$

$p = 3, \quad m = 7 \Rightarrow s \mid 7 \text{ and } s \equiv 1 \pmod{3} \Rightarrow s = \{1, 7\}$

\Rightarrow Sylow 3-subgroup K might be normal in G or not.

$K \triangleleft G \Rightarrow G \cong C_3 \times C_7 \cong C_{21}$ as in $|G| = 15$ case.

$K \not\triangleleft G \Rightarrow G$ not abelian, but still $H \cap K = \{1\} \Rightarrow |HK| = |H| \cdot |K| = 7 \cdot 3 = 21 = |G|$

$\Rightarrow G = HK. \quad H \triangleleft G \Rightarrow G \cong H \rtimes K$, but for which $\varphi: K \rightarrow \text{Aut } H$?
 $k \mapsto \varphi_k$

$H = \{1, h, h^2, \dots, h^6\}. \quad \text{Aut } H \cong C_6 \Rightarrow \varphi_k: x \mapsto x^a \text{ for } a \in \{2, 4\} \text{ since } \varphi_k(h)^3 = h^{a^3} = h$
 $\Rightarrow khk^{-1} = h^2 \text{ or } h^4. \quad 2^3 = 7+1, \quad 4^3 = 63+1$

But these yield isomorphic semidirect products under $k \mapsto k^2$.

$\therefore |G| = 21 \Rightarrow G \cong C_{21}$ or $G \cong C_7 \rtimes C_3$ (and there's only one such \rtimes)

Proofs of the Sylow thms

setup: p prime, $|G| = n = p^e m$, $p \nmid m$, $e \geq 1$

Sylow 1: $\exists H \leq G$ with $|H| = p^e$.

Lemma: $p \nmid \binom{n}{p^e} = \frac{n(n-1)\cdots(n-p^e+1)}{p^e(p^e-1)\cdots(p^e-p^e+1)}$.

Pf: Given $1 \leq k \leq p^e - 1$, write $k = p^f l$ with $p \nmid l$. Then

$$\left. \begin{aligned} n-k &= p^e - p^f l = p^f(p^{e-f}m - l) \\ p^e - k &= p^e - p^f l = p^f(p^{e-f} - l) \end{aligned} \right\} \Rightarrow \text{ord}_p\left(\frac{n-k}{p^e - k}\right) = \text{ord}_p\left(\frac{p^{e-f}m - l}{p^{e-f} - l}\right) = 0. \quad \square$$

Pf of Sylow 1: $G \setminus \binom{G}{p^e} = \text{union of orbits } \mathcal{O}$

$$\Rightarrow \binom{G}{p^e} = \sum_{\text{orbits } \mathcal{O}} |\mathcal{O}|$$

Lemma $\Rightarrow \binom{G}{p^e} \equiv 0 \pmod{p} \Rightarrow |\mathcal{O}| \not\equiv 0 \pmod{p}$ for some \mathcal{O} . Let $U \in \mathcal{O}$.

$$\text{Then } |G_U| \cdot |\mathcal{O}| = |G| = p^e m \Rightarrow p^e \mid |G_U|.$$

But $|G_U| \mid |U| = p^e$ by Prop p. 23. Set $H = G_U$. \square

Sylow 2: Fix $K \leq G$ with $p \mid |K|$. Sylow p -subgroup $H \leq G \Rightarrow$ Sylow p -subgroup $(gHg^{-1}) \cap K$.

Pf: $G \setminus X = G/H$. $|X| = m \not\equiv 0 \pmod{p} \Rightarrow \exists K\text{-orbit } \mathcal{O}$ with $p \nmid |\mathcal{O}|$.

$$\begin{aligned} x \in \mathcal{O} \Rightarrow x = gH \text{ for some } g \in G. \quad G_x &= ? \quad gHg^{-1} \quad agH = gH \Leftrightarrow g^{-1}ag \in H \\ &\Leftrightarrow a \in gHg^{-1} \\ \Rightarrow K_x &= (gHg^{-1}) \cap K \end{aligned}$$

$$\left. \begin{aligned} [K:(gHg^{-1}) \cap K] &= [K:K_x] = |\mathcal{O}| \text{ prime to } p. \\ |gHg^{-1}| &= p^e \Rightarrow (gHg^{-1}) \cap K \text{ is a } p\text{-group.} \end{aligned} \right\} \Rightarrow \begin{aligned} |K|/|(gHg^{-1}) \cap K| &\text{ has no } p \\ |(gHg^{-1}) \cap K| &\text{ is all } p \text{ (} p\text{-group)} \\ \Rightarrow (gHg^{-1}) \cap K &\leq K \text{ is a Sylow } p\text{-subgroup.} \end{aligned} \quad \square$$

Sylow 3: #Sylow p -subgroups of G divides m and $\equiv 1 \pmod{p}$.

Pf: $G \setminus X$ transitive by Cor 2 of Sylow 2

$$\Rightarrow |X| = [G:N] \text{ for } N = N_G(H), \text{ where } H \in X \text{ is arbitrary.}$$

$$H \leq N \Rightarrow [G:N] \mid [G:H] = m. \checkmark$$

$H \subset X$. Q. When does H stabilize $H' \in X$?

$$A. \Leftrightarrow hH'h^{-1} = H' \forall h \in H$$

$$\Leftrightarrow H \leq N_G(H').$$

But $H \leq N_G(H')$ is a normal Sylow p -subgroup of $N_G(H')$.

Since $H \leq N_G(H')$, it is also a Sylow p -subgroup.

Thus $H = H'$, since all Sylow p -subgroups are conjugate (Cor 2 of Sylow 2).

Conclusion: $H \subset X$ with only one orbit of size 1, and

$$p \mid |\mathcal{O}| \quad \forall \text{ other orbits } \mathcal{O} \neq \{H\}$$

$$\Rightarrow |X| \equiv 1 \pmod{p}. \quad \square$$

14.

Groups of order 12Fix • a group G with $|G| = 12$ • $H \leq G$ a Sylow 2-subgroup $|H| = ? \cancel{4}$ • $K \leq G$ a Sylow 3-subgroup $|K| = ? \cancel{3}$ Sylow 3 $\Rightarrow H$ has 1 or 3 conjugates $|3 \text{ and } \equiv 1(2)$ K has 1 or 4 conjugates $|4 \text{ and } \equiv 1(3)$ $H \cong C_4$ or $H \cong C_2 \times C_2$ Klein 4-groupLemma: $H \triangleleft G$ or $K \triangleleft G$ or both.Pf: $K \not\triangleleft G \Rightarrow 4$ conjugates of K $\Rightarrow 8$ elements of order 3 in G $\Rightarrow 4$ elements remain.Since H has no elements of order 3, $H = G \setminus \{\text{elements of order 3}\}$. $H \triangleleft G$ since same is true of gHg^{-1} . \square Lemma $\Rightarrow G = H \times K$ if both are normal $H \rtimes K$ if $K \not\triangleleft G$ $K \rtimes H$ if $H \not\triangleleft G$ • $H \times K$: $G \cong C_4 \times C_3$ or $G \cong C_2 \times C_2 \times C_3$ • $H \rtimes K$: $G \subset X = \{\text{conjugates of } K\}$ by conjugation

$$|X| = 4 \Rightarrow G \rightarrow S_4$$

$$X = \{K_1, \dots, K_4\}$$

$$\ker(G \rightarrow S_4) = \bigcap_{i=1}^4 N_G(K_i)$$

$$N_G(K_i) = |G_{K_i}| = |G| / |\mathcal{O}_{K_i}| = 12/4 = 3$$

$$\Rightarrow N_G(K_i) = K_i$$

$$\Rightarrow \bigcap_{i=1}^4 N_G(K_i) = \{1\}$$

$$\Rightarrow G \hookrightarrow S_4.$$

But G has 8 elements of order 3 in S_4
 generated by 3-cycles

(why? $|\text{subgroup}| \mid |G| = 12$)

\Rightarrow every permutation in G is even

$\Rightarrow G = A_4$ since $|A_4| = 12$.

Note: $H \cong C_2 \times C_2$ is forced

- $K \rtimes H$: Let $K = \{1, y, y^2\}$.

$$\text{Aut } K \cong C_2 = \{\text{id}_K, (y \leftrightarrow y^2)\}$$

Case 1: $H \cong C_4 \Rightarrow \exists!$ nontrivial $H \rightarrow \text{Aut } K$

$$\begin{array}{ll} \{1, x, x^2, x^3\} & x \mapsto (y \leftrightarrow y^2) \\ & x^2 \mapsto \text{id}_K \end{array}$$

$$G = \langle x, y \mid x^4 = 1, y^2 = 1, xyx^{-1} = y^2 \rangle.$$

Case 2: $H \cong C_2 \times C_2'$

$$H \xrightarrow{\varphi} \text{Aut } K \text{ nontrivial} \Rightarrow \exists! u \in H \text{ with } u: y \mapsto y \\ u \neq 1$$

$$\langle u \rangle = \ker \varphi; \text{ choose this to be } C_2'$$

$$\left. \begin{array}{l} C_2 \hookrightarrow \text{Aut } K \\ C_2' \text{ commutes with } K \end{array} \right\} \Rightarrow G = (K \rtimes C_2) \times C_2' \\ \cong S_3 \times C_2 \\ \cong D_6 \quad [\text{M1}\#1(c)].$$

Conclusion: #(groups of order 12) = 5.

15.

Free groups

Thm: Fix a set X . There is a free group F on X with the following universal property:

for any group G , $\text{maps}(X \rightarrow G) = \text{Hom}(F, G)$. = {homomorphisms $F \rightarrow G$ }

Intuition: F is generated by X with "no relations" Compare: B = basis for vector space V
 $\Rightarrow \text{maps}(B \rightarrow W) = \text{Hom}(V, W)$ \forall v.s. W

Def: A word on X of length n is an element $w \in X^n$. e.g. $X = \{a, \dots, z\}$ $w = \text{aardvark}$

$W = \bigcup_{n=0}^{\infty} X^n$ is the free semigroup on X : $v \cdot w = vw$ aardvark · syzygy = aardvarksyzygy

$X^{-1} = \{x^{-1} \mid x \in X\}$ $X' = X^{-1} \cup X$ Set $(x^{-1})^{-1} = x$ for $x^{-1} \in X^{-1}$.

