Math 501 — Algebraic Structures I — 08/29/2023

Office hours: Tu 2:40-4:00
W 2:00-3:15

Assignments due Thursdays, usually will have 2 weeks to do them

HW = 10% each
Midterms = 15% each
"final" = 20%

2 Midterms + 1 cumulative midterm = basically homework assignments

Distinction: Work w/ people for parts (but write your own writeups)
Work by yourself for exams
↳ you can ask stuff in office hours as well

Groups

Def: A group is a set G with a binary operation $G \times G \to G$, $(a,b) \mapsto ab$ (also $a*b$, $a+b$, $a \cdot b$, $a \circ b$)

that:
- is associative: $a(bc) = (ab)c$ (semigroup)
- has an identity e with $eg = ge = g \ \forall g \in G$ (monoid)
- ~~has an inverse g^{-1} for each $g \in G$: $g^{-1}g = e$~~
- has an inverse map: a bijection $G \to G$, $g \mapsto g^{-1}$ s.t. $g^{-1}g = e$

Let $gh = e$, then $g^{-1}gh = g^{-1}e$, $eh = g^{-1}e$, $h = g^{-1}$

so $g^{-1}g = gg^{-1} = e$

Note: $ab = ga$ not required

G is abelian if $G \times G \to G$ is commutative, $ab = ba \ \forall a,b \in G$

Examples:

$(\mathbb{N}, +)$ is a commutative monoid

$(\mathbb{Z}, +)$ is an abelian group = Grothendieck group of

$(\mathbb{Z} \setminus \{0\}, \cdot)$ is a monoid $(\mathbb{Q}^*, \cdot)$ is the abelian group = the group of units in the monoid $(\mathbb{Q}, \cdot)$

For example, $(\mathbb{Z}^*, \cdot) = \{\pm 1\}$

abelian ↑ / non-abelian if $n \geq 2$

any vector space over any field (under $+$)

$(\mathbb{F}^{n \times n}, \cdot)^*$

S_n = Permutations of $1, \dots, n$

Def/Example: A field is an abelian group $(F, +)$ with (additive) identity 0 s.t. $F^* = F \setminus \{0\}$ is an abelian group $(F^*, \cdot)$ and multiplication distributes over $+$, e.g. $a(b+c) = ab + ac \ \forall a,b,c \in F$

Lemma: $a \cdot 0 = 0 \quad \forall a \in F$

Why groups?

> **Symmetry:** an operation on some thing that leaves it looking as it did before.

Abstract the notion of "symmetry"

⇝ A set of operations ("symmetries") with composition, i.e. if f fixes figure and g fixes figure then $f \circ g$ and $g \circ f$ do too and f^{-1} does too.

G $\quad G \times G \to G \quad G \to G$, $f \mapsto f^{-1}$

These things come up in lots of places:

Combinatorics: discrete symmetries e.g. rotations of polyhedra
Geometry: continuous symmetries e.g. rotations of a sphere
} linear ⇒ given by matrices ⇝ matrix groups

Topology:

Circle × circle = torus which has "homology group" $\mathbb{Z} \times \mathbb{Z}$

$S^1 \times S^1 = T^2$

Computer Science: $\mathbb{Z}/n\mathbb{Z}$ (esp. when n prime), permutations

Back to fields

$\mathbb{R} + i\mathbb{R}$

Eg. $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{F}_2$ $\{0,1\}$, $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{Q}(i) = \{a+bi \mid a,b \in \mathbb{Q}\} \subseteq \mathbb{C}$, $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\} \subseteq \mathbb{C}$

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

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

Write $H \leq G$. (Just $H < G$ for a proper subgroup)

Lemma: $H \leq G$ is a group with same identity as

Proof: Associativity: $a,b,c \in H \Rightarrow (ab)c = a(bc)$ in G and hence in H

Inversion $\Rightarrow$ $aa^{-1} = e$ in G
$\Rightarrow e \in H$ is id. ☑

Example

$\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{C}$ is a field.
All that's needed is that $\mathbb{Q}(\sqrt{2})^*$ closed under $(\cdot)$, $(\,)^{-1}$

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

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

More examples of groups:

general linear group $GL_n(\mathbb{F}) = \{A \in \mathbb{F}^{n\times n} \mid \det(A) \neq 0\} = (\mathbb{F}^{n\times n})^*$

$GL_n(\mathbb{C})$
$\vee$
$GL_n(\mathbb{R})$
$\vee$
$GL_n(\mathbb{Q})$
$\vee$
$GL_n(\mathbb{Z})$ ... maybe. As it turns out, not a group, it's a monoid.

Special linear group: $SL_n(\mathbb{F}) = \{A \in \mathbb{F}^{n\times n} \mid \det A = 1\}$

$SL_n(\mathbb{R})$

Orthogonal group $O_n(\mathbb{R}) = \{A \in \mathbb{R}^{n\times n} \mid AA^T = I\}$

$AA^T = I$ and $BB^T = I$
$(AB)(AB)^T = ABB^TA^T = I$

we have $(\mathbb{Z}^{n\times n})^* = \{A \in \mathbb{Z}^{n\times n} \mid \det A \in \mathbb{Z}^*\}$
$\mathbb{Z}^* = \{\pm 1\}$

So we define $GL_n(\mathbb{Z})$

Next:

$SL_n(\mathbb{R})$
$\vee$
$\{A \in \mathbb{R}^{n\times n} \mid \det A = 1 \text{ and } AA^T = I\}$ $SO_n(\mathbb{R})$ $\subseteq S_n(\mathbb{R})$

"What is this screaming for?
It's screaming for a Lemma"

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

More examples:

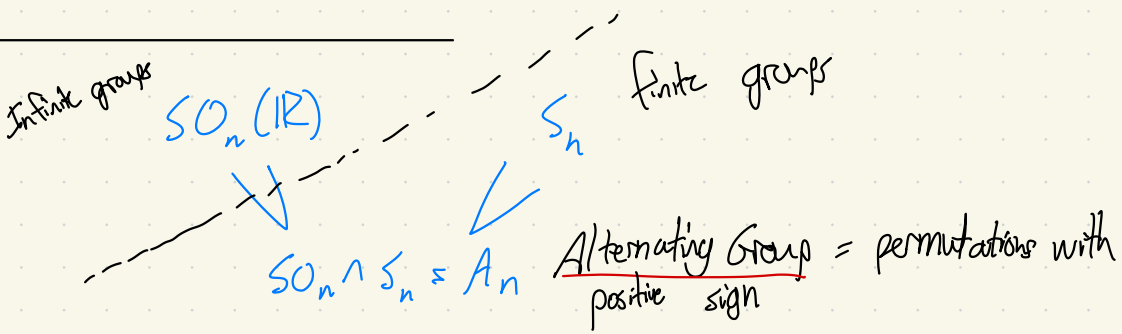
$$S_n = \{P \in \mathbb{R}^{n \times n} \mid P \text{ is a permutation matrix}\}$$

Def: A permutation of a set X is a bijection $X \to X$.

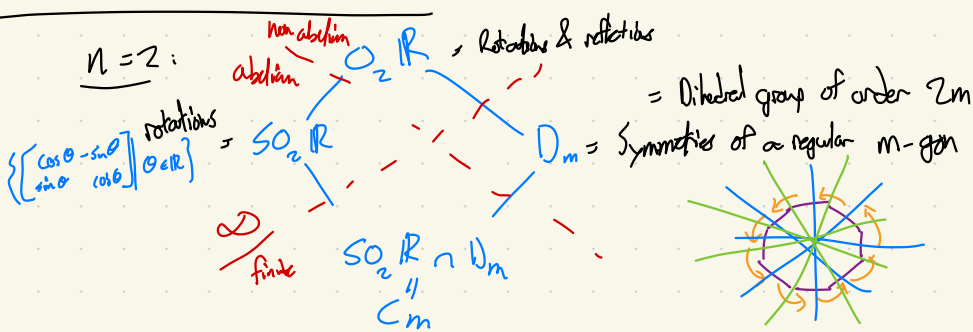
S_n = permutations of $\{1, \dots, n\}$

e.g. $\begin{matrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 2 & 1 & 3 \end{matrix} \longleftrightarrow \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$

one-line notation



$n = 2$:



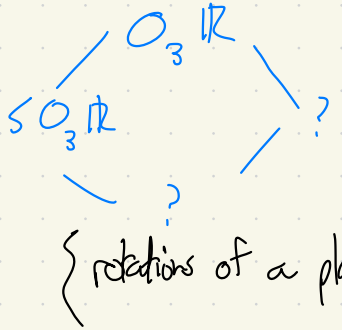
Cyclic Group of order m

$\parallel$

{rotations of a regular m-gon}

= {symmetries of m-pinwheel}

$n=3$



{symmetries of a platonic solid}

{rotations of a platonic solid}

Uniqueness for fixed a

- identity: $ga=a \Rightarrow g=e$

$$e = aa^{-1} = (ga)a^{-1}$$
$$= g(aa^{-1})$$
$$= ge \quad \text{since } aa^{-1}=e$$

so $e = ge = g$

More generally, operation in G is called cancellative

That is, $ab=ac \Rightarrow b=c$

- inverses: $ab=e \Rightarrow b=a^{-1}$
- bracketing: $a_1 \cdots a_n$ is well defined independent of bracketing

Proof: Induction on n.

Base case: $n=3$ $\quad a(bc)=(ab)c$ by definition

$n \geq 4$: show every bracketing equals $((\cdots((a_1a_2)a_3)\cdots)a_{n-1})a_n$

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

$k \geq 1$

$(ab)c = (\underbrace{\text{--}}_{b})a_n^{c}$ by induction

then rewrite as based by induction ☑

Question: $(a_1 \cdots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_1^{-1}$

Def $a^n = \underbrace{a \cdots a}_{n}$ for $n \in \mathbb{N}$

$a^0 = e$

$a^{-n} = \underbrace{a^{-1} \cdots a^{-1}}_{n}$

So a^n defined for all $n \in \mathbb{Z}$

Lemma "This is the course where you prove stupid looking statements...
... and we're about to make a stupid looking statement"

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

Warning don't write $\frac{a}{b}$. Is it ab^{-1} or $b^{-1}a$?

also $(ab)^n \neq a^n b^n$ in general (commutativity issues)

Subgroups of $\mathbb{Z}$

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

$H = 2\mathbb{Z}$

$p\mathbb{Z}$ p prime

$n\mathbb{Z}$ $n \in \mathbb{Z}$ $(n\mathbb{Z} = -n\mathbb{Z})$

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

Proof $H = \{0\} \Rightarrow d = 0$ ✓

Assume $|H| > 1$. Pick $d \in H$, $d \neq 0$ and $|d|$ minimal

WLOG $d \geq 0$ because $-d \in H$.
(don't type this in TeX)

Claim: $H = d\mathbb{Z}$

Proof: $\cdot\ d\mathbb{Z} \subseteq H$: $d \in H \Rightarrow \underbrace{d + \cdots + d}_{n \in \mathbb{Z}} \in H$

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

Then $qd \in H \Rightarrow r = m - qd \in H$.
But $r = 0$ by minimality (d had smallest absolute value)

Eg. $4\mathbb{Z} + 6\mathbb{Z} = \langle 4, 6 \rangle \leq \mathbb{Z}$
= subgroup generated by 4, 6.
$\{a+b \mid a \in A, b \in B\}$ = smallest subgroup containing 4 & 6.

But $\langle 4, 6 \rangle \neq \langle 4 \rangle$ and $\neq \langle 6 \rangle$
$\langle 4, 6 \rangle = \langle 2 \rangle = 2\mathbb{Z}$.

Corollary: $\langle a, b \rangle = \langle \gcd(a, b) \rangle$

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

$\Rightarrow d \mid a$ and $d \mid b$. But $d = \alpha a + \beta b$ for some $\alpha, \beta \in \mathbb{Z}$
so $d' \mid a$ and $d' \mid b \Rightarrow d' \mid (\alpha a + \beta b) = d$ ☐
anything that divides a and b divides d as well.