Def: The equivalence relation \sim on W' = free semigroup on X' is the transitive closure of

$v \sim w$ if $v = v_1 y y^{-1} v_2$ and $w = v_1 v_2$ for some $y \in X'$. determined by

$w \in W'$ is reduced if no string $y y^{-1}$ appears in w .

Lemma: $w \sim w_0$ for some reduced w_0 . \square

e.g. $\text{bab} \cancel{b} \cancel{b} \cancel{a} \cancel{c} \cancel{c} \cancel{a} = \text{bab} \cancel{b} \cancel{a} \cancel{c} \cancel{a}$

Prop: w reduces to unique reduced w_0 by a sequence of cancellations.

$\text{ba} \cancel{a} \cancel{c} \cancel{c} \cancel{a}$ $\text{ba} \cancel{b} \cancel{a} \cancel{a}$

Pf: Induct on length $l(w)$.

Notation: $w \rightsquigarrow v$ if w reduces to v .

$\cancel{b} \cancel{a} \cancel{c} \cancel{a}$ $\cancel{b} \cancel{a} \cancel{b}$

$l(w) = 0 \Rightarrow w = 1$ (empty word) is reduced.

ba ba

$l(w) > 0$: Assume $w \rightsquigarrow w_0 \neq w$ (else done) starts $w, \cancel{x} \cancel{x^{-1}} w_0$.

Suffices: $w \rightsquigarrow w_0' \Rightarrow w, w_2 \rightsquigarrow w_0'$, since already $w, w_1 \rightsquigarrow w_0$.

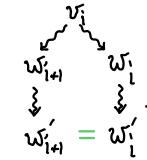
In w_0 , x or x' must go. • Both simultaneously: may as well do them first.

• One first \Rightarrow at $\cdots \cancel{x} \cancel{x^{-1}} \cdots$ or $\cdots \cancel{x} \cancel{x} \cdots$

\Rightarrow same as if xx^{-1} had been canceled first. \square

Cor: w_0 in Lemma is unique, and $w \rightsquigarrow w_0$.

Pf: $w \sim w_0' \Rightarrow w, \cancel{x}, \dots, \cancel{x}, w_0' \rightsquigarrow w_0$, and may as well assume w_i reduced $\forall i < r$ since



But then $= \forall i$ and $w_0 = w_r'$ by Prop. \square

Prop: $v \sim v'$ and $w \sim w' \Rightarrow vw \sim v'w'$.

Pf: $vw \rightsquigarrow v_0 w_0 \rightsquigarrow (v_0 w_0)_0 \rightsquigarrow v_0 w_0 \rightsquigarrow v_0 w' \rightsquigarrow v'w'$. \square

Cor: $F_X = W'/\sim$ is a group. \square E.g. $X = \{a\} \Rightarrow F_X \cong C_\infty$

Pf of Thm: Given $f: X \rightarrow G$ and $w = x_1^{z_1} \cdots x_n^{z_n} \in W'$, define $\varphi: F_X \rightarrow G$ by

$F_X \times F_X \rightarrow F_X$ ✓
 assoc. since concatenation is
 $1 \cdot w = w \cdot 1$ by def.
 $(xy \cdots z)^{-1} = z^{-1} \cdots y^{-1} x^{-1}$

$\varphi(w) = f(x_1)^{z_1} \cdots f(x_n)^{z_n}$. Then $w \sim w' \Rightarrow \varphi(w) = \varphi(w')$ since G is a group.

φ is a homomorphism by construction. \square $\varphi(vw) = \varphi(x_1^{z_1} \cdots x_n^{z_n} y_1^{z_1} \cdots y_m^{z_m}) = f(x_1)^{z_1} \cdots f(y_m)^{z_m} = \varphi(v)\varphi(w)$.

Generators and relations

- Notes: • $X \subseteq G$ generating set $\Leftrightarrow F_x \twoheadrightarrow G$.
- $X \subseteq G \Rightarrow \text{im}(F_x \rightarrow G) = \langle X \rangle \leq G$ subgroup generated by X

Def: If $\langle X \rangle = G$ then $\ker(F_x \rightarrow G) = N \trianglelefteq F_x$ consists of the relations on X .

So $N = \{\text{equivalence classes of words on } X' \text{ whose product in } G \text{ is 1}\}$.

E.g. $S_3 = G \ni X = \{(12), (23)\} \Rightarrow N = \{x^2, y^2, xyxyxy, xy^2x, xy^2x^{-1}, \dots\}$

Who wants to write them all?

Def: If $G = \langle X \rangle$ then $R \subseteq W'$ is a set of defining relations if

$N = \ker(F_x \rightarrow G)$ is the smallest normal subgroup of F_x containing R .

- Notes: • R need not generate N . Why? $F_x \rightarrow G$ group homomorphism $\Rightarrow N \trianglelefteq F_x$ and $G \cong F_x/N$.
- F_x has non-normal subgroups if $|X| \geq 2$ since $\exists G = \langle x, y \rangle \geq H$ with $H \not\trianglelefteq G$. e.g. $\langle (12) \rangle \leq S_3$

Thm (Universal property of quotient groups):

Fix $N \trianglelefteq G$ and $\bar{G} = G/N$ with $\pi: G \rightarrow \bar{G}$
 $a \mapsto aN$.

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ \pi \downarrow & \nearrow \exists! \bar{\varphi} & \\ \bar{G} & & \end{array}$$

$\Psi: G \rightarrow G'$ and $N \trianglelefteq \ker \Psi \Rightarrow \exists! \bar{\Psi}: \bar{G} \rightarrow G'$ with $\Psi = \bar{\Psi} \circ \pi$.

Pf: Exercise. (!!) Main point: partition of G by G/N refines partition by $G/\ker \Psi$ — it's the map of sets that matters.

E.g. $D_n = \langle x, y | x^n, y^2, xyxy \rangle$ defining relations: $D_n \cong F_{\{x,y\}}/N$ $x^n, y^2, xyxy \in N \trianglelefteq F_{\{x,y\}}$ minimal

Pf: $x = \text{rotation by } 2\pi/n$
 $y = (\text{any}) \text{ reflection}$ $\left. \begin{array}{l} x^n = 1, y^2 = 1, \text{ and } (xy)^2 = 1 \\ \end{array} \right\}$

$D_n = \langle x, y \rangle \Rightarrow F_{\{x,y\}} \xrightarrow{\Psi} D_n$ surjective.

$\begin{array}{l} \ker \Psi \trianglelefteq F_{\{x,y\}} \\ \ker \Psi \supseteq R \end{array} \Rightarrow \begin{array}{l} \ker \Psi \geq N \\ \Rightarrow F_{\{x,y\}}/N \xrightarrow{\bar{\Psi}} D_n \end{array}$

Need: $\bar{\Psi}$ injective. Enough: $|F_{\{x,y\}}/N| \leq 2n$.

Ex: Using R , every word in $x^{\pm 1}, y^{\pm 1}$ can be put into the form

$(x^i y^j \text{ with } i \in \{0, \dots, n-1\} \text{ and } j \in \{0, 1\}) = 2n$. \square

Q. Given $R \subseteq F_x$ and $v, w \in X'$, is $v = w$ in $\langle X | R \rangle$?

A. word problem: \exists no algorithm with bounded time complexity!

Q. $\langle X | xyx^{-1}y^{-1} \text{ for } x, y \in X \rangle = ?$ free abelian group on $X = \mathbb{Z}^X$.

16.

Simplicity of A_n Thm: A_n is simple if $n \geq 5$.

Reorganize proof as in 23/026 photo

Pf: Induction on n . $n = 5: A_5 \cong I$ is simple by Cor p. 22Assume $n \geq 6$. Let $H \trianglelefteq A_n$.Set $G_i = G_{A_n}(i)$, so $G_i \cong A_{n-1} \leq A_n$ simple $\forall i = 1, \dots, n$. $1 \neq \pi \in H$ with $\pi(i) = i \Rightarrow |H \cap G_i| \geq 1$ $\Rightarrow H \geq G_i$ since $H \trianglelefteq A_n$.But $\sigma \in A_n \Rightarrow \sigma G_i \sigma^{-1} = G_{\sigma(i)}$ $\Rightarrow H \geq G_j \quad \forall j$, again since $H \trianglelefteq A_n$.Every $\rho \in A_n$ is a product of an even # of transpositions
 $= \text{ " " } \underbrace{\text{some # of pairs of transpositions}}_{\text{each lies in } G_i \text{ for some } i, \text{ as } n \geq 5}$
Hence $\langle G_1, \dots, G_n \rangle = A_n$, so $H = A_n$.So assume $\pi(i) \neq i \quad \forall \pi \in H \setminus \{1\}$ and $\forall i \in \{1, \dots, n\}$.Then $\pi_1(i) = \pi_2(i) \Rightarrow \pi_1 = \pi_2$ in H because \downarrow
 $\pi_1^{-1} \pi_2(i) = i$ Suppose π has a ≥ 3 -cycle (a_1, a_2, a_3, \dots) in its cycle decomposition.Fix $\sigma \in A_n$ with $\sigma(a_1) = a_1$,and $\sigma(a_2) = a_2$ but $\sigma(a_3) \neq a_3$, possible because $n \geq 5$: $(a_3 a_4 a_5)$.Then $\pi' = \sigma \pi \sigma^{-1}$ has the ≥ 3 -cycle $(a_1, a_2, \sigma(a_3), \dots)$ in its cycle decomposition.(*) $\pi'(a_1) = \pi(a_1) = a_2 \Rightarrow \pi \notin H$, else $\pi' \in H$ since $H \trianglelefteq A_n$, so $\pi^{-1} \pi'(a_1) = a_1$.Now suppose $\pi = (a_1 a_2)(a_3 a_4)(a_5 a_6) \dots$ = product of disjoint transpositions.Set $\sigma = (a_1 a_2)(a_3 a_5) \in A_n$. Then

$$\pi' = \sigma \pi \sigma^{-1} = (a_2 a_1)(a_5 a_4)(a_6 a_3) \dots$$

 $\Rightarrow (*)$ again $\Rightarrow \pi \notin H$

$$\Rightarrow |H| = 1. \quad \square$$

Composition series and related concepts

Def: A composition series of a group G is a chain

$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{l-1} \trianglelefteq G_l = G$ such that $\underbrace{G_i/G_{i-1}}$ is simple $\forall i = 1, \dots, l$.
composition factor \bar{G}_i

E.g. $\begin{aligned} & 1 \trianglelefteq A_n \trianglelefteq S_n \quad \forall n \geq 5 \Rightarrow \bar{G}_1 = A_n \text{ and } \bar{G}_1 = ? C_2 \\ & \leftarrow \begin{array}{c} \cdot 1 \trianglelefteq C_2 \trianglelefteq V_4 \trianglelefteq A_4 \trianglelefteq S_4 \\ \text{go this way} \end{array} \Rightarrow \begin{array}{c} \bar{G}_i = C_2, C_2, C_3, C_2 \\ i=1 \ 2 \ 3 \ 4 \end{array} \end{aligned}$

Jordan - Hölder Thm: All composition series of finite G yield the same isomorphism classes and multiplicities of $\bar{G}_1, \dots, \bar{G}_l$ up to permutation.

Def: G is solvable if $|\bar{G}_i|$ is prime $\forall i$. "solvable" has roots in Galois theory

E.g. S_n is solvable if $n \leq 4$ but not if $n \geq 5$. How to tell if G is solvable?

Prop: Set $G' = [G, G] = \langle xyx^{-1}y^{-1} \mid x, y \in G \rangle$ commutator subgroup and

$G = G^0 \geq G^1 \geq \cdots \geq G^i \geq \cdots$ with $G^{i+1} = (G^i)'$, the derived series of G .

Then finite G is solvable $\Leftrightarrow G^m = \{1\}$ for some m .

Pf: Lemma: G/N is abelian $\Leftrightarrow N \geq [G, G]$.

Pf: $\begin{array}{c} \updownarrow \\ xyx^{-1}y^{-1} \in N \quad \forall x, y \in G \end{array} \quad \square$

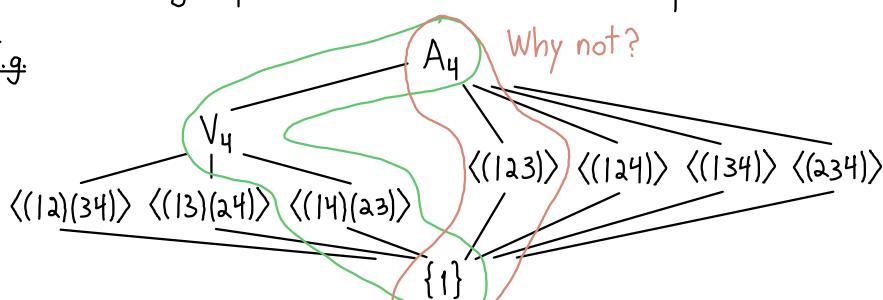
\Leftarrow : Refine the derived series.

\Rightarrow : Need $G^i \neq \{1\} \Rightarrow (G^i)' \neq G^i$. Jordan - Hölder $\Rightarrow G^i$ has an abelian quotient $C_p = G^i/H$
 $\Rightarrow G^i \geq H \geq (G^i)'$. \square

Q. What do all composition series look like, together in G ?

A. The subgroup lattice of G is $\Lambda(G)$ = poset of all subgroups of G .

E.g.



Q. $N \trianglelefteq G \Rightarrow \Lambda(G/N) = ?$ A. $\{\bar{H} \leq \bar{G} \mid N \trianglelefteq H \leq G\}$, where $\bar{-}$ means $/N$

and $\bar{H} \leq \bar{G} \Leftrightarrow H \trianglelefteq G$

Ex: $N \trianglelefteq H \trianglelefteq G$ with $N \trianglelefteq G \Rightarrow G/H \leftrightarrow \bar{G}/\bar{H} \cong \text{if } H \trianglelefteq G$ one of the isomorphism theorems

17.

RingsDef: A is a ring if it has

Anneau

$$+: A \times A \rightarrow A$$

$$\cdot : A \times A \rightarrow A$$

with $\cdot (A, +)$ abelian group $\cdot (A, \cdot)$ monoid

$$\text{distributivity: } x(y+z) = xy + xz$$

$$\text{and } (y+z)x = yx + zx \quad \forall x, y, z \in A$$

E.g. Why is $- \cdot - = +$?

$$1 + (-1) = 0 \Rightarrow x + (-1)x = 0x \quad 0 + 0 = 0 \quad \text{by def of identity}$$

$$\Rightarrow (-1)x = -x$$

$$\Rightarrow 0x + 0x = 0x$$

$$\Rightarrow -(xy) = (-x)y$$

$$\Rightarrow 0x = 0$$

$$\Rightarrow -(xy) + (-x)(-y) = (-x)y + (-x)(-y)$$

$$= (-x)(y + (-y))$$

$$= 0$$

$$\Rightarrow xy = (-x)(-y)$$

Def: $u \in A$ is a unit if $\exists v \in A$ with $uv = 1$
 and $w \in A$ with $wu = 1$

$$\Rightarrow w(uv) = (wu)v$$

$$\Rightarrow w = v.$$

 $A^* = \text{unit group of } A$

E.g. 1. $A = \mathbb{k}[x] = \{a_0 + a_1x + \dots + a_dx^d \mid d \in \mathbb{N} \text{ and } a_0, \dots, a_d \in \mathbb{k}\} \Rightarrow A^* = \mathbb{k}^*$

2. $\mathbb{Z}^{\mathbb{N}} = (a_0, a_1, \dots) \Rightarrow R = \text{Hom}_{\text{Ab}}(\mathbb{Z}^{\mathbb{N}}, \mathbb{Z}^{\mathbb{N}})$

$= \{f: \mathbb{Z}^{\mathbb{N}} \rightarrow \mathbb{Z}^{\mathbb{N}} \mid f(\underline{a} + \underline{b}) = f(\underline{a}) + f(\underline{b})\}$ is a ring.

PF?

$T(a_0, a_1, \dots) = (0, a_0, a_1, \dots) \Rightarrow T$ has left inverse but not right.

3. $A^* = A \setminus \{0\} \Rightarrow A$ is a division ring (skew field)

and $xy = yx \quad \forall x, y \in A \Rightarrow A$ is a field

A is a commutative ring note: not "abelian"

4. \mathbb{Z} is a commutative integral domain (\mathbb{Z} is entire): $\neq 0$ and $ab = 0 \Rightarrow a = 0$ or $b = 0$ (34)

5. $\mathbb{Z}/6\mathbb{Z}$ is commutative with zero divisors: $\bar{2} \cdot \bar{3} = \bar{6} = 0$ in $\mathbb{Z}/6\mathbb{Z}$

6. monoid algebras: monoid G and ring A

$$\Rightarrow R = A[G] = \left\{ \sum_{g \in G} a_g g \mid \text{almost all } a_g = 0 \right\} \quad \text{e.g. } R = \mathbb{k}[x] = \mathbb{k}[\mathbb{N}]$$

$$\alpha = \sum_{g \in G} a_g g \quad \text{and} \quad \beta = \sum_{g \in G} b_g g \Rightarrow \alpha \beta = \sum_{g \in G} \sum_{h \in G} a_g b_h g h$$

convolution product

$$= \sum_{x \in G} \left(\sum_{gh=x} a_g b_h \right) x$$

This is just the usual product on polynomials

7. function rings X set (top. space manifold analytic space complex manifold algebraic variety)

yes if $|X| \geq 2$ R ring \mathbb{R} \mathbb{R} \mathbb{R} \mathbb{C} \mathbb{k} Körper

$$A = \{f: X \rightarrow R\} \quad \text{continuous} \quad C^\infty \quad \text{analytic} \quad \mathbb{C}\text{-analytic} \quad \text{algebraic}$$

$$f+g: x \mapsto f(x)+g(x) \quad \text{yes} \quad \text{yes} \quad \text{no} \longrightarrow$$

$$fg: x \mapsto f(x)g(x)$$

commutative? yes if R is

zero divisors?

8. matrix rings $M_n(R) = n \times n$ matrices with entries in ring R

$$\mathbb{k} \text{ field} \Rightarrow M_n(\mathbb{k})^* = GL_n \mathbb{k} \quad (\det \neq 0)$$

commutative? only if $n=1$ and R is commutative

zero divisors? yes unless $n=1$ and R is an integral domain

Def: $f: A \rightarrow B$ is a ring homomorphism if

$$(A, +) \rightarrow (B, +) \text{ is an abelian group homomorphism} \quad f(a+a') = f(a)+f(a'), \quad f(0) = 0$$

$$(A, \cdot) \rightarrow (B, \cdot) \text{ is a monoid morphism} \quad f(aa') = f(a)f(a') \quad f(1) = 1$$

Lemma: $\exists!$ ring homomorphism $\mathbb{Z} \rightarrow A$ for any ring A .

Pf: $1 \mapsto 1$. \square

$$\ker = n\mathbb{Z}. \quad n = p \text{ prime} \Rightarrow A \text{ has characteristic } p \Rightarrow A \supseteq \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$$

0

0

\mathbb{Z}

Def: $A \subseteq B$ is a subring if the inclusion is a homomorphism.

E.g. $A \subseteq B$ subring and $S \subseteq B$ subset $\Rightarrow A[S] = \left\{ \sum_{\text{finite}} a_{s_1} \cdots a_{s_n} s_1 \cdots s_n \right\} \subseteq B$ subring

18.

Ideals

Q. What does $\ker(f: A \rightarrow B)$ look like?

Def: $I \subseteq A$ is a left ideal in the ring A if $AI \subseteq I$.

right
2-sided

both

no adjective
default: "ideal" means 2-sided

E.g. • any $A \Rightarrow I = \{0\}$ is 2-sided

- $\mathbb{Z} \geq n\mathbb{Z}$ 2-sided
- $M_2(\mathbb{k}) \geq \begin{bmatrix} 0 & * \\ 0 & * \end{bmatrix}$ left, but not right

Def: $a \in A \Rightarrow Aa = \text{principal left ideal}$

$AaA = \text{principal ideal}$

general: $Aa_1 + \dots + Aa_n = \text{left ideal generated by } a_1, \dots, a_n \in A$

$$Aa_1A + \dots + Aa_nA = \text{ideal} \quad " \quad " \quad = \langle a_1, \dots, a_n \rangle$$

E.g. {polynomials with even constant term} = $\langle 2, x \rangle \subseteq \mathbb{Z}[x]$

Q. Why ideals?

Prop: $f: A \rightarrow B$ ring homomorphism $\Rightarrow \ker f$ is an ideal.

Pf: $f(a) = 0 \Rightarrow f(bab') = 0 \quad \forall b, b' \in A. \quad \square$

In fact:

Thm: $I \subseteq A$ is an ideal $\Leftrightarrow \exists$ ring homomorphism $f: A \rightarrow B$ with $I = \ker f$.