Def: In a group G, the cyclic subgroup generated by $a \in G$ is $\langle a \rangle$

$= \{\text{the set of powers of } a\}$

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

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

E.g. In $G = \mathbb{Q}^*$, $a = 3 \Rightarrow$

$\langle a \rangle = \{\dots, \frac{1}{9}, \frac{1}{3}, 1, 3, 9, 27, \dots\}$

E.g. In $G = S_5$, $a = (1\,3\,4)(2\,5)$ in cycle notation for $\begin{matrix} 1 \to 3 \\ \uparrow \quad \swarrow \\ 4 \end{matrix}$ $\begin{matrix} 2 \\ \downarrow \\ 5 \end{matrix}$

$|a| = ?$

a^0	a^1	a^2	a^3	a^4	a^5	a^6
e	a	$(1\,4\,3)$	$(2\,5)$	$(1\,3\,4)$	$(1\,4\,3)(2\,5)$	e

So $|a| = 6$

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

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

- $d = 0 \iff |a| = \infty$
- $d > 0 \iff |a| = d$

Proof: S is a subgroup:

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

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

$\Rightarrow -m \in S.$

In any group, important: $a^m = a^n \iff a^{m-n} = e \iff m - n \in d\mathbb{Z}$

- $d = 0$: $\iff m = n$
- $d > 0$: $\Rightarrow \langle a \rangle = \{e, a, a^2, \dots, a^{d-1}\}$ (all distinct)

$\Rightarrow |\langle a \rangle| = d$ ✅

Revisiting def of proof: we don't need to stipulate that $a \mapsto a^{-1}$ is a bijection

We have

$$\begin{cases} \text{associativity} \\ ae = ea = a \ \ \forall a \in G \\ \forall a \in G \ \exists\, b \in G \text{ with } ab = e \end{cases}$$

$ab = e \Rightarrow abr = er$ (define $b = r$)

$ae = er$

$a = r$. ☑

Homomorphisms

"there's just too many m's and n's you don't know where to stop"

Def. A map $\varphi : G \to G'$ of groups is a

- **homomorphism** if $\varphi(ab) = \varphi(a)\varphi(b)$ (in G / in G')
- **isomorphism** if also φ is bijective

we write $G \xrightarrow{\sim} G'$ or $G \cong G'$

Examples

1. $GL_n(\mathbb{F}) \xrightarrow{\det} \mathbb{F}^*$ because $\det(AB) = \det(A)\det(B)$

   $O_n(\mathbb{R}) \xrightarrow{\det} \{\pm 1\} = \mathbb{Z}^*$

   $S_n \xrightarrow{\det} \{\pm 1\}$

> **Sidenote.**
> **Def** A unit in a monoid M is an element with a two-sided inverse.
> $u \in M^*$ if $\exists\, a \in M$ with $au = ua = e$

2. Fix $P \in GL_n F$. Then $GL_n F \xrightarrow{\sim} GL_n F$ $(A \mapsto PAP^{-1})$ (Conjugation by P, similarity, change of basis, etc.)

   Check: $\varphi(AB) = PABP^{-1} = PAP^{-1}PBP^{-1} = \varphi(A)\varphi(B)$

3. C_∞ = infinite cyclic group

$\langle a \rangle = \{ \dots, a^{-2}, a^{-1}, e, a, a^2, \dots \}$

$|a| = \infty$

$\Rightarrow \mathbb{Z} \xrightarrow{\sim} C_\infty$

$1 \mapsto a$

$C_d = \langle a \rangle = \{ e, a, a^2, \dots, a^{d-1} \}$

$\Rightarrow \mathbb{Z} \twoheadrightarrow C_d$

$1 \mapsto a$ $\quad \varphi(m+n) = a^{m+n} = a^m a^n$

surjective

4. $\varphi : F^+ \to GL_2 f$

$a \mapsto \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$ $\quad \varphi(a+b) = \varphi(a)\varphi(b) = \begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix}$

f = field? ✓ Turns out f can be

$f = \mathbb{Z}$? ✓ any ring.

5. $\mathbb{Q}^n \to \mathbb{Q}^m$ homomorphisms $\Leftrightarrow$ linear

$\mathbb{R}^n \to \mathbb{R}^m$?

Exercise: Find $\mathbb{R}^n \to \mathbb{R}^m$ which is a homomorphism but not linear

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

Proof: isomorphisms are bijections. ∎

Lemma': If $\varphi : G \xrightarrow{\sim} G'$ then $|a| = |\varphi(a)| \quad \forall a \in G$

Proof: $\varphi(\langle a \rangle) = \langle \varphi(a) \rangle$

Def: An isomorphism $G \xrightarrow{\sim} G$ is an automorphism

$\mathrm{Aut}(G) :=$ set of automorphisms of G

Example: conjugation by $g \in G$ is an automorphism: $a \mapsto gag^{-1}$
$g^{-1}ag \mapsto a$
Inner automorphism

Example: $\mathrm{Aut}\, C_8 = ?$

$C_8 = \langle a \rangle = \{e, a, a^2, a^3, a^4, a^5, a^6, a^7\}$
orders: $1 \mid 8 \mid 4 \mid 8 \mid 2 \mid 8 \mid 4 \mid 8$

By lemma, $|\langle a \rangle| = |\varphi(\langle a \rangle)| = 8$

$\varphi: C_8 \to C_8$ determined by $\varphi(a)$ (ex. $\varphi(a^3) = \varphi(a)\varphi(a)\varphi(a)$)

So $\varphi(a) \in \{a, a^3, a^5, a^7\}$

try $\varphi: C_8 \to C_8$, $b \mapsto a^2 b$ but $\varphi(xy) = a^2xy \neq \varphi(x)\varphi(y) = (a^2x)(a^2y)$

try $\varphi(b) = b^3$ — works!

Lemma: G abelian $\Rightarrow G \xrightarrow{\varphi_n} G$, $g \mapsto g^n$ is a homomorphism.

$\Downarrow$

$|\mathrm{Aut}\, C_8| = 4$

Proof: check.

Proposition: If $\varphi: G \to G'$ is a homomorphism then

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

(ii) $\mathrm{im}\,\varphi = \{\varphi(a) \mid a \in G\}$
$\ker\varphi = \{a \in G \mid \varphi(a) = e'\}$ kernel of φ } are subgroups

(iii) $\ker\varphi$ is a normal subgroup. That is
$a \in \ker\varphi$ and $g \in G \Rightarrow gag^{-1} \in \ker\varphi$
→ closed under conjugation by G

(iv) φ surjective $\Leftrightarrow \mathrm{im}\,\varphi = G'$
φ injective $\Leftrightarrow \ker\varphi = \{e\}$

Proof: (i) $\varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1})$

$= \varphi(e) = e'$

$a = e$:

$\varphi(e) = \varphi(e)\varphi(e)$

$e' = \varphi(e)$

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

(ii) $a' = \varphi(a)$ and $b' = \varphi(b) \Rightarrow a'b' = \varphi(a)\varphi(b) = \varphi(ab)$

$(a')^{-1} = \varphi(a^{-1})$ by (i) so $\operatorname{Im}\varphi \leq G$

$\varphi(a) = e'$ and $\varphi(b) = e' \Rightarrow \varphi(ab) = \varphi(a)\varphi(b) = e'e' = e'$

$\varphi(a^{-1}) = \varphi(a)^{-1} = (e')^{-1} = e'$ so $\ker\varphi \leq G$

(iii) $a \in \ker\varphi \Rightarrow \varphi(a) = e'$

$\Rightarrow \varphi(gag^{-1}) = \varphi(g)\varphi(a)\varphi(g^{-1})$

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

(iv) $\operatorname{im}\varphi = G' \Rightarrow \varphi$ surjective by definition

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

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

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

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

i.e.

$[\varphi(c) = e' \Leftrightarrow c = e \ \forall c \in G]$

$\Rightarrow \ker\varphi = \{e\}$ ☑

Equivalence Relations

Fix a set S.

1. a partition of S: $S = \bigsqcup_{i \in I} S_i$ (disjoint union; block; index set)
   with $S_i \neq \emptyset$ and $S_i \cap S_j = \emptyset \ \forall i \neq j$

2. equivalence relation $\sim$ on S:
   for some pairs $a, b \in S$, we have $a \sim b$. Must be:
   - Reflexive: $a \sim a \ \forall a \in S$
   - Symmetric: $a \sim b \Leftrightarrow b \sim a \ \forall a, b \in S$
   - Transitive: $a \sim b$ and $b \sim c \Rightarrow a \sim c \ \forall a, b, c \in S$

   Formally, $\sim \subseteq S \times S$ $\{(a,b) \mid a \sim b\}$

   $S \times S$ has 2 maps
   $(a,b) \to b$
   $S \times S \xrightarrow{\pi_2} S$
   $\pi_1 \downarrow$
   $a \quad S$

   Note a relation is just a subset of $S \times S$

   The equivalence class of a is
   $[a], \bar{a}, \ldots = \{x \in S \mid x \sim a\}$

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

This stuff is all equivalent!

E.g. 1

(i) $\{1,2,3,4,5\} = \{1,3\} \cup \{2,5\} \cup \{4\}$

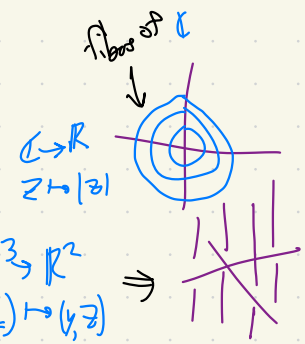
(ii) $\mathbb{Z} = \{\text{evens}\} \cup \{\text{odds}\}$

E.g. 2

(i) $1 \sim 3 \quad 2 \sim 5 \quad \forall a, a \sim a$
$3 \sim 1 \quad 5 \sim 2$
$[3] = [1] = \{1,3\}$

(ii) $\{\text{evens}\} \cup \{\text{odds}\}$
$\| \qquad \|$
$\bar{0} \qquad \bar{1}$

E.g.



Proof:

3 ⇒ 1: $S = \bigcup_{t \in T} \varphi^{-1}(t)$. No empty fibre b/c surjection. Disjoint b/c function.

1 ⇒ 2: blocks are equivalence classes

2 ⇒ 3: $S \to$ Quotient set

General example

G group

$a \sim b$ if $gag^{-1} = b$ for some $g \in G$

↗ similarity of matrices, change of basis

Conjugacy classes!

Check:

$g = e \Rightarrow eae^{-1} = a \Rightarrow a \sim a$

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

$a \sim b, b \sim c \Rightarrow a \sim c \to gag^{-1} = b,\ hbh^{-1} = c$

$hgag^{-1}h^{-1} = c$

Ex: $G = S_3 = \{e, (12), (13), (23), (123), (132)\}$

What are the conjugacy classes?

if something commutes with everything, then it's in its own conjugacy class

↓

abelian groups?

every element in an abelian group is its own conjugacy class

e | (12) (23) (13) | (123) (132)

$geg^{-1} = e$ always

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

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

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

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

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

Remark (as promised): Can use $S \to T$ not surjective but must omit empty fibers from partition.

General Example: homomorphism $\varphi: G \to G'$ $\quad N = \ker\varphi = \{g \in G \mid \varphi(g) = e'\}$

$$\varphi(a) = \varphi(b) \iff e' = \varphi(a)^{-1}\varphi(b)$$
$$= \varphi(a^{-1}b)$$
$$\iff a^{-1}b \in N$$
$$\iff b \in aN$$

all nonempty fibers have the form aN for some $a \in G$.

looks kind of like $y = mx$

$\varphi^{-1}(\varphi(a)) = aN \to$ coset!

$\varphi(aN) = \varphi(a)\varphi(N)$, $\varphi(N) = e'$

Cosets of kernel are fibers

Cosets

fix subgroup $H \leq G$.

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

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

Prop: The left cosets of H partition G.