Pf: \Leftarrow : Prop.

$\Rightarrow: I \subseteq A$ ideal $\Rightarrow A/I$ is a ring with $(x+I)(y+I) = xy + I$

quotient ring = quotient abelian group

i.e. $a \in x+I$ and $b \in y+I \Rightarrow ab \in xy+I$

Why? Because $xI + Iy + I^2 \subseteq I! \quad \square$

Thm (Universal property): $A \xrightarrow{\varphi} B$ ring homomorphism with $\ker \varphi \supseteq I$

$\pi \downarrow \quad \exists! \varphi_*: A/I \rightarrow B$ with $\varphi = \overline{\varphi} \circ \pi$.

Pf: True for $(A, +) \rightarrow (B, +)$. The claim: φ_* is already a ring homomorphism:

$$\begin{aligned} \varphi_*(\pi(x)\pi(y)) &= \varphi_*(\pi(xy)) = \varphi(xy) \\ &= \varphi(x)\varphi(y) = \varphi_*(\pi(x))\varphi_*(\pi(y)). \quad \square \end{aligned}$$

Commutative rings Fix commutative ring R.

Def: An ideal $\mathfrak{p} \subseteq R$ is
 • prime if R/\mathfrak{p} is entire (an integral domain)
 • maximal if $\mathfrak{p} \neq R$ and $I \supseteq \mathfrak{p} \Rightarrow I \in \{\mathfrak{p}, R\}$

R entire $\Leftrightarrow 0$ is prime

Prop: R is a field $\Leftrightarrow 0$ is maximal.

Cor: maximal \Rightarrow prime.

Pf: $\Rightarrow: x \notin \langle 0 \rangle \Rightarrow \langle x \rangle = R$

$$\langle x \rangle = \langle 1 \rangle$$

Pf: Every field is entire. \square

$\Leftarrow: x \neq 0 \Rightarrow \langle x \rangle = R$ since $\langle 0 \rangle$ is maximal $\Rightarrow 1 = xy$ for some $y \in R^*$ $\Rightarrow x \in R^*$. \square

Generally: Let $a, b \in R$ entire. Then $\langle a \rangle = \langle b \rangle \Leftrightarrow b = ua$ for some $u \in R^*$.

Pf: $b \in \langle a \rangle \Rightarrow b = xa$, $a \in \langle b \rangle \Rightarrow a = yb = yxa \Rightarrow a(1 - xy) = 0 \Rightarrow a = 0 \quad \text{or} \quad xy = 1$. \square

E.g. $p \in \mathbb{Z}$ prime $\Leftrightarrow \langle p \rangle \subseteq \mathbb{Z}$ prime

$\Leftrightarrow \langle p \rangle \subseteq \mathbb{Z}$ maximal, since $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ is a field.

Thm: If $I_1, \dots, I_n \subseteq R$ are ideals with $I_i + I_j = R \quad \forall i \neq j$

then $f: R \rightarrow R/I_1 \times \dots \times R/I_n$ is surjective.

$$x \mapsto (x+I_1, \dots, x+I_n) \Rightarrow \ker f = ?$$

$$0 \quad 0 \quad \Rightarrow x \in I_1, \dots, x \in I_n \Leftrightarrow x \in I_1 \cap \dots \cap I_n$$

Pf: Suffices: $\exists y_1, \dots, y_n \in R$ with $y_i \mapsto (0, \dots, 0, 1, 0, \dots, 0)$
 \uparrow
 ith slot

analogue: map of vector spaces

surjective \Leftrightarrow image \supseteq basis

$$I_1 + I_2 = R \Rightarrow \exists a_j \in I_1 \quad \text{with} \quad a_j + b_j = 1.$$

and $b_j \in I_2$

$$\text{E.g. } R = \mathbb{Z} \quad I_1 = 4\mathbb{Z}$$

$$\Rightarrow 1 = (a_2 + b_2) \cdots (a_n + b_n) \in I_1 + b_2 \cdots b_n,$$

$$I_1 = 6\mathbb{Z}$$

so take $y_1 = b_2 \cdots b_n$, and similarly for $i = 2, \dots, n$. \square

$$\mathbb{Z} \rightarrow \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$$

$$x \mapsto (x \pmod{4}, x \pmod{6})$$

Cor (Chinese Remainder Theorem):

If $I_1, \dots, I_n \subseteq R$ are ideals with $I_i + I_j = R \quad \forall i \neq j$,

$$\begin{array}{c|c} 0 & 0 \\ 1 & 1 \\ 2 & 2 \\ 3 & 3 \\ 4 & 4 \\ 5 & 5 \end{array}$$

then $x_1, \dots, x_n \in R \Rightarrow \exists x \in R$ with $x \equiv x_i \pmod{I_i} \quad \forall i$. \square

$$? \mapsto (0, 1)$$

E.g. $m_1, \dots, m_n \in \mathbb{Z}$ with $\gcd(m_i, m_j) = 1 \quad \forall i \neq j$.

In particular, $m = p_1^{e_1} \cdots p_n^{e_n}$ factorization into distinct primes

$$\Rightarrow |(\mathbb{Z}/m\mathbb{Z})^*| \cong \left| \left(\prod_{i=1}^n \mathbb{Z}/p_i^{e_i}\mathbb{Z} \right)^* \right|$$

Euler φ function $\Rightarrow \varphi(m) = \prod_{i=1}^n \varphi(p_i^{e_i}) = \prod_{i=1}^n (p_i - 1)p_i^{e_i - 1}$. \square

19.

PID and UFD

Fix a commutative integral domain R .

Def: $a \in R$ is irreducible if $a = bc \Rightarrow b \in R^*$ or $c \in R^*$ but not both.

$$\langle a \rangle = \langle c \rangle \text{ or } \langle a \rangle = \langle b \rangle$$

Lemma: $\langle p \rangle$ prime $\Rightarrow p$ irreducible.

Pf: $p = ab \Rightarrow a \in \langle p \rangle$ or $b \in \langle p \rangle$; say $a \in \langle p \rangle$.

Then $a = pc$, so $\underbrace{p = ab = pcb}_{\Rightarrow cb = 1}$ since R is entire. \square

Def: $a | b$ if $ac = b$ for some $c \in R$.

$$b \in \langle a \rangle$$

$d \in R \setminus \{0\}$ is a gcd of a and b if

- $d | a$ and $d | b$
- $c | a$ and $c | b \Rightarrow c | d$.

Def: R (a commutative integral domain) is a PID if every ideal is principal.

Prop: In a PID, $\langle a, b \rangle = \langle d \rangle \Rightarrow d$ is a gcd of a and b .

Pf: Let $d = \alpha a + \beta b$ and suppose $a = ex$ and $b = ey$.

Then $d = \alpha ex + \beta ey$

$$= e(\alpha x + \beta y) \Rightarrow e | d.$$

But $d | a$ and $d | b$ because $a, b \in \langle d \rangle$. \square

Cor: $\langle p \rangle$ prime $\Leftrightarrow p$ irreducible if R is a PID.

Pf: $p | ab$ and $p \nmid a \Rightarrow \langle p, a \rangle = \langle d \rangle \supsetneq \langle p \rangle$

$$\Rightarrow p = cd \text{ but } c \notin R^*$$

$\Rightarrow d \in R^*$ since p is irreducible may as well take $d = 1$

$$\Rightarrow 1 = xp + ya$$

$$\Rightarrow b = \underbrace{xp_b}_{p|} + \underbrace{yab}_{p|}$$

$$\Rightarrow p | b. \quad \square$$

Def: R (a commutative integral domain) is factorial (or a UFD) unique factorization domain (38)

if every $r \in R \setminus \{0\}$ factors uniquely into irreducible elements:

$$r = u p_1 \cdots p_k \text{ with } u \in R^* \text{ and}$$

$$r = v q_1 \cdots q_l \text{ with } v \in R^* \Rightarrow k = l \text{ and } q_i = u_i p_i \text{ for some } u_i \in R^* \text{ after permuting the } q_i.$$

Thm: PID \Rightarrow UFD.

Pf: Claim: Every $r \in R$ factors into irreducibles. no uniqueness yet

Pf: Let $S = \{\langle r \rangle \subseteq R \mid r \text{ doesn't factor into irreducibles}\}.$

Assume $S \neq \emptyset$. Then S has a maximal element $\langle r \rangle$ because

- every chain $\langle r_1 \rangle \subseteq \langle r_2 \rangle \subseteq \dots$ yields an ideal $\langle b \rangle = \langle r_1 \rangle \cup \langle r_2 \rangle \cup \dots$
- $b \in \langle r_n \rangle$ for some $n \Rightarrow \langle b \rangle \subseteq \langle r_n \rangle \subseteq \langle b \rangle$
 $\Rightarrow \langle b \rangle = \langle r_n \rangle \in S$ is an upper bound.

Note: r is reducible since $r \in S$, so $r = cd$ with $c, d \notin R^*$.

But then $\langle r \rangle \subsetneq \langle c \rangle$ and $\langle r \rangle \subsetneq \langle d \rangle$, so

c and d have factorizations. Hence r does, too. $\rightarrow \star$

Thus $S = \emptyset$. \square

$$\begin{aligned} r = u p_1 \cdots p_k &= v q_1 \cdots q_l \Rightarrow p_k \text{ prime by Cor} \\ &\Rightarrow p_k \mid q_i \text{ for some } i; \text{ assume } i = l \text{ by permutation} \\ &\Rightarrow p_k = u_k q_l \text{ with } u_k \in R^* \text{ since } q_l \text{ is irreducible} \\ &\Rightarrow u p_1 \cdots p_{k-1} = v u_k q_1 \cdots q_{l-1} \text{ because } R \text{ is entire.} \end{aligned}$$

Done by induction. \square

E.g. • $R = \mathbb{Z}$ PID by Euclidean algorithm next week
• $R = \mathbb{k}[x]$

- Thm: R factorial $\Rightarrow R[x]$ is, too $\Rightarrow \mathbb{Z}[x_1, \dots, x_n], \mathbb{k}[x_1, \dots, x_n]$ UFD
- $\mathbb{k}[[x]]$ formal power series is UFD; one variable \Rightarrow PID
- $\mathbb{k}[x^2, x^3]$ not UFD
- $\mathbb{Z}[\sqrt{-5}]$ not UFD

Localization

Def: $S \subseteq R$ is a multiplicative subset if S is a submonoid of (R, \cdot) .