Proof: $a = ae$ and $e \in H \Rightarrow a \equiv a$

$b = ah \Rightarrow a = bh^{-1}$ and $h^{-1} \in H \Rightarrow a \equiv b \iff b \equiv a$

$b = ah$ and $c = bh' \Rightarrow c = ahh'$ and $hh' \in H \Rightarrow a \equiv b,\ b \equiv c \Rightarrow a \equiv c$

Corollary: $aH \cap bH \neq \emptyset \iff aH = bH$

Def: G/H (G "mod" H) $= \{$left cosets of H in $G\}$

$G \twoheadrightarrow G/H$ has fibers aH for $a \in G$

Example: Another way to see S_3

e	(12)	(23)	(13)	(123)	(132)
1	x	y	xyx $=yxy$	xy	yx

So we can write $S_3 = \langle x, y \mid x^2=1,\ y^2=1,\ xyx=yxy \rangle$

(x, y: generators; relations)

$H = \langle x \rangle \leq S_3$ $= \{1, x\}$ cosets: $\begin{cases} H \\ yH \\ xyH \end{cases}$

Example: $G = \mathbb{Z}$, $H = 2\mathbb{Z}$

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

For fun: $H = 3\mathbb{Z}$

Note: We can use the fact that homomorphisms have inverses on HW

Def: The index of a subgroup $H \leq G$ is $[G:H] = |G/H|$ (set of left cosets of H $=$ # of left cosets of H)

Proposition: All cosets of H have the same size (cardinality).

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

Proof: Consider $aH \to bH$. To get this map, we left multiply by ba^{-1}. That is, $g \mapsto ba^{-1}g$. Then this has an inverse $ab^{-1} \leftarrow\!\shortmid g$ so our map is bijective and all cosets have the same size.

Now consider $|G| = |H|[G:H]$. Both sides will be ∞ unless $[G:H] = r < \infty$ in which case $G = a_1H \cup \cdots \cup a_rH \Rightarrow |G| = |a_1H| + \cdots + |a_rH| = r|H|$. ∎

($\cup$: dot = disjoint union)

Corollary [Lagrange's theorem]: If $H \leq G$ and G finite then $|H| \mid |G|$. (specifically, $|G| = |H|[G:H]$)

"This is how we know we've really gotten to algebra"

Corollary: $a \in G \Rightarrow |a| \mid |G|$

Proof: $|a| = |\langle a \rangle|$ by def. and since $\langle a \rangle \leq G$, we get done by Lagrange's theorem.

Corollary: $|G| = p$ prime $\Rightarrow G \cong C_p$. (C_p = cyclic group of order p)

Proof: Let $g \in G$. Either $g = e$ so $|g| = 1$ or $g \neq e$, so $|g| = p$ and $G = \langle g \rangle$.

Prop: $\varphi: G \to G'$ homomorphism. Then $|G| = |\ker\varphi| \cdot |\mathrm{im}\varphi|$

So this is basically rank-nullity theorem

E.g.: $G = F^d$, where $|F| = q < \infty$ then G is an F-vector space.

Take $\varphi: G \to V$ F-linear. Then

$\dim G = \dim(\ker\varphi) + \dim(\mathrm{im}\varphi)$

(nullity, rank)

$d = n + r$

$|\dim G| \quad |\ker\varphi| \quad |\mathrm{im}\varphi|$

$q^d = q^n \cdot q^r$

if the dimensions add, the orders multiply

W is an F-vector space where $|F| = q < \infty$ then $|W| = q^{\dim W}$

Proof: $\mathrm{im}\varphi$ is a subset of G' so $\mathrm{im}\varphi \leftrightarrow \{\text{nonempty fibers of } \varphi\}$ (bijection)

$= G/H$ for $H = \ker\varphi$

$\Rightarrow |\mathrm{im}\varphi| = \left|\frac{G}{H}\right| = [G:\ker\varphi]$

So $|G| = |H|[G:H] = |\ker\varphi||\mathrm{im}\varphi|$

Modular arithmetic "let us recognize modular arithmetic in our day-to-day lives... but first, let's define it"

Def: for $a, b, n \in \mathbb{Z}$, we write $a \equiv b \pmod n$ if (equivalently): $n \mid (a-b)$

a is congruent to b modulo n

$a - b \in n\mathbb{Z}$

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

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

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

Proof: Division with remainder: $m = qn + r$ with $0 \leq r \leq n-1$ ($|n|$)

$\mathbb{Z}$ is a commutative ring

Question: $\mathbb{Z}$ have $+, 0, -, \times, 1$; 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 $\mathbb{Z}/n\mathbb{Z}$.

"$\mathbb{Z}/n\mathbb{Z}$ is a ring"

"$\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is a homomorphism of rings"

Proof: Need: $a-a' \in n\mathbb{Z}$ and $b-b' \in n\mathbb{Z}$ $\Rightarrow$ $\overline{a+b} = \overline{a'+b'}$

But $(a+b)-(a'+b') = \underbrace{(a-a')}_{\in n\mathbb{Z}} + \underbrace{(b-b')}_{\in n\mathbb{Z}} \in n\mathbb{Z}$

$n\mathbb{Z}$ is an ideal $\Rightarrow$ closed under multiplication by anything in $\mathbb{Z}$.

Now for $\overline{ab} \overset{?}{=} \overline{a'b'}$, we have $ab - a'b' = ab - ab' + ab' - a'b'$

$a(b-b') + (a-a')b' \in n\mathbb{Z}$ ✓

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

$\bar{0}+\bar{0} = \bar{0}$ even + even = even

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

$\bar{0}\,\bar{0} = \bar{0}$

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

E.g. $n=12$ "clock arithmetic"

E.g. $n=10$ "the last digit of $2179 \cdot 636$ is 5"

$\overline{2179} \cdot \overline{636} = \bar{9}\cdot\bar{6} = \overline{15} = \bar{5}$

$\overline{2179} \cdot \overline{636} = \bar{9}\,\bar{6} = \overline{54} = \bar{4}$

E.g. $n=7$ "weekdays"

What day of the week will Sep 14th, 2024 be?

Thu $\equiv 5 \pmod 7$ $\qquad 365 \equiv 1 \pmod 7$

$\overline{350} + \overline{15} = \bar{1}$

Thu + 365 + 1 $\equiv 5+1+1 \pmod 7$

$\equiv$ Saturday

Question $(\mathbb{Z}/n\mathbb{Z})^* = ?$

m invertible $\Leftrightarrow$? $\Leftrightarrow$ $am \equiv 1 \ (n)$ for some $a \in \mathbb{Z}$

$\Leftrightarrow am \in 1 + n\mathbb{Z}$

$\Leftrightarrow am \in 1 - bn$

$\Leftrightarrow am + bn = 1$ → bezout's

$\gcd(m,n) = 1$

E.g. music theory $n=12$

$\mathbb{Z}/12\mathbb{Z} = \{C, C^\#, D, D^\#, \ldots, \underbrace{B^\flat}_{=A^\#}, B\}$

$\# = +1$ on notes

$\flat = -1$

octave $\equiv$ unison

octave + third $\equiv$ third

E.g.: Circle of fifths:

$\ldots, B^\flat, F, C, G, D, A, \ldots$ (2♭, 1♭, ♮, 1♯, 2♯, 3♯)

$0 \quad 7 \quad 14 \equiv 2 \quad 9$

$\# = +7$ on key signatures

$\gcd(7,12) = 1 \Rightarrow$ all

Dmitry Tymoczko

"The geometry of music"

Groups of small order

$\lvert G \rvert$	abelian	non-abelian
1	$\{e\}$	
2	$C_2 \cong \mathbb{Z}/2\mathbb{Z}$	
3	C_3	
4	C_4, $C_2 \times C_2$	None by HW
5	C_5	
6	$C_6 \cong C_2 \times C_3$	$S_3 \cong D_3$
7	C_7	
8	C_8, $C_2 \times C_4$, $C_2 \times C_2 \times C_2$	Q_8, D_4

Lemma The product

$G \times G' = \{(g, g') \mid g \in G, g' \in G'\}$

is a group under componentwise composition

$(g_1, g_1') \circ (g_2, g_2') = (g_1 \circ g_2, g_1' \circ g_2')$

($\circ$ in $G \times G'$; $g_1 \circ g_2$ in G; $g_1' \circ g_2'$ in G')

Proof: no

Homomorphisms:

$G \times G' \to G'$ (projection)

G

$G \to G \times G'$, $g \mapsto (g, e')$ (e' in G'; g' in G')

	1	(12)	(13)	(23)	(123)	(132)
1	1	(12)	(13)	(23)	(132)	(123)
(12)	(12)	1	(123)	(132)	(13)	(23)
(13)	(13)	(132)	1	(123)	(23)	(12)
(23)	(23)	(123)	(132)	1	(12)	(13)
(123)	(123)	(23)	(12)	(13)	(132)	1
(132)	(132)	(13)	(23)	(12)	1	(123)

multiplication table for S_3

$C_4 = \langle a \rangle$ $\quad C_2 \times C_2 = \langle x \rangle \times \langle y \rangle$ $\quad (1, x, 1, y)$

$C_6 = \langle a \rangle \quad C_2 \times C_3 = \langle x \rangle \times \langle y \rangle$

$a \longrightarrow xy$

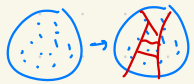
C_4 has an element of order 4

$C_2 \times C_2$ doesn't have any elements of order 4

$Q_8 = \{\pm 1, \pm i, \pm j, \pm k \mid ij = -ji = k\}$

Quotient Groups

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



A: when $H \trianglelefteq G$.

Proof: ($\Rightarrow$): Prop p.6: $\ker(G \to G/H) = H$

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

Lemma: if $H \trianglelefteq G$, then ($\forall$) $gH = Hg \ \forall g \in G$

Proof: ($\Rightarrow$)
$$gH = \{gh \mid h \in H\} = \{g(g^{-1}hg) \mid h \in H\} = \{hg \mid h \in H\} = Hg$$ ☑

Also, ($\in$) holds. Proof is simple enough.

Now compute
$$\begin{aligned} (aH)(bH) &= (a(Hb)H) \\ \overline{a}\ \overline{b} &= (ab\,H)H \\ &= abHH \\ &= abH \\ &= \overline{ab} \end{aligned}$$

Ex. Let G a group and S a set with a map $S \times S \to S : (s,t) \mapsto st$.
If $\varphi : G \to S$ with $\varphi(ab) = \varphi(a)\varphi(b) \ \forall a, b \in G$ then S is a group.

Now take $S = G/H$

Cor: $N \trianglelefteq G \iff \exists$ hom. $\varphi : G \to G'$ with $\ker \varphi = N$.

Proof: ($\Rightarrow$): prop p.8 (replace G' by $\operatorname{im} G$ for surjectivity)

($\Leftarrow$) $\varphi : G \twoheadrightarrow G/N$ ☑

Examples: $n\mathbb{Z} \trianglelefteq \mathbb{Z}$

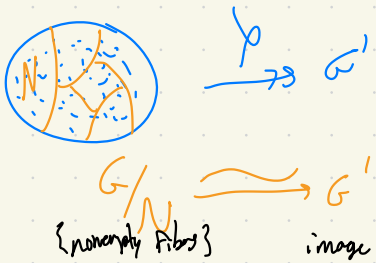
$n\mathbb{Z} = \ker(\mathbb{Z} \to C_n = \langle a \rangle)$, $1 \mapsto a$

$\mathbb{Z}/n\mathbb{Z} \cong C_n$

In general: What if $G \xrightarrow{\varphi} G'$ with $N = \ker\varphi$

then $G' \cong G/N$ (First isomorphism theorem)

$G/N \xrightarrow{\sim} G'$



Proof: exercise.

How it's used:

1. $G/\ker\varphi \xrightarrow{\sim} \operatorname{im}\varphi$
2. If $G \to G'$ by φ is any homomorphism and $N \trianglelefteq G$ with $N \leq \ker\varphi$ then φ induces a homomorphism $G/N \to G'$

Group Actions

General principle:

Aut (anything) } Form a group
Symmetry (anything) }

$id: X \to X$ $\quad id(x) = x$

$g: X \xrightarrow{\sim} X$
$g': X \to X$
$\Rightarrow g' \circ g: X \to X$
$g^{-1}: X \to X$

$x \in X \Rightarrow gx \in X$
$g'(gx) \in X$

Def a group action (or operation) of G on a set S is a map $G \times S \to S$ $\quad (g, s) \mapsto gs$

Satisfying:

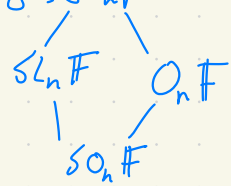
(i) $1s = s$

(ii) $\forall g, g' \in G$, $g'(gs) = (g'g)s$ (in S / in G)

$\forall s \in S$.