- $1 \in S$ and
- $xy \in S \quad \forall x, y \in S$

The ring of fractions is

$$S^{-1}R = R[S^{-1}] = R \times S / \sim$$

where the class of (a, s) is denoted $\frac{a}{s}$

and $\frac{a}{s} = \frac{a'}{s'}$ if $\exists t \in S$ with $t(s'a - sa') = 0$.

$s'a - sa'$ is annihilated by something that's supposed to be a unit.

$$\begin{aligned} \text{Note: } \frac{a}{s} = \frac{a'}{s'} \text{ and } \frac{a'}{s'} = \frac{a''}{s''} \Rightarrow s''t' t(s'a - sa') &= 0 = -st t'(s'a - sa'') \\ \Rightarrow s't' t(s'a - sa'') &= 0 \\ \Rightarrow \sim \text{ is transitive} &\quad \text{symmetric and reflexive: easy} \end{aligned}$$

Prop: $R[S^{-1}]$ is a ring with $\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$ and $\frac{a}{s} + \frac{b}{t} = \frac{ta+bs}{st}$.

$$\begin{aligned} \text{Pf: e.g. } \frac{a}{s} = \frac{a'}{s'} \Rightarrow u(s'a - sa') &= 0 \\ \Rightarrow u(\underline{s'tab} - \underline{a'bst}) &= 0 \\ \Rightarrow \frac{ab}{st} &= \frac{a'b}{s't}. \quad \square \end{aligned}$$

Cor: $R \rightarrow R[S^{-1}]$ is a ring homomorphism.

$$a \mapsto \frac{a}{1}$$

$$Q. R = \mathbb{R}[x, y]/\langle xy \rangle \Rightarrow \ker(R \rightarrow R[x^{-1}]) = \cancel{\langle y \rangle} \xrightarrow{\text{next page}} \text{stuff annihilated by something that's supposed to be a unit!}$$

E.g. 1. $S = R^* \Rightarrow R[S^{-1}] = R$. We'll see why shortly, with the universal property

2. R integral domain and $S = R \setminus \{0\}$

$$\Rightarrow R[S^{-1}] = K(R) = \text{fraction field of } R \quad \text{not "quotient field": } R/\mathfrak{m} \text{ vs. } K(R)$$

$$\text{e.g. } R = \mathbb{Z} \Rightarrow K(R) = \mathbb{Q}$$

$$R = \mathbb{k}[x_1, \dots, x_n] \Rightarrow K(R) = \mathbb{k}(x_1, \dots, x_n) \text{ field of rational functions in } x_1, \dots, x_n \text{ over } \mathbb{k}$$

3. $\mathfrak{p} \subseteq R$ prime ideal and $S = R \setminus \mathfrak{p}$

$$\Rightarrow S^{-1}R \stackrel{\text{def}}{=} R_{\mathfrak{p}}, \text{ the localization of } R \text{ at } \mathfrak{p} \quad \#2: \mathfrak{p} = 0$$

$R_{\mathfrak{p}}$ is a local ring: it has a unique maximal ideal Pf: Exercise

$$4. S = \{1, t, t^2, \dots\}$$

$$\Rightarrow S^{-1}R = R[S^{-1}] \stackrel{\text{def}}{=} R_t$$

$$\ker(R \rightarrow R_t) = ? \quad \frac{a}{t} = \frac{0}{1} \Leftrightarrow ua = 0 \text{ for some } u \in S \\ \Leftrightarrow t^d a = 0 \text{ for some } d \in \mathbb{N}$$

e.g. $R = \mathbb{k}[x, y]/\langle xy \rangle \Rightarrow R = \mathbb{k}\{1, x, x^2, \dots, y, y^2, \dots\}$ basis as vector space / \mathbb{k}

$$x^d f(x, y) = 0 \text{ for some } d \in \mathbb{N} \Leftrightarrow xy \mid x^d f(x, y) \\ \Leftrightarrow y \mid f(x, y)$$

$\ker(R \rightarrow R[x^{-1}]) = \langle y \rangle$

Prop: {prime ideals of $S^{-1}R$ } \leftrightarrow {prime ideals $\mathfrak{p} \subseteq R$ with $\mathfrak{p} \cap S = \emptyset$ }

$$\mathfrak{p}S^{-1}R \leftrightarrow \mathfrak{p}$$

the point: $I \subseteq R$ remains a proper ideal $\Leftrightarrow I$ has no element that becomes a unit

Pf: $\mathfrak{p} \mapsto \{a \in R \mid \frac{a}{1} \in \mathfrak{p}\}$. The rest: Exercise. \square

Prop: Let \mathcal{C} = category of ring homomorphisms $R \xrightarrow{f} A$ such that
 $f(s) \in A^* \quad \forall s \in S$.

Then $R \rightarrow S^{-1}R$ is universally repelling in \mathcal{C} :

Pf: Let $f: R \rightarrow A$ be an object in \mathcal{C} .

Define $f_*: S^{-1}R \rightarrow A$ by $\frac{a}{s} \mapsto f(a)f(s)^{-1}$ uses $f(s) \in A^*$

Then $\frac{a}{s} = \frac{a'}{s'} \Rightarrow t(s'a - sa') = 0$ for some $t \in S$

$$\Rightarrow (f(t)(f(s')f(a) - f(s)f(a')) = 0) \cdot f(t)^{-1}f(s')^{-1}f(s)^{-1} \\ \Rightarrow f(a)f(s)^{-1} - f(a')f(s')^{-1} = 0,$$

so f_* is well defined.

Exercise: f_* • is a ring homomorphism and
• makes the diagram commute. \swarrow this is by def.

f_* is unique because it is determined by where it sends R . \square

Cor: $R[(R^*)^{-1}] = R$.

Pf: Any ring homomorphism $R \rightarrow A$ factors through $R \xrightarrow{\text{id}} R$,
so $R \xrightarrow{\text{id}} R$ satisfies the universal property. \square

21.

Euclidean domainsFix a commutative ring R .Def: A norm on R is a function $R \rightarrow \mathbb{N}$ with $0 \mapsto 0$ A norm N is positive if $N(a) > 0 \quad \forall a \neq 0$.A domain R is Euclidean if \exists norm $N: R \rightarrow \mathbb{N}$ such that $a, b \in R$ with $b \neq 0 \Rightarrow \exists q, r \in R$ satisfying

$$a = qb + r \quad \text{with } r = 0 \text{ or } N(r) < N(b)$$

quotient remainder

E.g. • $R = \text{field } \mathbb{k}$, $N = \text{anything: } a = qb$ for $q = ab^{-1}$.• $R = \mathbb{Z}$, $N = |\cdot|$ Thm: $R = \mathbb{k}[x]$ is Euclidean if $N = \deg$, and moreover q and r are unique.Pf: $a(x) = 0 \Rightarrow q = r = 0$.

$$a(x) = \lambda \in \mathbb{k}^* \Rightarrow \begin{cases} q = 0 \text{ and } r = \lambda \text{ if } \deg b \geq 1 \\ q = \lambda b^{-1} \text{ and } r = 0 \text{ if } \deg b = 0. \end{cases}$$

 $\deg a = n \geq 1$: use induction.Let $a(x) = a_n x^n + \dots + a_0$ and $b(x) = b_m x^m + \dots + b_0$ with $a_n \neq 0 \neq b_m$. $m > n \Rightarrow q = 0$ and $r = a$ suffice. $m \leq n$: set $a' = a - \frac{a_n}{b_m} x^{n-m} b$. Then $\deg a' < n$, so

$$= q'b + r \quad \text{with } r = 0 \text{ or } \deg r < m.$$

Set $q = q' + \frac{a_n}{b_m} x^{n-m}$. Then $qb + r = (q' + \frac{a_n}{b_m} x^{n-m})b + r$

$$= q'b + r + \frac{a_n}{b_m} x^{n-m} b$$

$$= a - \cancel{\frac{a_n}{b_m} x^{n-m} b} + \cancel{\frac{a_n}{b_m} x^{n-m} b} \quad \text{---}$$

Why are q and r unique?

$$\left. \begin{aligned} a &= \hat{q}b + \hat{r} \text{ with } \hat{r} = 0 \text{ or } \deg \hat{r} < m \Rightarrow (\underbrace{\hat{q} - q}_\text{deg} b) = r - \hat{r} \text{ has } \deg < m \\ &= qb + r \end{aligned} \right\} \begin{aligned} \deg &= \deg(\hat{q} - q) + m \\ \text{if } \hat{q} - q &\neq 0 \end{aligned} \Rightarrow \hat{q} - q = 0$$

$$\Rightarrow r - \hat{r} = 0. \quad \square$$

Lemma: R Euclidean domain \Rightarrow PID, and $I \subseteq R$ ideal $\Rightarrow I = \langle d \rangle$ for any $d \neq 0$ of minimal norm. 42

Pf: Fix such $d \in I$.

$$a \in I \Rightarrow a = qd + r \text{ with } r = a - qd \in I. \quad N(r) < N(d) \Rightarrow r = 0. \quad \square$$

Cor: $\mathbb{k}[x]$ is a PID and hence UFD.

Q. Is $\mathbb{k}[x, y]$? answer in a bit

Prop: R PID and $0 \neq p$ prime $\Rightarrow \langle p \rangle$ maximal.

Pf: $a \notin \langle p \rangle \Rightarrow \langle a, p \rangle = \langle d \rangle$ for some gcd of a and p ,
but $p \nmid d$ since $a \notin \langle p \rangle$. Unique factorization $\Rightarrow d \in R^*$.

So every ideal properly containing $\langle p \rangle$ is generated by a unit. \square

A. No: $R[y]$ PID $\Rightarrow R$ is a field because

$R[y]/\langle y \rangle \cong R$ is a domain $\Rightarrow \langle y \rangle$ is prime
 $\Rightarrow \langle y \rangle$ is maximal.

$\mathbb{k}[x, y] = \mathbb{k}[x][y]$ but $\mathbb{k}[x]$ is not a field.