Terminology: S is a G-set with a left action (note: right action $S \times G \to S$, $(s,g) \mapsto sg$)

E.g. 1. $S = \mathbb{F}^n$, $G = GL_n\mathbb{F}$



$SO_2(\mathbb{R}^2) \times \mathbb{R}^2 \to \mathbb{R}^2$

2. $G = S_n$ $S = \{1, \dots n\}$

3. $S =$ points in $\mathbb{R}^n$ / lines / planes / ⋮ $G =$ rigid motions or $G =$ translations

Notation $\lambda_g : S \to S$, $s \mapsto gs$ left multiplication by g

$\rho_g(s) = sg$

7. $S = \mathbb{F}^{n \times n}$ $G = GL_n\mathbb{F}$

Left action $\lambda_g(s) = gs$ $\lambda'_g(s) = sg^{-1}$

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

$\rho : S \times G \to S$, $(s,g) \mapsto sg$

$\rho_g =$ restriction of ρ to g

4. $S =$  $G =$ cyclic, dihedral

$S =$  , [icosahedron]

$G = A_4$ S_4 A_5 → analog of cyclic

S_4 $S_4 \times C_2$ H_3 → analog of dihedral = doesn't have to preserve orientation of ambient space (includes reflections)

$A_4 \trianglelefteq S_4$

5. $S = \mathbb{C}$ $\quad G = C_2 = \{1, r\}$

$r \cdot \alpha = \bar{\alpha}$

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

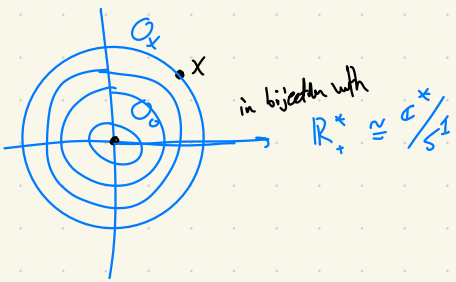
Def Let G act on S we write $G \curvearrowright S$

The orbit of $s \in S$ is

$$\mathcal{O}_s = \{gs \mid g \in G\}$$

$$= Gs$$

Example 1 $\quad G = SO_2\mathbb{R}$, $S = \mathbb{R}^2$



2. S_n $\quad \mathcal{O}_i = \{1, \dots, n\}$ $\forall i$ $\quad$ **Def.** transitive = 1 orbit

3.

S	G = rigid motions	G = translations
points	transitive	transitive
lines	transitive	parallel class of $l = \mathcal{O}_l$
planes	"	"

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

$= \{\alpha\}$ if $\alpha \in \mathbb{R}$

Lemma: the orbits of G on S partition S.

Proof: write $s \sim s'$ if $s' = gs$ for some $g \in G$.
Prove equivalence relation. ☑

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

Proof: almost trivial ☑

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

Smaller orbit $\iff$ bigger stabilizer

Eg. 1. $G_0 = SO_2$
$G_x = \{id\}$

3. G_s = rotations/reflections about s $\quad$ G_ℓ = translations along ℓ

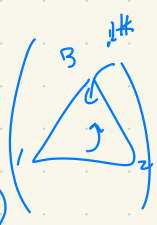
5. $G_\alpha = \{1\}, G$

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

Proof: $(ba^{-1})aH = bH$

Q. $G_{1H} = H$

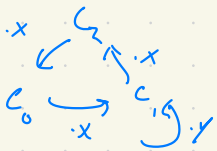
E.G. Symmetries



$H = \{1, y\}$

$G/H = \{1, y\}\ C_0$
$\{x, xy\}\ C_1$
$\{x^2, x^2y\}\ C_2$

$D_3 = \langle x, y \mid x^3 = 1, y^2 = 1, xy = yx^2 \rangle$



Prop: $G \curvearrowright X \iff G \xrightarrow{\text{hom}} S_X$, $g \mapsto \lambda_g$

Where $\lambda_g : X \to X$, $x \mapsto gx$

$D_3 = \langle x, y \mid x^3 = 1,\ y^2 = 1,\ xy = yx^2 \rangle$ (rotation, reflection)

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

Ex.: $D_3 \xrightarrow{\varphi} S_3 = \text{permutations}\ (D_3/H)$ for $H = \langle y \rangle$

$\lambda_g : aH \mapsto gaH$

$\ker \varphi \leq H$ since $g \cdot C_i = C_i\ \forall i = 1,2,3$

$\Rightarrow gH = H$

$\Rightarrow g \in H$

but $y \cdot \{x, xy\} = \{x^2, x^2y\}$ (C_2, C_3)

$y \mapsto (23)$

Any (injection / surjection) b/w finite sets is a (surjection / injection)

$\Rightarrow |\ker \varphi| = 1 \Rightarrow \varphi$ isomorphism $\Rightarrow D_3 \xrightarrow{\sim} S_3$, $D_3 \cong S_3$

Prop: Fix $G \curvearrowright X$ and fix $x \in X$ with stabilizer $G_x = H$ and orbit $\mathcal{O}_x$ ($\mathcal{O}$: \mathcal{O})

There is a natural bijection

$G/H \xrightarrow{\varphi} \mathcal{O}_x$, $aH \mapsto ax$

It satisfies $\varphi(gC) = g\varphi(C)$ for $g \in C$ and $C \in G/G_x$

Proof: Need $aH = bH \Rightarrow ax = bx$

But $aH = bH \iff a^{-1}b \in H$

$\iff a^{-1}bx = x$

$\iff bx = ax$

φ surjective by def

injective b/c $bx = ax \Rightarrow aH = bH$

Loose ends: $G \leq \mathrm{Isom}(\mathbb{R}^2)$ finite $\Rightarrow G \cong C_n$ or D_n

translations have infinite order $\Rightarrow \notin G$

Need $r \in G$ rotation $\Rightarrow G \cong D_n$

Proof: $H = \{\text{rotations in } G\} \leq G$

$\Rightarrow H \cong C_n$ for some n

$\Rightarrow G \geq H \cup rH = D_n$

But $g \in G$ reflection $\Rightarrow \sigma^{-1} g =$ rotation

$\Rightarrow g \in rH$ ☑

Aside

$r \in O_2(\mathbb{R}) \xrightarrow{r \mapsto -1} \{\pm 1\}$

$g \in O_2(\mathbb{R}) \xrightarrow{g \mapsto -1} \{\pm 1\}$ $\Rightarrow rg \mapsto 1$ bc sign is a homomorphism

Loose ends 2:

Prop: Let $G \curvearrowright X$ fix $x \in X$ and $x' \in G_x$, say $x' = ax$

Then $\{g \in G \mid gx = x'\} = aG_x$

and $G_{x'} = aG_x a^{-1}$ ⟶ change of basis!

$x \mapsto x'$ $x \mapsto x$ $x' \mapsto x$

Counting

Recall $|G| = |H| \cdot |G/H|$ ($[G:H]$). Let $G \curvearrowright X$

Cor: $|G| = |G_x| \cdot |O_x|$ for $x \in X$

Proof: $H = G_x$ + proposition

Lemma: $|X| = \sum_{\text{orbit } O} |O|$

Proof: The orbits partition X ☑

E.g. G = orientation-preserving isometries of icosahedron ($\to$ 20 sides) I = 

1. Q: $|G| = ?$

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

G acts $F = \{\text{faces of } I\}$ let $f \in F$

$|O_f| = |F| = 20$ $\quad |G| = |G_f| |O_f| = 3 \cdot 20 = 60$

$|G_f| = 3$

G acts on $V = \{\text{vertices of } I\}$

Let $v \in V$

$|G_v| = 12$

$|G_v| = 5$

$|G| = 5 \cdot 12 = 60$

$E = \{\text{edges of } I\} \Rightarrow |G| = ?$

$G \curvearrowright E$ let $e \in G$

$|G_e| = ?$

$|G_e| = 2$

$\Rightarrow |G_e| = 60/2 = 30$

3. $V \curvearrowleft H = G_v \Rightarrow |V| = 12 = 12 \cdot 1$ or $7 \cdot 1 + 5$ or $2 \cdot 1 + 2 \cdot 5$ ↓ not ok

$V = G_v v \dots$

Finite rotation groups

rotations about some line through the origin

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

- C_k cyclic group of rotations by $2\pi/k \cdot m$ about fixed l
- D_k dihedral group
- T symmetries of tetrahedral group $|T| = 12$
- O symmetries of octahedral $|O| = 24$
- I symmetries of icosahedral $|I| = 60$

Proof: Set $n = |G|$. $1 \neq g \in G$ then g fixes unique line l then g fixes a unique pair of points in S^2 poles $l \cap S^2$ of g

G acts on $P = \bigcup_{1 \neq g \in G} \text{poles}(g)$.

p is a pole of g and $a \in G$ then ap is a pole of aga^{-1}

$|P| =$ dunno.

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

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

How many times does $\rho \in \ell$ appear in M? $|G_\rho| - 1$

Set $r_\rho = |G_\rho|$. Then $|M| = 2n-2 = \sum_{\rho \in \ell} (r_\rho - 1)$

Note: $G_\rho \cong C_{r_\rho} = \langle \text{rot } \frac{2\pi}{r_\rho}(\ell) \rangle$

$\ell = \text{span } \rho$.

$r_\rho \geq 2$ since $1 \neq g \in G_\rho$ if $\rho \in \text{poles}(g)$.

Let $O_1, O_2, \ldots$ be the orbits. Set $m_i = |O_i|$

Observe: $r_\rho = r_{\rho'} = \frac{n}{m_i}$ if $\rho, \rho' \in O_i$ since $|G_\rho| \cdot |O_\rho| = |G|$, i.e. $r_i \cdot m_i = n$

$2n - 2 = \sum_i m_i (r_i - 1)$

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

$\Rightarrow$ # of orbits ≤ 3

# of orbits:

1: $2 - \frac{2}{n} = 1 - \frac{1}{r}$ ✗

2: $2 - \frac{2}{n} = 1 - \frac{1}{r_1} + 1 - \frac{1}{r_2}$

$\frac{2}{n} = \frac{1}{r_1} + \frac{1}{r_2}$

$\geq \frac{1}{2} \quad \geq \frac{1}{n}$

but $r_i \leq n$ since $r \mid n$

$\Rightarrow r_1 = r_2 = n$

$\Rightarrow |O_1| = |O_2| = 1$

$\Rightarrow \rho = \{\pm \rho\}$

$\Rightarrow G = G_\rho \cong C_\rho$

3: $\frac{2}{n} = \frac{1}{r_1} + \frac{1}{r_2} + \frac{1}{r_3} - 1$.

Assume $r_1 \leq r_2 \leq r_3$

Then $r_1 = 2$ 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: $r_2 \geq 3$

$\frac{2}{n} = \frac{1}{r_3} \Rightarrow n = 2r_3$ and $|O_3| = 2$

$\Rightarrow O_3 = \{\pm p\}$ and $G_p = C_r$ about $\ell = \text{span}(p)$

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

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

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

$r_2 \geq 3$

$\Rightarrow r_2 = 3$, $r_3 \geq 6$

$\Rightarrow \frac{1}{2} + \frac{1}{3} + \frac{1}{r_3} \leq 1$ ✗

$\Rightarrow r \in \begin{Bmatrix} (2,3,3) \\ (2,3,4) \\ (2,3,5) \end{Bmatrix}$ $n = 12$, $n = 24$, $n = 60$

$n = 60$, $r = (2,3,5)$

$|O_3| = \frac{60}{5} = 12$

12 vertices = icosahedron

Cayley's Theorem

Every finite group is isomorphic to a subgroup of S_n for some n.

Proof Let $n = |G|$. $G \curvearrowright G$ by $G \times G \to G$, $(g, x) \mapsto gx$

$$\Rightarrow G \xrightarrow{\varphi} S_n, \quad g \mapsto (\lambda g : x \mapsto gx)$$

What if $gx = x \Rightarrow g = 1$ (x^{-1}, x^{-1}) $\Leftrightarrow G_x = \{1\}$ (derangement)

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

Example of group acting on itself:

Conjugation $G \curvearrowright G$ by $G \times G \to G$, $(g, x) \mapsto gxg^{-1}$

Stabilizer $G_x = \{ g \in G \mid gx = xg \} = Z(x) \leq G$ (centralizer of x) Note: $1, x \in Z(x)$

$\ker (G \xrightarrow{\text{conjugation}} S_G) = Z(G)$, $a \mapsto (x \mapsto gxg^{-1})$ (center of G)

Class equation:

$$|G| = \sum_{\text{conjugacy classes } C} |C| \quad \text{(set, orbits)}$$

- Each $|C| \mid |G|$ since $|G| = |G_x||O_x|$ (basically Lagrange) (see page 16 of lecture notes)

E.g. $G = S_4$ $|S_4| = 24$

C_1	$C_{(12)}$	$C_{(123)}$	$C_{(12)(34)}$	$C_{(1234)}$	$24 = 1+6+8+3+6$
Size: 1	$\binom{4}{2} = 6$	$2 \cdot \binom{4}{3} = 8$	$\frac{1}{2} \cdot \binom{4}{2} = 3$	$24 - 18 = 6$ or $3!$	
			18		

Lemma: $x \in Z(G) \iff Z(x) = G$
$\iff$ conj. class of $x = \{x\}$
$\iff |C_x| = 1$

- At least one $|C| = 1$

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

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

Proof: $p \mid |C|$ $\forall$ conj. classes C except when $|C| = 1$

$\because p^e = |G| = 1 + \sum_{\text{classes } C \neq C_1} |C|$

(p divides; $|C| > 1$; so not for some C.)

$p \nmid |C| \Rightarrow |C| = 1$ since $|C| = p^k$ for some k.

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

Proof: $|Z(G)| \geq p$ by Prop (nontrivial & divides p^2).

Suppose $x \notin Z(G) \Rightarrow Z(x) \supseteq \{x\} \cup Z(G)$
$\Rightarrow |Z(G)| \geq p+1$
$\Rightarrow |Z(G)| = p^2$ ← must be: power of p, divide p^2, bigger than p
$\Rightarrow Z(x) = G$
$\Rightarrow x \in Z(G)$ ↯ ☑

Proof!: $H \leq Z(G)$, $G/H \Rightarrow G$ abelian. (midterm #3)

$|G/H| = p \Rightarrow$ cyclic. ☑

Cor: $|G| = p^2 \Rightarrow G \cong C_{p^2}$ or $C_p \times C_p$

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

The icosahedral group I

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

E.g. C_p p prime

Theorem: I is simple.

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

Proof: $x \in N \Rightarrow gxg^{-1} \in N \ \forall g \in G$. ☑

Lemma $\Rightarrow |N| = \sum_{C \subseteq N} |C|$

conjugate: $I \subsetneq I$

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

No subsum contains 1 and divides 60.

$\Rightarrow$ Can't construct normal subgroup $\neq \{1\}, I$

Corollary: $A_5 \cong I$ simple.

Proof: I acts on 5 inscribed cubes

$\Rightarrow I \xrightarrow{\varphi} S_5$

$\ker \varphi \neq I$ since I moves a cube.

$\Rightarrow \ker \varphi = \{1\}$ by Thm $(\ker \varphi \trianglelefteq I)$

$\Rightarrow I \hookrightarrow^{\varphi} S_5$

$[S_5 : I] = 2$ (120, 60)

sign: $S_5 \to \{\pm 1\}$

induces $I \to \{\pm 1\}$

$\ker\left(I \xrightarrow{\psi} \{\pm 1\}\right) \trianglelefteq I$

index $\neq 2$ by Thm $\Rightarrow$ index $= 1$

$\Rightarrow \ker \psi = I \Rightarrow I = A_5$ ☺

$\hookrightarrow I \xrightarrow{\psi} \{1\}$

$I \leq A_5$

but $|I| = |A_5| \Rightarrow I = A_5$

Let's prove the class equation for I:

Supposed to be $60 = 1 + 15 + 20 + 12 + 12$

$\lvert g \rvert$	#
1	1
2	≥ 15
3	≥ 20
5	≥ 24
6	60
12	
30	

X	$\lvert I_x \rvert$	#copies $\subseteq I$
face	3	$20/2 = 10$
edge	2	$30/2 = 15$
vertex	5	$12/2 = 6$

all conjugate

$I_f \cap I_{f'} = \{1\}$ bc cyclic of prime order (5) simple + at least one element differs

Same conjugacy class $\Rightarrow$ same order

do we have to break up any blocks?

$60 = 1 + 15 + 20 + 12 + 12$

15: order 2 $\Rightarrow$ non-identity elements are conjugate

Actions on subsets

$G \curvearrowright X \Rightarrow 2^X = \mathcal{P}(X)$ = subsets of X (maps from X into a set of order 2)

$U \subseteq X \Rightarrow gU = \{g_u \mid u \in U\}$

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

($\binom{X}{d}$: set of d-element subsets of X)

E.g. $G = O$ octahedral group

$\Rightarrow G \curvearrowright X$ = {vertices of $\square$}

$\left|\binom{X}{2}\right| = \binom{|X|}{2} = 28$ pairs of vertices

orbits:
- $\mathcal{O}_1 = 2(e)$ $\quad |\mathcal{O}_1| = 12$
- $\mathcal{O}_2$ = face diagonals $\quad |\mathcal{O}_2| = 2 \cdot 6 = 12$
- $\mathcal{O}_3$ = body diagonals $\quad |\mathcal{O}_3| = 8/2 = 4$

Note: $gU = U \Rightarrow g$ permutes U

Lemma: If $H \curvearrowright X$ and $U \subseteq X$ then H stabilizes U $(H_U = H)$ iff U a union of (some) $\underbrace{H\text{-orbits}}_{\text{in } X}$ ☑

Prop: Let $G \curvearrowright G$ by left mult.
Then $|G_u| \mid |U|$.

Proof: set $H = G_u$. Lemma $\Rightarrow$ U is a union of H-orbits.
H-orbit $= Hu$ (right coset of H)
$$\Rightarrow |U| = \sum_{\substack{H\text{-orbits} \\ \mathcal{O} \subseteq U}} |\mathcal{O}|$$
$$= k|H|.$$ ☑

Corollary: $\gcd(|U|, |G|) = 1 \Rightarrow G_u = \{1\}$.
Proof: $|G_u| \mid |G|$ by Lagrange and $|G_u| \mid |U|$ by prop. ☑

E.g. $G \curvearrowright G$ by conj. $H \leq G \Rightarrow G_H$ is the normalizer
$N_G(H) = \{g \in G \mid gHg^{-1} = H\}$

# of subgroups conj. to $H = [G : N_G(H)]$
$$= |G| / |N_G(H)|$$
$|G_H| \cdot |G_H| = |G|$

The Sylow Theorems

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

Sylow 1: G has a subgroup of order p^e called a Sylow p-subgroup.

Cor: G has an element of order p.
Proof: Let $H \leq G$ $|H| = p^e$.
Let $a \in H \setminus \{e\}$. $|a| = p^k$ by Lagrange for $1 \leq k \leq e$.
Then $|a^{p^{k-1}}| = p$. ☑

Sylow 2: 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 are conjugate.

Proof: 1. pick H as in Sylow 2. Then $(gHg^{-1}) \cap K$ Sylow p-subgroup in K
$\Rightarrow (gHg^{-1}) = K \Rightarrow K \leq gHg^{-1}$

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

Sylow 3: Let s = # of Sylow p-subgroups of G. Then $s \mid m$ and $s \equiv 1 \pmod p$

and Sylow p-subgroup is normal ⟺ $s_p = 1$

E.g. $|G| = 15 \Rightarrow G \cong C_{15}$ if G abelian.

$n = 15 = 3 \cdot 5$
$p = 3$ $m = 5$ $s \mid 5$ and $s \equiv 1 \pmod 3$
$\Rightarrow s = 1, 5$ $s \neq 5$ $s = 1$
$\Rightarrow$ Sylow 3-subgroup $H \trianglelefteq G$.
$p = 5$, $m = 3 \Rightarrow s \mid 3$ $s \equiv 1 \pmod 5$
$s = 1, 3$ $s \neq 1, s = 3$
$\Rightarrow$ Sylow 5-subgroup $K \trianglelefteq G$

HW2 #21 $\Rightarrow$ G abelian $\Rightarrow G \cong C_3 \times C_5 \cong C_{15}$

Semidirect product

Note: $k \in K \leq G$ and $H \trianglelefteq G$

$\Rightarrow khk^{-1} \in H$ if $h \in H$

$h \mapsto khk^{-1}$ is an automorphism $\varphi_k : H \to H$

Def: fix an automorphism $K \to \mathrm{Aut}\, H$, $k \mapsto \varphi_k$ (intuition)

The semidirect product of H and K is $H \rtimes K = (H \times K, \cdot)$ with $(h,k)\cdot(h',k') = (h\varphi_k(h'), kk')$

The point: $khk^{-1} = \varphi_k(h')$

$\Rightarrow hkh'k' = h\underbrace{kh'k^{-1}}_{\varphi_k}kk'$

Lemma $H \trianglelefteq H \rtimes K$ and $kHk^{-1} = \varphi_k(H)$ $\forall k \in K$, $h \in H$ ☑

Example: $|G| = 21$

$p=7, m=3 \Rightarrow s \mid 3$ $s \equiv 1 \pmod 7 \Rightarrow s = 1$

$\Rightarrow$ sylow 7-subgroup $H \trianglelefteq G$.

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

$\Rightarrow$ sylow 3-subgroups K either normal or not

$K \trianglelefteq G \Rightarrow G \cong C_{21}$

$K \not\trianglelefteq G \Rightarrow G$ not abelian but still $H \cap K = \{1\}$ by Lagrange

$\Rightarrow |HK| = \frac{|H||K|}{|H\cap K|} = |H||K| = 21$

$\Rightarrow G = HK$

$H \trianglelefteq G \Rightarrow G \cong H \rtimes K$ but for which $\varphi : K \to \mathrm{Aut}\, H$? $k \mapsto \varphi_k$

$\varphi_k : H \to H$, $h \mapsto khk^{-1}$ $\qquad (hk)(h'k') = (\underbrace{hkh'k^{-1}}_{\varphi_k})(kk')$

Lemma: $p \nmid \binom{n}{p^e}$ $\qquad n = p^e m$, $p \nmid m$

$\binom{n}{p^e} = \frac{n(n-1)\cdots(n-k)\cdots(n-p^e+1)}{p^e(p^e-1)\cdots(p^e-k)\cdots 1}$

$\mathrm{Aut}\, H \cong C_6$, $h \mapsto h^a$ $\Rightarrow \varphi_k : X \mapsto X^a$ for $X \in \{2, 4\}$ since $\varphi_k(1)^3 = 1^{a^3} = 1$, $2^3 = 7+1$, $4^3 = 63+1$

$\Rightarrow kHk^{-1} = H^2$ or H^4

Proof: Given $1 \leq k \leq p^e$ write $k = p^f \ell$ with $p \nmid \ell$. Then $n - k = p^e m - p^f \ell = p^f(p^{e-f} m - \ell)$

$p^e - k = p^e - p^f \ell = p^f(p^{e-f} - \ell)$

$\binom{n}{p^e} = \prod_{k=0}^{p^e-1} \frac{(n-k)}{(p^e-k)} = \prod \frac{p^f(p^{e-f}m - \ell)}{p^f(p^{e-f} - \ell)} = \prod \frac{p^{e-p}m - \ell}{p^{e-f} - \ell}$ but $p \nmid \{p^{e-f}m - \ell,\ p^{e-p} - \ell\}$ so $p \nmid \binom{n}{p^e}$

Sylow Theorem proofs

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

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

Proof: $G \curvearrowright \binom{G}{p^e}$ = union of orbits $\mathcal{O}$ (left mult)

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

$\binom{|G|}{p^e} \not\equiv 0 \pmod p \Rightarrow |\mathcal{O}| \not\equiv 0 \pmod p$ for some $\mathcal{O}$

Let $u \in \mathcal{O}$ (subset of G of card p^e). 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. on page 73 of notes

So $|G_u| = p^e$ so let $H = G_u$.