Euclidean algorithm

Input: $a, b \in R$ with $b \neq 0$

Output: $\gcd(a, b)$

Init: q_0, r_0 with $a = q_0 b + r_0$ (0)	e.g. $\begin{array}{r} a \\ 108 \\ \hline b \\ 30 \\ \hline \end{array}$ $= 3 \cdot 30 + 18$
q_1, r_1	$30 = 1 \cdot 18 + 12$
$i = 1$	$18 = 1 \cdot 12 + 6$
$r_0 = q_1 r_1 + r_2$ (2)	$12 = 2 \cdot 6$

While: $r_i \neq 0$

$$12 = 2 \cdot 6$$

$$\begin{aligned} \text{Do: write } r_{i-1} &= q_{i+1} r_i + r_{i+1} & r_0 &= q_1 r_1 + r_2 & r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1} & (n-1) \\ i &\leftarrow i+1 & r_{n-2} &= q_n r_{n-1} + r_n & & & (n) \end{aligned}$$

Return: r_{i-1} (call it r_n)

$$r_{n-1} = q_{n+1} r_n \quad (n+1)$$

Thm: $\langle a, b \rangle = \langle r_n \rangle$. that's the one you want.

Pf: (0) $\Rightarrow r_0 \in \langle a, b \rangle$. (1) $\Rightarrow r_1 \in \langle b, r_0 \rangle \subseteq \langle a, b \rangle$. (i) $\Rightarrow r_i \in \langle r_{i-2}, r_{i-1} \rangle \subseteq \langle a, b \rangle$ by induction.

(n+1) $\Rightarrow r_n | r_{n-1}$. (n) $\Rightarrow r_n | r_{n-2}$. (i) $\Rightarrow r_n | r_{i-2}$ for $i \geq 2$ by induction. on n-i

(1) $\Rightarrow r_n | b$. (0) $\Rightarrow r_n | a$. \square

Modules

Fix a ring A .

M is a left module over A , or a left A -module if M is

- an abelian group with

- a left action of (A, \cdot) that is distributive:

$$\begin{cases} \cdot (x+y)m = xm + ym \\ \cdot x(m+n) = xm + xn \end{cases}$$

Ex: $-m = -1 \cdot m$, $x(-m) = -(xm)$, $0m = 0$

Assume "module" = "left module"

Def: $N \subseteq M$ is a submodule if $AN \subseteq N$.

E.g. • A is a free A -module with basis $1 \in A$.

• $I \subseteq A$ submodule \Leftrightarrow left ideal

• A/I cyclic A -module generated by $\bar{1} \in A/I$

• \mathbb{Z} -module = ? abelian group

• \mathbb{k} field $\Rightarrow \mathbb{k}$ -module = ? vector space/ \mathbb{k}

• V = vector space/ \mathbb{k} and $T: V \rightarrow V \Rightarrow V$ is a $\mathbb{k}[x]$ -module via $x \cdot v = T^v$

• $A = R^{n \times n} = n \times n$ matrices/ring $R \Rightarrow R^n = \{\boxed{\quad}\}$ left ideal $f(x) \cdot v = f(T)v$
and $R_{\text{row}}^n = \{\boxed{\quad}\}$ right ideal pick which column

• set S and A -module $M \Rightarrow \text{maps}(S \rightarrow M)$ is an A -module via $(af)(s) = a(\underbrace{f(s)}_{\in M})$

Def: M is generated by $\{m_\lambda \mid \lambda \in \Lambda\} \subseteq M$ if $m \in M \Rightarrow m = \sum_{\lambda \in \Lambda} x_\lambda m_\lambda$

for $\{x_\lambda \mid \lambda \in \Lambda\} \subseteq A$ almost all 0.

linear combination

E.g.: $\mathbb{Z} \times \mathbb{Z}$ is generated by $\{[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}], [\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}]\}$ but also $\{[\begin{smallmatrix} 1 \\ 2 \end{smallmatrix}], [\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}]\}$.

Lemma: $N \subseteq M$ submodule \Rightarrow group M/N is naturally a module.

Pf: $xm \equiv xm' \pmod{N}$ if $m - m' \in N$ because then $xm - xm' = x(m - m') \in N$. \square

E.g. $\underbrace{M}_{\mathbb{Z}}$ $\begin{bmatrix} 3 \\ 6 \end{bmatrix} \Rightarrow im = N \cong \mathbb{Z}$. What is M/N ?

$\mathbb{Z} \times \mathbb{Z} \leftarrow \mathbb{Z}$ Use \circlearrowleft : $N = 3\mathbb{Z}[\begin{smallmatrix} 1 \\ 2 \end{smallmatrix}] \times 0 \subseteq \mathbb{Z}[\begin{smallmatrix} 1 \\ 2 \end{smallmatrix}] \times \mathbb{Z}[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}] \Rightarrow M/N \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}$.

Def: Fix module M over a commutative domain R .

The torsion submodule is $M_{\text{tor}} = \{m \in M \mid rm = 0 \text{ for some } r \in R \setminus \{0\}\}$

E.g.: $(M/N)_{\text{tor}} \cong \mathbb{Z}/3\mathbb{Z}$.

Def: $I \subseteq A$ left ideal $\Rightarrow IM = \{ \text{linear combinations of elements of } M \text{ with coefficients in } I \}$. (4)

Ex: IM is a submodule. $I(JM) = (IJ)M$ and $(I+J)M = IM + JM$.

Def: $\varphi: M \rightarrow M'$ is a module homomorphism if φ is a group homomorphism

$(M, +) \rightarrow (M', +)$ with $\varphi(xm) = x\varphi(m) \quad \forall x \in A \text{ and } m \in M.$
 \uparrow
 $\varphi \text{ is } A\text{-linear}$

Note: $A\text{-Mod}$ is a category: objects M • $1_M: M \rightarrow M$ identity
morphisms $\varphi: M \rightarrow M'$ • $\varphi: M \rightarrow M'$ and $\psi: M' \rightarrow M'' \Rightarrow \psi \circ \varphi: M \rightarrow M''$

$A\text{-Mod}$ has initial object: $\mathbb{Z}0$ • associative and $1_M \circ \varphi = \varphi = \varphi \circ 1_{M'}$.
terminal object: $\mathbb{Z}0$

Ex: $\ker(M \rightarrow M') \subseteq M$ submodule

$\text{im}(M \rightarrow M') \subseteq M'$ submodule

Def: $\text{coker}(M \rightarrow M') = M'/\text{im}(M \rightarrow M')$ quotient module

Isomorphism theorems

1. $N, N' \subseteq M$ submodules $\Rightarrow N+N' \subseteq M$ submodule and

$N/N \cap N' \xrightarrow{\sim} (N+N')/N'$. Pf: $N \twoheadrightarrow (N+N')/N'$ has kernel $N \cap N'$; apply universal property.

2. $M \supseteq M' \supseteq M'' \Rightarrow M/M' \xrightarrow{\sim} (M/M'')/(M'/M'')$. Pf: similar.

3. homomorphism $\varphi: M \rightarrow M'$ and $N' \subseteq M' \Rightarrow \varphi^{-1}(N') \subseteq M$ submodule and

$$M/\varphi^{-1}(N') \hookrightarrow M/N'.$$

Def: The sequence $M \xrightarrow{\psi} M' \xrightarrow{\varphi} M''$ is exact at M if $\text{im } \psi = \ker \varphi$.

If $\varphi \circ \psi = 0$ then the sequence has homology $\ker \varphi / \text{im } \psi$.

Lemma: $N \subseteq M \Rightarrow$ short exact sequence $0 \rightarrow N \rightarrow M \rightarrow M/N \rightarrow 0$.

Pf: Discuss: $0 \rightarrow N \rightarrow M$ exact $\Leftrightarrow N \hookrightarrow M$ monomorphism (or embedding)

$M \rightarrow M' \rightarrow 0$ exact $\Leftrightarrow M \twoheadrightarrow M'$ epimorphism.

$N \rightarrow M \rightarrow M/N$ exact at M . \square

Def: Fix a commutative ring R . An R -algebra is a ring A with a ring homomorphism $R \xrightarrow{f} A$ such that $\text{im } f \subseteq \text{center}(A)$.

Lemma: $\Rightarrow A$ is an R -module. \square

23.

Products, sums, and free modules

Def: A product of objects $\{M_i\}_{i \in I}$ in a category is

- an object P with
- morphisms $P \xrightarrow{\pi_i} M_i \forall i \in I$ satisfying
- a universal property: $N \xrightarrow{\psi_i} M_i \forall i \in I \Rightarrow \exists! N \rightarrow P$ making $\begin{array}{ccc} N & \xrightarrow{\exists! \quad \pi_i} & P \\ & \searrow \psi_i & \downarrow \pi_i \\ & & M_i \end{array}$ commute.

"A product is terminal in the category of objects with morphisms to all M_i "

E.g. In $A\text{-MOD}$, $P = \prod_{i \in I} M_i$. Same notation in any category, if P exists.

Def: A coproduct of objects $\{M_i\}_{i \in I}$ in a category is

an object Q that is universal (initial) in the category of objects with morphisms from all M_i .

Thus $M_i \rightarrow N \forall i \in I \Rightarrow \exists! Q \rightarrow N$ making $\begin{array}{ccc} M_i & \longrightarrow & Q \\ & \searrow & \downarrow \\ & & N \end{array}$ commute.

E.g. In $A\text{-MOD}$, $Q = \bigoplus_{i \in I} M_i$, the direct sum.

Discuss infinite cases: $\bigoplus_{i \in I} M_i \hookrightarrow \prod_{i \in I} M_i$, with $\cong \Leftrightarrow |I| < \infty$

Proofs of E.g.s: $A = \mathbb{Z} \checkmark$

$A = \text{arbitrary}$: check universal maps are A -linear. \square

E.g. $\{M_i\}_{i \in I}$ family of submodules of M induces

$\bigoplus_{i \in I} M_i \rightarrow M$. Def: direct sum decomposition if \cong .

Def: $x \in M$ generates cyclic submodule $Ax \subseteq M$.

A family $\{x_\lambda \mid \lambda \in \Lambda\}$ of elements of M is linearly independent over A if

$$\bigoplus_{\lambda \in \Lambda} A \xrightarrow{\cong} \bigoplus_{\lambda \in \Lambda} Ax_\lambda \xrightarrow{\varphi} M. \quad \cong : x_\lambda \text{ nzd} \quad \hookrightarrow : M \text{ decomposes as} \\ \oplus \text{ cyclic submods}$$

Lemma: $\Leftrightarrow \left(\sum_{\lambda \in \Lambda} a_\lambda x_\lambda = 0 \Rightarrow a_\lambda = 0 \forall \lambda \right)$

Pf: $\ker \varphi = \{\text{linear dependence relations on the } x_\lambda\}$
 $\stackrel{\text{def}}{=} \{\text{syzgyies on the } x_\lambda\}$. \square

Note: x_λ could equal x_λ for $\lambda \neq \lambda'$.