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

Proof: $G \curvearrowright X = G/H$ by left mult. $|X| = m = |G|/|H|$ ($\not\equiv 0 \pmod p$)

$\Rightarrow \exists$ K-orbit $\mathcal{O}$ with $p \nmid |\mathcal{O}|$. $x \in \mathcal{O} \Rightarrow x = gH$ for some $g \in G$

$G_x = gHg^{-1}$ $\quad g(gH) = agH \Leftrightarrow g^{-1}ag \in H \Leftrightarrow a \in gHg^{-1}$

$\Rightarrow K_x = (gHg^{-1}) \cap K$

$[K : (gHg^{-1}) \cap K] = [K : K_x] = |\mathcal{O}|$ coprime with p.
$|gHg^{-1}| = p^e \Rightarrow (gHg^{-1}) \cap K$ is a p-group!

$|K| / |(gHg^{-1}) \cap K|$ has no p

$|(gHg^{-1}) \cap K|$ has all p

$\Rightarrow (gHg^{-1}) \cap K \leq K$ is a Sylow p-subgroup of K.

Sylow 3: # Sylow p-subgroups of G ($= x$): divides m and $\equiv 1 \pmod p$

Proof: $G \curvearrowright X$ by conjugation $\rightarrow$ permutes them $\rightarrow$ acts transitively (cor. 2 of Sylow 2)

$\Rightarrow |X| = |G|/|N| = [G : N]$ for $N = N_G(H)$ where $H \in X$ is arbitrary

$[G:N]\,[N:H] = |N|/|H|$

$H \le N \Rightarrow [G:N] \mid [G:H] = m$ ✓

Now let $H \curvearrowright X$ again by conjugation.

Q: When does H stabilize $H' \in X$?

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

$\Leftrightarrow H \le N_G(H')$

But $H' \trianglelefteq N_G(H')$ by definition

H, H' is a normal Sylow p-subgroup of $N_G(H')$

$\Rightarrow H = H'$ by Cor 2 of Sylow 2

Conclusion: $H \curvearrowright X$ with only 1 orbit of size 1 and $p \mid |\mathcal{O}|$ for all other orbits $\mathcal{O} \neq \{H\} \Rightarrow |X| \equiv 1 \pmod p$ ▣

$|G| = 12$

- $H \le G$ Sylow 2-subgroup $|H| = 4$
- $K \le G$ Sylow 3-subgroup $|K| = 3$

Sylow 3 $\Rightarrow$ H has 1 or 3 conjugates

$\Rightarrow$ K has 1 or 4 conjugates

Lemma: $H \trianglelefteq G$ or $K \trianglelefteq G$ or both

Proof: $K \not\trianglelefteq G \Rightarrow 4$ conjugates

$\Rightarrow 8$ elements of order 3 in G

$\Rightarrow$ 4 elements remain $= H \trianglelefteq G$. ▣

Lemma $\Rightarrow G = H \times K$ if both $\trianglelefteq$.

$= H \rtimes K$ if $K \trianglelefteq G$

$= K \rtimes H$ if $H \trianglelefteq G$

Counting:

- $H \times K$: $G = C_4 \times C_3$ (5) or $G = C_2 \times C_2 \times C_3$ (4)

  ↑ element of order 4

- $H \rtimes K$: $G \overset{\text{conj}}{\curvearrowright} X = \{\text{conjugates of } K\}$

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

  Check ↪ (see lecture notes)

  3-cycles $\Rightarrow G = A_4$ (3)

  $(H = C_2 \times C_2)$

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

  Aut $K \cong C_2 = \{id_K, (y \mapsto y^2)\}$

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

  $\{1, x, x^2, x^3\}$

  $\Rightarrow G = \langle x, y \mid x^4 = 1,\ y^3 = 1,\ xyx^{-1} = y^2 \rangle$ (2)

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

  $H \twoheadrightarrow \text{Aut}\, K$ nontrivial $\Rightarrow \exists!$ $u \overset{\varphi}{\to} \text{id}_K$

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

  $C_2 \xrightarrow{\sim} \text{Aut}\, K$ $\quad G = (K \rtimes C_2) \times C_2'$

  $C_2' \to 1$. $\quad = S_3 \times C_2' \cong D_6$ (1)

Free Groups:

analog for "basis"

Theorem: Fix a set X. There is a free group $F(F_X)$ on X with the following universal property: for any group G, $\text{Maps}(X \to G) \leftrightarrow \text{Hom}(F, G)$.

Intuition: $F = \langle X \rangle$ no relations → we don't have to check relations.

Def: A word on X of length n is an element $w \in X^n$.

(e.g. $X = \{a, \dots, z\}$ w = aardvark)

$W = \bigcup_{n=0}^{\infty} X^n$ is the free semigroup (technically a monoid...) on X $\quad v \cdot w = vw$ ← concatenation

(e.g. aardvark · syzygy = aardvarksyzygy)

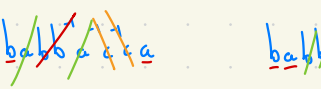
$X^{-1} = \{x^{-1} \mid x \in X\}$ $\quad X' = X^{-1} \cup X$ $\quad$ set $(x^{-1})^{-1} = x$ for $x^{-1} \in X^{-1}$

Def: The equiv. 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 $y \in X'$.

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

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

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

e.g. 

Proof: Induct on length $\ell(w)$.

$\ell(w) = 0 \Rightarrow w$ is empty $\Rightarrow$ reduced.

$\ell(w) > 0$. Assume $w \rightsquigarrow w_0 \neq w$ starts $w_1 x x^{-1} w_2$. Suffices to show $w \rightsquigarrow w_0' \Rightarrow w_1 w_2 \rightsquigarrow w_0'$

Since already $w_1 w_2 \rightsquigarrow w_0$ ($\ell(w_1 w_2) < \ell(w)$; induction hypothesis).

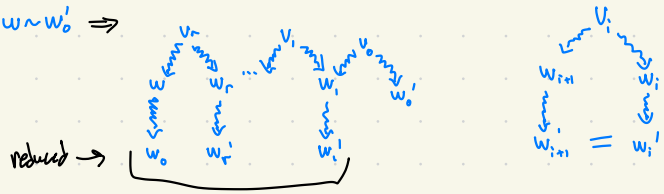
In w_0, x or x' must go.

- Both go simultaneously: may as well do them first. ✓
- One first: at $\dots x x^{-1} \dots$ but this leaves the string the same as if xx^{-1} had been cancelled first.

  or $\dots x x^{-1} x \dots = \dots x \dots = \dots x x^{-1} x \dots$

Cor: $w_0 \sim w$ for unique reduced w_0 and $w \rightsquigarrow w_0$.

Proof: $w \sim w_0' \Rightarrow$



So $w_0 = w_0'$.

Prop: $v \sim v'$ and $w \sim w' \Rightarrow vw \sim v'w'$ $\rightarrow$ $w \mapsto w'$ homomorphism

Proof: $vw \rightsquigarrow v_0 w \rightsquigarrow v_0 w_0 \rightsquigarrow (v_0 w_0)_0$

$v'w' \rightsquigarrow v_0 w' \rightsquigarrow v_0'' w_0$

Corollary: $F_X = W' / \underset{\text{congruence}}{\sim}$ is a group. ∎

E.g. $X = \{a\} \Rightarrow F_X \cong \mathbb{Z} \cong C_\infty$

Recall Thm: Fix a set X. There is a free group $F(F_X)$ on X with the following universal property: for any group G, $\text{Maps}(X \to G) \leftrightarrow \text{Hom}(F, G)$.

Proof: Given $f: X \to G$ and $w = x_1^{t_1} \cdots x_n^{t_n} \in W'$, define $\varphi: F_X \to G$ by $\varphi(w) = f(x_1)^{t_1} \cdots f(x_n)^{t_n}$

Then $w \sim w' \Rightarrow \varphi(w) = \varphi(w')$ because G is a group.

So φ is a homomorphism by construction. ∎

"F_X is the Grothendieck group of W"

Generators and Relations

Notes:

- Special case? $X \subseteq G$ generating set $\Leftrightarrow F_X \twoheadrightarrow G$
- $X \subseteq G \Rightarrow \text{im}(F_X \to G) = \langle X \rangle \leq G$

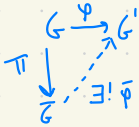
Def: If $\langle X \rangle = G$ then $\ker(F_X \twoheadrightarrow G) = N \trianglelefteq F_X$ consists of the relators on X.

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

Example: $S_3 = G \supseteq X = \{(1\ 2), (2\ 3)\}$
$\Rightarrow N = \{x^2, y^2, xyxy\ xy, xy^2x, xy^2x^{-1}, \dots\}$

Def: If $G = \langle X \rangle$ then $R \subseteq W'$ is a set of defining relations if $N = \ker(F_X \to G)$ is the smallest normal subgroup of F_X containing R. (Note R need not generate N)

Theorem (Universal property of quotient groups): Fix $N \trianglelefteq G$ and $\bar{G} = G/N$ with $\pi: G \to \bar{G}$, $a \mapsto aN$
$\varphi: G \to G'$ and $N \leq \ker\varphi \Rightarrow \exists!\ \bar{\varphi}: \bar{G} \to G'$ with $\bar{\varphi} = \varphi \circ \pi$



Proof: ex.

E.g.: $D_n = \langle x, y \mid x^n, y^2, xyxy \rangle$
Proof: x = rot $2\pi/n$, y = any reflection $\Rightarrow$

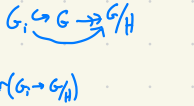
$\Rightarrow D_n = \langle x, y \rangle \Rightarrow F_{\{x,y\}} \twoheadrightarrow D_n$
$\ker\varphi \trianglelefteq F_{\{x,y\}}$, $\ker\varphi \geq R$ $\Rightarrow \ker\varphi \geq N = \bigcap_{R \subseteq K \trianglelefteq F_{\{x,y\}}} K$.
$\Rightarrow F_{\{x,y\}}/N \xrightarrow{\bar{\varphi}} D_n$.

Need: $\bar{\varphi}$ injective. Check by cardinality.
Ex: Using relations, every word in $x^{\pm1}$ and $y^{\pm1}$ can be put into the form $x^i y^j$ $i \in \{0, \dots, n-1\}$ $j \in \{0,1\}$, and there are $2n$ of these. ☑

Simplicity of A_n

Thm: A_n is simple if $n \geq 5$.
Proof: Induction on n. Base case is $A_5 \cong I$ is simple by corollary on last notes p.22
Assume $n \geq 6$. Let $H \trianglelefteq A_n$. Set $G_i = G_{A_n}(i)$ for $i = 1, \dots, n$ (stabilizer = even permutations which don't move i).

So $G_i \cong A_{n-1} \leq A_n$ simple for all i.
Let $1 \neq \pi \in H$ with $\pi(i) = i$ so $|H \cap G_i| \geq 1$
$\Rightarrow H \geq G_i$ since H normal in G $\Rightarrow$ $H \cap G_i$ normal in G_i



$(\sigma G_i \sigma)\sigma_i = \sigma G_i i = \sigma i$

Let $\sigma \in A_n \Rightarrow \sigma G_i \sigma^{-1} = G_{\sigma(i)}$

$\Rightarrow H \geq G_i$ for all i by same argument

Every $\rho \in A_n$ is a product of an even # of transpositions

= a product of some # of pairs of transpositions

has at most 4 letters in it $\Rightarrow \in G_i$ for some i as $n \geq 5$.

Hence $\langle G_1, \dots, G_n \rangle = A_n$ so $H = A_n$ (So if H contains a non-derangement, then H is just A_n)

So assume $\pi(i) \neq i$ for all $\pi \in H \setminus \{1\}$ and for all $i \in \{1, \dots, n\}$

Then if $\pi_1(i) = \pi_2(i)$ with $\pi_1, \pi_2 \in H$. $\pi_2^{-1}(\pi_1(i)) = i$, so $\pi_1 = \pi_2$ because otherwise $\pi_2^{-1}(\pi_1)$ wouldn't be a derangement.

So suppose $\pi \in A_n$ contains a ≥ 3-cycle $(a_1\ a_2\ a_3 \dots)$ in its cycle decomposition.

Fix $\sigma \in A_n$ with $\sigma(a_1) = a_1$ (possible since $n \geq 5$)

and $\sigma(a_2) = a_2$

but $\sigma(a_3) \neq a_3$

Then $\pi' = \sigma\pi\sigma^{-1}$ has the ≥ 3-cycle $(a_1\ a_2\ \sigma(a_3) \cdots)$

$\pi'(a_1) = \pi(a_1) = a_2 \Rightarrow \pi \in H$ or else we would have $\pi' \in H$ by normality $\Rightarrow \pi^{-1}\pi'(a_1) = a_1$

Now suppose $\pi = (a_1\ a_2)(a_3\ a_4)(a_5\ a_6) \cdots$ = product of disjoint transpositions

Set $\sigma = (a_1 a_2)(a_3 a_5) \in A_n$. Then $\pi' = \sigma\pi\sigma^{-1} = (a_2\ a_1)(a_5\ a_4)(a_3\ a_6)$

$\Rightarrow \pi, \pi' \notin H$

$\Rightarrow |H| = 1$ ☹

What's next?

Composition Series

Def: A composition series of G is a chain $\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{k-1} \trianglelefteq G_k = G$ "Filtration"

such that $G_i/G_{i-1} \xrightarrow{\sim} \overline{G_i}$ is simple $\forall i = 1, \dots, k$

G_i/G_{i-1}: composition factor; we couldn't insert a $G_i \trianglelefteq H \trianglelefteq G_{i+1}$ → "this chain is as fine as possible"

Jordan-Hölder Thm

multiset $\{\{\overline{G_i}\}\}$ is unique up to isomorphism & permutation

Examples: S_n: $1 \trianglelefteq A_n \trianglelefteq S_n$ $n \geq 5$

$\overline{G_1} = 1$

$\overline{G_2} = C_2$

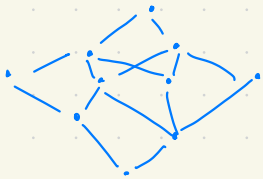
S_4: $1 \trianglelefteq C_2 \trianglelefteq V_4 \trianglelefteq A_4 \trianglelefteq S_4$

$\overline{G_i}$: C_2 C_2 C_3 C_2 — hence multiset

Def: A group G is solvable (from Galois theory) if $|\overline{G}_i|$ is prime for all i.

Eg S_4 but not S_n $n \geq 5$.

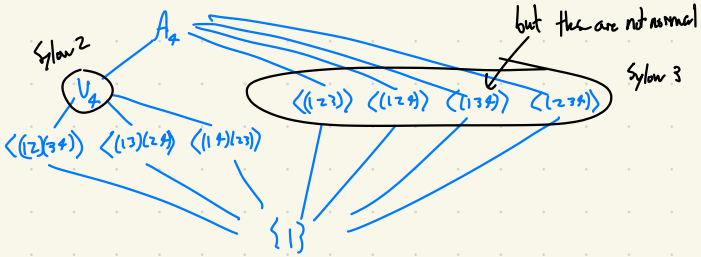
Poset example



Q: What do all composition series for G look like?

A: Subgroup lattice of G is

$\Lambda(G)$ = poset of all subgroups of G.



$N \trianglelefteq G \Rightarrow \Lambda(G/N) \subseteq \Lambda(G)$

$\Lambda(G/N) = \{\overline{H} \leq \overline{G} \mid N \leq H \leq G\}$ and $\overline{H} \trianglelefteq \overline{G} \Leftrightarrow H \trianglelefteq G$

Ex. $N \leq H \leq G$ with $N \trianglelefteq G$

$\Rightarrow G/H \hookrightarrow \overline{G}/\overline{H} = G/N \,/\, H/N$ (isomorphism)

$\cong$ if $H \trianglelefteq G$

(Anneaux in French)

Rings (math 501 part 2)

Def: A is a ring if it has:

$+ : A \times A \to A$ (addition)

$\cdot : A \times A \to A$ (multiplication)

With
- $(A, +)$ is an abelian group 0 is
- $(A, \cdot)$ is a monoid 1 is
- distributivity: $x(y+z) = xy + xz$

$(y+z)x = yx + zx$ $\forall x, y, z \in A$

What if $1 = 0$? Then $A = \{0\}$.

$0 = 0 + 0$

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

$\Rightarrow 0 = 0x$

$0 = 1 \Rightarrow 0x = 1x = x$ $\forall x \in A$

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

$1 + (-1) = 0$ by definition

$\Rightarrow 1x + (-1)x = 0x = 0$

$\Rightarrow x + (-1)x = 0$

$\Rightarrow -x$

Now we have $-x = (-1)x$

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

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

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

$(-x)(y + (-y)) = (-x)0 = 0$

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

Lemma: $v = w$.

Proof: $w = wuv = v$. ☐

$A^* =$ unit group of A

E.g. 1. $A = \underset{R}{\mathbb{k}}[x] = \left\{ \begin{matrix} \text{polynomials in } x \\ \text{with coeffs in } \mathbb{k} \end{matrix} \right\}$ $\mathbb{k}$ (viper) = "corpse" = field

$\Rightarrow A^* = \mathbb{k}^*$

$\supseteq R^*$ but maybe not $=$

2. $\mathbb{Z}^{\mathbb{N}} = \{(a_0, a_1, a_2, \dots)\}$

$R = \underset{\text{Ab}}{\text{Hom}}(\mathbb{Z}^{\mathbb{N}}, \mathbb{Z}^{\mathbb{N}})$ (hom of groups not rings) (linear maps of // free groups)

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

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

3. $A^* = A \setminus \{0\} \Rightarrow A$ is a division ring (or skew field) $\rightsquigarrow$ basically a field but not necessarily commutative.

Ex. quaternions $\mathbb{H} = \mathbb{R}[\{1, i, j, k\}] = \mathbb{R}[Q_8]$

If $xy = yx \ \forall x, y \in A$ then A is a field.

We say A is commutative (not abelian for... no reason...)

4. $\mathbb{Z}$ is a commutative [integral domain ("whole"/like the integers) "$\mathbb{Z}$ is entire"]

↳ $\Rightarrow ab = 0 \Rightarrow a = 0$ or $b = 0$

$(\mathbb{Z}, \cdot)^{\setminus\{0\}}$ is a cancellative monoid

IN $ab = ac \Rightarrow b = c$

$(\mathbb{R}, \cdot)$ $\Downarrow$ $a(b-c) = 0,\ a \neq 0 \Rightarrow b - c = 0 \Rightarrow b = c$

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, ring A $\Rightarrow R = A[G] = \left\{ \sum_{g \in G} a_g \cdot g \;\middle|\; \text{almost all } a_g \text{ are } 0 \right\}$ (finite a_g nonzero)

α

$A[\mathbb{N}] = A[x]$

and $b = \sum_{g \in G} b_g g \Rightarrow \alpha\beta = \sum_{g \in G} \sum_{h \in G} a_g b_h (gh)$ (convolution product)

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

7. function rings — look out notes

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

k field $\Rightarrow M_n(k)^* = GL_n(k)$

Is $M_n(R)$ commutative? Only if $n=1$ and R commutative.

Does it have zero divisors? $\begin{bmatrix} 0 & * \\ 0 & 0 \end{bmatrix}$ – yes unless $n=1$ and R is entire.

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

$(A,+) \to (B,+)$ group
$(A,\cdot) \to (B,\cdot)$ monoid homomorphism

a monoid homomorphism is a group homomorphism if your monoid happens to be a group.

Lemma: $\exists!$ ring hom $\mathbb{Z} \to A$ for any ring A.

Proof: $1 \mapsto 1$.

The kernel is $n\mathbb{Z}$. $n=p$ prime $\Rightarrow A$ has characteristic p
$\Rightarrow A \supseteq \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$

$n=0 \Rightarrow A$ has char 0
$\Rightarrow A \supseteq \mathbb{Z}$, injective

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

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

Ideals: What does the kernel $\ker(f: A \to B)$ look like?

Def $I < A$ is a left ideal in the ring A if $AI \subseteq I$
right ideal $IA \subseteq I$
two-sided ideal both.

E.g.
- any $A \Rightarrow I = \{0\}$ two-sided
- $\mathbb{Z} \supseteq n\mathbb{Z}$ two-sided
- $M_2(k) \supseteq \begin{bmatrix} 0 & * \\ 0 & * \end{bmatrix}$ left but not right ideal

Def: $a \in A \Rightarrow Aa$ $\quad \mathbb{Z} \to A$, $1 \mapsto 1$ $\Rightarrow Aa \leq A$ $\quad xa+ya=(x+y)a$, $a+a=2a$

Aa = principal left ideal

AaA = principal ideal

General: $Aa_1 + \cdots + Aa_n$ = left ideal generated by $a_1, \ldots, a_n$ $\approx$ linear combinations

$Aa_1A + \cdots + Aa_nA$ = ideal generated by $a_1, \ldots, a_n = \langle a_1, \ldots, a_n \rangle$

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

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

Proof: $f(a)=0 \Rightarrow f(bab') = f(b)f(a)f(b') = f(b) \cdot 0 \cdot f(b') = 0$

Theorem: $I \subseteq A$ is an ideal $\Leftrightarrow$ $\exists$ ring homomorphism $f: A \to B$ with $\ker f = I$

Proof: $\Leftarrow$ (prop)

$\Rightarrow$ $I \subseteq A$ ideal $\Rightarrow$ A/I is a ring with

$(x+I)(y+I) = xy+I$

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

Why? Because $xI + Iy + I^2 \subseteq I$ ☑

Theorem (Universal Property): $A \xrightarrow{\varphi} B$ ring hom. with ideal $I \subseteq \ker\varphi$

$\pi \downarrow$ $\nearrow \exists! \rho_*$ $\Rightarrow$ $\exists! \rho_* : A/I \to B$ with $\varphi = \rho_* \circ \pi$

A/I

"Any hom. that kills I might as well have been modded out by I that is, it factors through I"

Proof: True for $(A,+) \to (B,+)$. The claim: ρ_* is already a ring hom. ☑

Commutative rings

fix commutative ring R. $ab = ba$

Def: an ideal (with Frak $\mathfrak{p}$) $\mathfrak{P} \subseteq R$ is

- prime if $R/\mathfrak{P}$ is entire (an integral domain $\Rightarrow$ $x,y \neq 0 \Rightarrow xy \neq 0$) $\Leftrightarrow$ $(ab \in \mathfrak{P} \Leftrightarrow a \in \mathfrak{P}$ or $b \in \mathfrak{P})$
- maximal if $\mathfrak{P} \neq R$ and $I \supseteq \mathfrak{P} \Rightarrow I \in \{\mathfrak{P}, R\}$

Prop: R is a field $\iff$ $\{0\}$ is maximal.

Proof: ($\Rightarrow$) $x \notin \langle 0 \rangle \Rightarrow \langle x \rangle = R$.

($\Leftarrow$) $x \neq 0 \Rightarrow \langle x \rangle = R$ by maximality

$\Rightarrow 1 = xy$ for some $y \in R^*$

$\Rightarrow x \in R^*$ ☑

Cor: Maximal $\Rightarrow$ prime.

Proof: Every field is entire. ☑

R/I field $\Rightarrow R/I$ entire

E.g. $\mathbb{Z} \supset \underset{\text{max}}{\langle p \rangle} \supset \underset{\text{prime}}{\langle 0 \rangle}$

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

Proof: $b \in \langle a \rangle \Rightarrow b = xa$

$a \in \langle b \rangle \Rightarrow a = yb$

$= yxa$

$\Rightarrow a(1 - yx) = 0$

$\Rightarrow a = 0$ or $xy = 1$

$\Downarrow$

$b = 0$ ☑.