Q. When is $M = M_1 \oplus \dots \oplus M_n$ for $M_1, \dots, M_n \subseteq M$?

A. $M = M_1 + \dots + M_n$ and $M_i \cap \sum_{j \neq i} M_j = 0 \forall i$.

Def: M is free if it has a generating linearly independent subset.

basis

S any set \rightsquigarrow free module with basis S is $\bigoplus_{s \in S} A \stackrel{\text{def}}{=} A^{\oplus S}$
 \cong finitely supported functions $S \rightarrow A$

Thm: $\{x_\lambda\}_{\lambda \in \Lambda}$ basis of M and

$\{y_\lambda\}_{\lambda \in \Lambda}$ any elements of N

$\Rightarrow \exists!$ homomorphism $\varphi: M \rightarrow N$ with

$$\varphi(x_\lambda) = y_\lambda \quad \forall \lambda \in \Lambda.$$

Pf: $M = A$ with basis $\{1\}$: cyclic submodule $\Rightarrow Ax_\lambda \rightarrow N \quad \forall \lambda$

General case: universal property of \bigoplus $\Rightarrow \bigoplus_\lambda Ax_\lambda \rightarrow N$. \square

Def: For a module M , a (free) presentation is a morphism

$F_1 \rightarrow F_0$ with cokernel $F_0 \twoheadrightarrow M$ (with both F_i free).

E.g. $T: V \rightarrow V$ vector space/ \mathbb{k} $\dim < \infty$ V is a $\mathbb{k}[x]$ -module via $x \cdot v = Tv$

$V = \langle v \rangle$ cyclic $\Leftrightarrow V = \text{span}_{\mathbb{k}}\{v, Tv, \dots, T^{d-1}v\}$ for $d = \dim V$

$$\Leftrightarrow \mathbb{k}[x] \twoheadrightarrow V$$

$$\begin{array}{rcl} 1 & \mapsto & v \\ x & \mapsto & ?Tv \end{array} \quad \text{ker } = ? \text{ minimal polynomial } p(x) \text{ of } T$$

$$\Leftrightarrow \mathbb{k}[x] \xrightarrow{p(x)} \mathbb{k}[x]$$

$$f \mapsto p(x)f \quad \text{is a presentation of } V.$$

Def: An exact sequence $0 \rightarrow K \xrightarrow{\psi} M \xrightarrow{\varphi} N \rightarrow 0$ splits if

it has a section σ with $\varphi\sigma = \text{id}_N$.

Note: Sequence is short exact $\Rightarrow M = K + \sigma(N)$ by #5 on midterm 2.

But $K \cap \sigma(N) = 0$ since $\sigma(N) \hookrightarrow N$.

Hence split $\Leftrightarrow M = K \oplus \sigma(N)$.

often written: $M = K \oplus N$. $\text{but wrong: needs } \cong, \text{ not } =$

Cor: N free \Rightarrow sequence splits.

Pf: If $\{x_\lambda\}_{\lambda \in \Lambda}$ in M maps to basis $\{y_\lambda\}_{\lambda \in \Lambda}$ of N , then

use Thm to construct $\sigma: y_\lambda \mapsto x_\lambda \quad \forall \lambda \in \Lambda$. \square

Free modules/PID

Def: The rank of a free module F over a nonzero commutative ring is $\text{rank } F = |\text{basis of } F|$.

Lemma: does not depend on basis.

Pf: Suppose $F \cong \bigoplus_{s \in S} R$. Let $\mathfrak{p} \subseteq R$ be maximal.

$$F/\mathfrak{p}F \cong \bigoplus_{s \in S} R/\mathfrak{p}$$
 is a vector space over R/\mathfrak{p} of $\dim |S|$. \square

Thm: Fix F free / PID R and a submodule $M \subseteq F$. Then M is free of $\text{rank } \leq \text{rank } F$.

Pf: $F \cong \bigoplus_{\lambda \in \Lambda} Rx_\lambda$ for a basis $\{x_\lambda\}_{\lambda \in \Lambda}$.

$J \subseteq \Lambda \Rightarrow M_J \stackrel{\text{def}}{=} M \cap \bigoplus_{j \in J} Rx_j$ has the form

(*) and $M_J = \bigoplus_{j \in J} Ry_j$ for some $y_j \in M_J$

Warning: some of the y_j might be 0

or not. Order the set Y of

families $\{y_j\}_{j \in J}$ for which \exists basis $\{x_\lambda\}_{\lambda \in \Lambda}$ satisfying (*)

by inclusion: $\{y_j\}_{j \in J} \subseteq \{y'_j\}_{j \in J'}$ if $J \subseteq J'$ and $y_j = y'_j \forall j \in J$.

If C is a chain in Y then $\bigcup_{c \in C} c \in Y$ since any dependence relation involves only finitely many y_j .

Hence \exists family $\{y_j\}_{j \in J}$ maximal in Y . Want $J = \Lambda$.

Suffices: $k \in \Lambda \setminus J \Rightarrow \star$. Let $K = J \cup \{k\}$ and $M \hookrightarrow F \xrightarrow{\pi_k} Rx_k$.

Then $\pi_k(M_K) = \langle a \rangle x_k \subseteq Rx_k$ since R is a PID.

But $\ker \pi_k|_{M_K} = M_J$, so

$$0 \rightarrow M_J \rightarrow M_K \xrightarrow{\pi_k} \pi_k(M_K) \rightarrow 0$$

is exact and splits because $\langle a \rangle x_k$ is free!

Thus $\{y_j\}_{j \in K} \in Y$ if $y_k = ax_k$. \star

So $J = \Lambda$. \square

Cor: M finitely generated / PID R and $N \subseteq M$ submodule $\Rightarrow N$ f.g.

Pf: $f: R^n \twoheadrightarrow M \Rightarrow f^{-1}(N)$ free of rank $\leq n$

$\Rightarrow N$ f.g. since $f^{-1}(N) \twoheadrightarrow N$. \square

•
•
•
•
•

•
•
•
•
•

□
□

□
□

□
□

□

•
•
•
•
•

□

25.

Structure thm for modules over PIDThm: Fix f.g. nonzero module $M / \text{PID } R$. $\exists!$ proper ideals $\langle q_1 \rangle \subseteq \dots \subseteq \langle q_n \rangle$ Def: the invariants of M with $M \cong R/\langle q_1 \rangle \oplus \dots \oplus R/\langle q_n \rangle$.E.g. $R = \mathbb{Z} \Rightarrow M \cong \underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_{r = \text{rank } M} \oplus \underbrace{\mathbb{Z}/n_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/n_k\mathbb{Z}}_{\bigoplus_p \mathbb{Z}/p^{e_i(p)}\mathbb{Z}} \quad \text{with } n_k | \dots | n_1$ $e_1(p) \geq \dots \geq e_k(p) \quad \forall \text{ primes } p, \text{ and almost all } 0$

$$\begin{aligned} \text{e.g. } \mathbb{Z}^3 &\oplus \boxed{\mathbb{Z}/32\mathbb{Z}} \oplus \boxed{\mathbb{Z}/32\mathbb{Z}} \oplus \boxed{\mathbb{Z}/4\mathbb{Z}} \oplus \boxed{\mathbb{Z}/2\mathbb{Z}} \oplus \boxed{\mathbb{Z}/2\mathbb{Z}} \oplus \boxed{\mathbb{Z}/2\mathbb{Z}} \\ &\oplus \boxed{\mathbb{Z}/81\mathbb{Z}} \oplus \boxed{\mathbb{Z}/27\mathbb{Z}} \\ &\oplus \boxed{\mathbb{Z}/625\mathbb{Z}} \oplus \boxed{\mathbb{Z}/25\mathbb{Z}} \oplus \boxed{\mathbb{Z}/5\mathbb{Z}} \oplus \boxed{\mathbb{Z}/5\mathbb{Z}} \end{aligned}$$

Fundamental thm of f.g. abelian groups

$$\mathbb{Z}^3 \oplus \mathbb{Z}/\langle 162000 \rangle \oplus \mathbb{Z}/\langle 2160 \rangle \oplus \mathbb{Z}/\langle 20 \rangle \oplus \mathbb{Z}/\langle 10 \rangle \oplus \mathbb{Z}/\langle 2 \rangle \oplus \mathbb{Z}/\langle 2 \rangle$$

E.g. $R = \mathbb{k}[x] \Rightarrow$ module V is a vector space $/ \mathbb{k}$ with $x \cdot v = T v$ for some $T: V \rightarrow V$ Thm $\Rightarrow V \cong \mathbb{k}[x]^r \oplus (\dim < \infty)$

\uparrow
easy, so assume $\dim V < \infty$ this is Math 221!

$$\text{Thm} \Rightarrow V \cong \bigoplus_p \mathbb{k}[x]/\langle p^{e_i(p)} \rangle \oplus \dots \oplus \bigoplus_p \mathbb{k}[x]/\langle p^{e_k(p)} \rangle$$

 $e_1(p) \geq \dots \geq e_k(p) \quad \forall \text{ primes } p, \text{ and almost all } 0$ Q. What is $\{p\}$ the set of all prime elements up to units?

A. all irreducible polynomials up to units

Q. What if $\mathbb{k} = \mathbb{C}$?A. $p = x - \alpha$ for $\alpha \in \mathbb{C}$ Q. For fixed $p = x - \alpha$, what is $\mathbb{k}[x]/\langle p^{e_i(p)} \rangle \oplus \dots \oplus \mathbb{k}[x]/\langle p^{e_k(p)} \rangle$?i.e. $\mathbb{k}[x]/\langle (x - \alpha)^e \rangle \oplus \dots \oplus \mathbb{k}[x]/\langle (x - \alpha)^e \rangle$?Q. What is $\mathbb{k}[x]/\langle (x - \alpha)^e \rangle$?A. cyclic, with minimal polynomial $p(x) = (x - \alpha)^e$ = a Jordan block of size e for eigenvalue α by Lec. 23.Conclusion: over $\mathbb{k}[x]$, Thm \Leftrightarrow Jordan form thm

course evals

Pf overview

Recall: M/commutative domain R has torsion submodule

$$M_{\text{tor}} = \{m \in M \mid rm = 0 \text{ for some } r \in R \setminus \{0\}\}.$$

Fix M f.g./PID R.

Prop 1: $M = M_{\text{tor}} \oplus F$ with

- F free
- $\text{rank } M \stackrel{\text{def}}{=} \text{rank } F < \infty$ well defined.

Prop 2: $M = M_{\text{tor}} \Rightarrow M = \bigoplus_p M(p)$ where

- $p^e M(p) = 0$ for some $e \in \mathbb{N}$
- $M(p) = 0$ for almost all p. immediate from \bigoplus , since M f.g.

$M(p) = \{m \in M \mid p^e m = 0 \text{ for } e \gg 0\}$. analogue of Sylow p-subgroup!

Prop 3: $M = M(p) \Rightarrow M \cong R/\langle p^{e_1} \rangle \oplus \dots \oplus R/\langle p^{e_k} \rangle$.

\exists : Props $\Rightarrow M \cong R^l \oplus \bigoplus_p R/\langle p^{e_{l+1}(p)} \rangle \oplus \dots \oplus R/\langle p^{e_{l+k}(p)} \rangle$ with $e_{l+1}(p) \geq \dots \geq e_{l+k}(p)$.

Set $q_1, \dots, q_l = 0$

and $q_i = \prod_p p^{e_i(p)}$ for $i > l$, where $e_i(p) = 0$ for $i > l+k$.

Then $\dots | q_n | \dots | q_1$ by construction, so $\langle q_1 \rangle \subseteq \dots \subseteq \langle q_n \rangle \subseteq \dots$ $n = \max_{e_i(p) \neq 0} i$

$\cdot \bigoplus_p R/\langle p^{e_i(p)} \rangle \cong R/\langle q_i \rangle$ by CRT. ✓

!: $\#\{i \mid q_i = 0\} = \text{rank } M$. Henceforth assume $M = M_{\text{tor}}$.

Suppose q_1, \dots, q_n satisfy thm.

Uniqueness is trivial when $q_1 \dots q_n = p$ is prime: $n=1$ and $q_1 = p$.

If $q_1 \dots q_n = pa$ with $a \notin R^*$

then $\#\{i \mid p \mid q_i\} = \dim_{R/\langle p \rangle} M/pM$ since

$$pR/\langle q \rangle \cong \begin{cases} R/\langle q \rangle & \text{if } p \nmid q \\ R/\langle q/p \rangle & \text{if } p \mid q. \end{cases}$$

Induction on # prime factors of $q_1 \dots q_n \Rightarrow$ uniqueness for pM :

$\text{ord}_p\left(\frac{q_i}{\gcd(p, q_i)}\right)$ is well defined.

Hence $\text{ord}_p(q_i)$ is well defined, too: add 1 or not, as appropriate. □

26.

Pf of Prop 1: $M_{\text{tor}} = \ker(M \rightarrow M_{\langle 0 \rangle})$, where $M_p = S^{-1}M$ for $S = R \setminus p$.

Suffices: $E = \text{im}(M \rightarrow M_{\langle 0 \rangle})$ is free, since then $0 \rightarrow M_{\text{tor}} \rightarrow M \rightarrow E \rightarrow 0$ splits.

Why is rank F well defined? Because $F \cong M/M_{\text{tor}}$!

Will prove $E \subseteq$ f.g. free submodule of $M_{\langle 0 \rangle}$, so Thm p. 47 applies.

$M = \langle m_1, \dots, m_k \rangle \Rightarrow M_{\langle 0 \rangle} = \text{span}_{R_{\langle 0 \rangle}} \left\{ \frac{m_1}{1}, \dots, \frac{m_k}{1} \right\}$ over $R_{\langle 0 \rangle} = K(R) = \text{field}$.

$$E = \left\langle \frac{m_1}{1}, \dots, \frac{m_k}{1} \right\rangle \quad \text{over } R.$$

Choose basis x_1, \dots, x_n for $M_{\langle 0 \rangle}$.

Let $a \in R$ be \prod (all denominators in coeffs on x_1, \dots, x_n in $\frac{m_1}{1}, \dots, \frac{m_k}{1}$).

Then $E \subseteq R_a^{x_1} \oplus \dots \oplus R_a^{x_n}$. \square

Ex: $\text{rank } M = n$.

Lemma: $M(p) = \ker(M \rightarrow M[p^{-1}])$. \square

Lemma: If $M = M_{\text{tor}}$ then $M(p) \hookrightarrow M$ induces an isomorphism $M(p)_{\langle p \rangle} \xrightarrow{\sim} M_{\langle p \rangle}$.

Pf: Need \rightarrow by HW5 #9b. But

$$\begin{aligned} \frac{x}{a} \in M_{\langle p \rangle} &\Rightarrow p^n \frac{x}{a} = 0 \text{ since } M_{\langle p \rangle} \text{ is torsion and } R_{\langle p \rangle} \text{ has just one prime } \neq \langle 0 \rangle \text{ local + PID} \\ &\Rightarrow bp^n x = 0 \text{ for some } b \notin \langle p \rangle \\ &\Rightarrow bx \in M(p) \\ &\Rightarrow \frac{x}{a} = \frac{bx}{ab} \in M(p)_{\langle p \rangle}. \quad \square \end{aligned}$$

Lemma: $p^n N = 0 \Rightarrow N \xrightarrow{\sim} N_{\langle p \rangle}$.

Pf: $p^n N = 0 \Rightarrow N$ is a module over $R/\langle p^n \rangle$. Write $R \twoheadrightarrow R/\langle p^n \rangle$.

Then $\bar{r} \in (R/\langle p^n \rangle)^*$ $\forall r \notin \langle p^n \rangle$, since $\langle r, p^n \rangle = 1$.

Hence, if $S = R \setminus \langle p \rangle$ then $N_{\langle p \rangle} = S^{-1}N = S^{-1}RN = S^{-1}R/\langle p^n \rangle N = R/\langle p^n \rangle N = N$. \square

Pf of Prop 2: $M(p) \neq 0 \Rightarrow \exists 0 \neq x_p \in M(p)$ with $px_p = 0$. Thus

$\langle x_p | M(p) \neq 0 \rangle$ f.g. by Cor p. 47, so $\underbrace{M(p) = 0 \text{ for almost all } p}_{\bigoplus_p M(p) \cong \prod_p M(p)}$

$$\bigoplus_p M(p) \cong \prod_p M(p).$$

This is crucial; like finiteness of rank, it is a key place where f.g. is used

Lemmas $\Rightarrow M(p) \rightarrow M_{\langle p \rangle} = M(p)_{\langle p \rangle} = M(p) \Rightarrow M(p) \xrightarrow{\sim} M_{\langle p \rangle} \forall p$.

But $M(q)_{\langle p \rangle} = 0 \quad \forall \langle q \rangle \neq \langle p \rangle$. Thus

$M \rightarrow \prod_p M_{\langle p \rangle} = \prod_p M(p) = \bigoplus_p M(p)$ becomes \cong locally at every $\langle p \rangle$. \square

Nakayama's Lemma: Fix local ring A with maximal ideal \mathfrak{p} and f.g. A -module N .

Then $N = \mathfrak{p}N \Rightarrow N = 0$.

$$\begin{aligned}\text{Pf: } N = \langle x_1, \dots, x_n \rangle &\Rightarrow x_1 = \sum_{i=1}^n a_i x_i \quad \text{with } a_i \in \mathfrak{p} \quad \forall i \\ &\Rightarrow (\underbrace{1-a_1}_{\in A \setminus \mathfrak{p}}) x_1 = \sum_{i=2}^n a_i x_i \quad \text{with } a_i \in \mathfrak{p} \quad \forall i \\ &\quad \epsilon A \setminus \mathfrak{p} = A^*\end{aligned}$$

$\Rightarrow x_1 \in \langle x_2, \dots, x_n \rangle$. Done by induction ($n=0$ trivial). \square

Nakayama's Lemma: (A, \mathfrak{p}) local ring with f.g. A -module M . Write

$$M \rightarrow M/\mathfrak{p}M$$

$$x \mapsto \bar{x}$$

Assume $M/\mathfrak{p}M = \langle \bar{x}_1, \dots, \bar{x}_n \rangle$. Then $M = \langle x_1, \dots, x_n \rangle$.

Pf: Apply previous to $N = M/\langle x_1, \dots, x_n \rangle$, so $\mathfrak{p}N = \mathfrak{p}M + \langle x_1, \dots, x_n \rangle$

$$\begin{aligned}0 = \mathfrak{p}M + \langle x_1, \dots, x_n \rangle / M + \langle x_1, \dots, x_n \rangle &\rightsquigarrow M + \langle x_1, \dots, x_n \rangle \\ &= N. \quad \square\end{aligned}$$

N is a set of cosets;

so is $\mathfrak{p}N$

again, a set of cosets

E.g. x_1, \dots, x_n basis of $F \Leftrightarrow \bar{x}_1, \dots, \bar{x}_n$ basis of $F/\mathfrak{p}F$.

Prop 3: Assume R local PID with $\langle p \rangle$ maximal and M f.g. with $p^e M = 0$.

If $0 \rightarrow K \rightarrow F \rightarrow M \rightarrow 0$ is exact with $F \cong R^n$,

then F has a basis f_1, \dots, f_n such that

$p^{e_1} f_1, \dots, p^{e_n} f_n$ is a basis of K for some $e_1, \dots, e_n \in \mathbb{N}$.

Pf: $F/\mathfrak{p}F \twoheadrightarrow M/\mathfrak{p}M$.

F has basis $B = B' \cup B''$ with $B'' \leftrightarrow$ basis \bar{B}'' for $M/\mathfrak{p}M$.

Using B'' , assume $F/\mathfrak{p}F \cong M/\mathfrak{p}M$, so $\mathfrak{p}F \supseteq K$ because $K \rightarrow F \rightarrow M \rightarrow M/\mathfrak{p}M$.

$e=1$: Any basis of F will do, since $F/\mathfrak{p}F \cong M = M/\mathfrak{p}M = 0$.

$e \geq 2$: $\mathfrak{p}F/K = \mathfrak{p}M$ is killed by p^{e-1} .

Induction \Rightarrow choose basis g_1, \dots, g_n of $\mathfrak{p}F$ with

$p^{e_1-1} g_1, \dots, p^{e_n-1} g_n$ basis of K .

$g_i \in \mathfrak{p}F \Rightarrow g_i = pf_i$ for some (unique) $f_i \in F$, so $p^{e_i} f_i = p^{e_i-1} g_i$.

Nakayama $\Rightarrow f_1, \dots, f_n$ basis of F . \square