Chinese Remainder Theorem

Let R be a commutative ring.

Theorem: IF $I_1, \dots, I_n \subseteq R$ ideals with $I_i + I_j = R \ \forall i \neq j$

then $R \to R/I_1 \times \cdots \times R/I_n$ is surjective.

$x \mapsto (x + I_1, \dots, x + I_n)$

$x \mapsto (0, \dots, 0) \iff x \in I_1 \cap \cdots \cap I_n$

(Non) Example: $R = \mathbb{Z}$ $I_1 = 4\mathbb{Z}$ $I_2 = 6\mathbb{Z} \Rightarrow I_1 + I_2 = 2\mathbb{Z}$

$\mathbb{Z} \to C_4 \times C_6$

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

$0, 1, 2, 3$ $\quad$ $0, 1, 2, 3, 4, 5$

What maps to $(0,1)$?

x would have to be both odd and even. ✗

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

$\forall j \neq 1$

$I_1 + I_j = R \Rightarrow \exists\, a_j \in I_1$ with $a_j + b_j = 1$.
$b_j \in I_j$

Thus $\underbrace{(a_2 + b_2)\cdots(a_n + b_n)}_{\in I_1 + b_2 \cdots b_n} = 1$, so take $y_1 = b_2 \cdots b_n$

($b_2 \cdots b_n$: only term without $a_j \Rightarrow$ not in I_1)

and similarly for $i = 2, \dots, n$. ∎

$b_2 \cdots b_n = 1$ - something in I_1

$\equiv 1 \pmod{I_1}$

Corollary (Chinese Remainder Theorem)

IF $I_1, \dots, I_n$ are ideals in R with $I_i + I_j = R \; \forall i \neq j$ then given $x_1, \dots, x_n \in R \Rightarrow \exists x \in R$ with $x \equiv x_i \pmod{I_i} \; \forall i$. ∎

Eg $m_1, \dots, m_n \in \mathbb{Z}$ with $\gcd(m_i, m_j) = 1 \; \forall i \neq j$

In particular,

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

Then $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_n^{e_n}\mathbb{Z}$ FTFGAG!

$$\left|\left(\mathbb{Z}/m\mathbb{Z}\right)^*\right| \cong \left|\left(\mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_n^{e_n}\mathbb{Z}\right)^*\right|$$

$$\varphi(m) = \left|\left(\mathbb{Z}/p_1^{e_1}\mathbb{Z}\right)^* \times \cdots \times \left(\mathbb{Z}/p_n^{e_n}\mathbb{Z}\right)^*\right|$$

$$= \varphi(p_1^{e_1}) \times \cdots \times \varphi(p_n^{e_n})$$

$$= (p_1 - 1)p_1^{e_1 - 1} \cdots (p_n - 1)p_n^{e_n - 1}$$

Principle Ideal Domains & Unique Factorization Domains (PIDs & UFDs)

Fix R commutative integral domain.

Def: an element $a \in R$ is irreducible if

$a = bc \Rightarrow b \in R^*$ or $c \in R^*$.

$\langle a \rangle = \langle c \rangle$ $\quad \langle a \rangle = \langle b \rangle$

Lemma: $\langle p \rangle$ prime $\Leftrightarrow$ p irreducible (R_p)

Proof: $p = ab \Rightarrow a \in \langle p \rangle$ or $b \in \langle p \rangle$
Since $\langle p \rangle$ is prime. WLOG, say $a \in \langle p \rangle$.
Then $a = pc$, so $p = ab = pcb \Rightarrow cb = 1$. (integral domain $\Rightarrow$ cancellative)

Def: $a \mid b$ if $ac = b$ for some $c \in R$.
$\Leftrightarrow b \in (a)$.

Def: $d \in R \setminus \{0\}$ is a gcd if
- $d \mid a$ and $d \mid b$
- if $c \mid a$ and $c \mid b$ then $c \mid d$

Def: R is a PID if every ideal is principal.

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

Proof: Let $d = \alpha a + \beta b$ and suppose that $a = ex$ and $b = ey$.
Then $d = \alpha ex + \beta ey = e(\alpha x + \beta y) \Rightarrow e \mid d$. ☑

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

Proof: $p \mid ab$ and $p \nmid a \Rightarrow \langle p, a \rangle = \langle d \rangle \supsetneq \langle p \rangle$
$\Rightarrow p = cd$ but $c \in R^* \Rightarrow d \in R^*$ since p irreducible
$\Rightarrow 1 = xp + ya \Rightarrow b = xpb + y\frac{ab}{p} \Rightarrow p \mid b$ ☑.

PID $\Rightarrow$ UfD for R a commutative integral domain

Def: R is factorial (or a UFD = unique factorization domain) ($a = bc \Rightarrow b \in R^*$ or $c \in R^*$)
if every $r \in R \setminus \{0\}$ factors uniquely into irreducibles
meaning $r = u \cdot p_1 \cdots p_k = v q_1 \cdots q_\ell$ with $u, v \in R^*$
$\Rightarrow k = \ell$ and $q_i = u_i p_i$ with $u_i \in R^*$ after permuting the q_i.

Theorem PID $\Rightarrow$ UFD

Proof: Claim: Every $r \in R$ factors into irreducibles
Proof: Let $S = \{(r) \subseteq R \mid r \text{ doesn't factor}\}$
Assume $S \neq \emptyset$. Then S has a maximal element $\langle r \rangle$ by Zorn's Lemma because
because
- every chain $\langle r_1 \rangle \subseteq \langle r_2 \rangle \subseteq \cdots$
yields an ideal $\langle r_1 \rangle \cup \langle r_2 \rangle \cup \cdots = \langle b \rangle \Rightarrow \langle b \rangle \subseteq \langle r_n \rangle \subseteq \langle b \rangle \Rightarrow \langle b \rangle = \langle r_n \rangle \in S$ is an upper bound

Note r is reducible since $\langle r\rangle \in S$

(r irreducible $\Rightarrow r=1\cdot s$ is factorization and $\langle r\rangle \in S \Rightarrow r$ doesn't factor)

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 $\langle c\rangle, \langle d\rangle \notin S \Rightarrow c,d$ have factorizations and hence so does r ↯

Thus $S=\emptyset$. ∎

Now let $r=up_1\cdots p_k = vq_1\cdots q_\ell \Rightarrow p_k$ prime by Lem (irreducible $\Leftrightarrow$ prime in PID)

$\Rightarrow p_k \mid q_i$ for some i. Assume $i=\ell$ by permutation.

$\Rightarrow p_k = u_k q_\ell$ with $u_k \in R^*$ since q_i is irreducible.

$\Rightarrow up_1\cdots p_{k-1} = (vu_k)q_1\cdots q_{\ell-1}$ (because PID $\Rightarrow$ cancellative)

Done by induction ∎

E.g.

- $R=\mathbb{Z}$ every subgroup is cyclic } by Euclid's algorithm
- $R=\mathbb{k}[x]$ "field"

Thm: R factorial $\Rightarrow R[x]$ is too.

$\Rightarrow \mathbb{k}[x_1,\dots,x_n]$ is UFD

- $\mathbb{k}[[x]]$ formal power series is a UFD
- $\mathbb{C}\{\{x\}\}$ convergent series is a UFD
- $\mathbb{k}[x^2,x^3]$ not UFD MCNUGGET PROBLEM
  $\mathbb{k}[\mathbb{N}\setminus\{1\}]$
  $\mathbb{Z}[\sqrt{-5}] = \{a+b\sqrt{-5} \mid a,b\in\mathbb{Z}\}$ not a UFD.

Localization

Fix a commutative ring R

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

- $1\in S$
- $xy\in S$ for all $x,y\in S$

The ring of fractions is $S^{-1}R = R[S^{-1}] = R\times S/\sim$ (if R entire & $0\notin S$, we don't need this)

where the class of (a,s) is denoted $\frac{a}{s}=\frac{a'}{s'}$ $\exists\, t\in S$ with $t(s'a-sa')=0$

Eg. $0 \in S \Rightarrow S^{-1}R = \{0\}$

Check equivalence relation $\sim$

- reflexive $sa - sa = 0$ ✓
- symmetric (by commutativity) ✓
- transitive $\frac{a}{s} = \frac{a'}{s'} = \frac{a''}{s''} \Rightarrow \frac{a}{s} = \frac{a''}{s''}$

$\frac{a}{s} = \frac{a'}{s'} \Rightarrow s't(s'a - sa') = 0 = -st'(sa' - s'a'')$

$\Rightarrow s''t's'a = sts'a''$

$\Rightarrow \underbrace{t't s'}_{\in S}(s''a - sa'') = 0$ ✓

□

Proposition $R[S^{-1}]$ is a ring with ← a localization of R

$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$

$\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}$.

Proof: e.g. $\frac{a}{s} = \frac{a'}{s'} \Rightarrow u(s'a - sa') = 0$

$\Rightarrow u(s'tab - a'bst) = 0$

$\Rightarrow \frac{ab}{st} = \frac{a'b}{s't}$

Cor: $R \to S^{-1}R$

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

Q: $R = \mathbb{R}[x,y]/(xy)$ $\quad S = \{1, x, x^2, \dots\}$ (N)

$\Rightarrow \ker\left(R \to \underbrace{R[x^{-1}]}_{R_x}\right) = ?$

Eg. 1. $S = R^* \Rightarrow S^{-1}R = R$.

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

$\Rightarrow S^{-1}R = K(R)$ = fraction field of R

(not $R/_m$ = quotient field)

E.G. $K(\mathbb{Z}) = \mathbb{Q}$

$K(\mathbb{R}[x_1, \dots, x_n]) =$ rational function $= \mathbb{R}(x_1, \dots, x_n)$

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

0 multi subset $\Leftrightarrow \mathfrak{p}$ prime

$\Rightarrow S^{-1}R = R_{\mathfrak{p}}$ = localization of R at $\mathfrak{p}$

#2: $\mathfrak{p} = 0$.

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

4. $S = \{1, t, t^2, \dots\} \Rightarrow S^{-1}R \overset{\text{def}}{=} R_t$

Recall

$\ker(R \to R_t) = ?$

$\frac{a}{1} = \frac{0}{1} \iff ua = 0$ for some $u \in S$

$\iff t^d a = 0$ for some $d \in \mathbb{N}$

$R = \mathbb{R}[x,y]/\langle xy \rangle$

Basis for $\mathbb{R}[x,y]$ = all monic monomials in x, y.

Modding out by $\langle xy \rangle$ sets everything with an xy to 0

So $\mathbb{R}[x,y]/\langle xy \rangle = \mathbb{R}\{1, \bar{x}, \bar{x}^2, \dots, \bar{y}, \bar{y}^2, \dots\}$

$x^d f(x,y) \in \langle xy \rangle$ for some $d \in \mathbb{N}$

$\iff xy \mid x^d f(x,y)$

$\iff y \mid f(x,y)$

So $\ker(R \to R_x) = \langle y \rangle$

Prop Let $\mathcal{C}$ = category of ring homs.

$R \xrightarrow{f} A$ such that $f(s) \in A^\times \; \forall s \in S$

morphism → $\begin{array}{ccc} R & = & R \\ \downarrow & & \downarrow \\ R & \to & A \end{array}$

Then $R \to S^{-1}R$ is universal (universally repellent) in $\mathcal{C}$

$\begin{array}{ccc} & & S^{-1}R \\ & \nearrow & \downarrow \exists! f_* \\ R & \xrightarrow{f} & A \end{array}$ $\qquad$ $\begin{array}{ccc} R & \to & S^{-1}R \\ \| & & \downarrow \uparrow \mathbb{R} \\ R & \to & U \end{array}$

Proof: Look at notes.

Corollary $R[(R^\times)^{-1}] = R$.

Proof: Every homomorphism $R \to A$ factors through $R \xrightarrow{\mathrm{id}} R$ so $R \xrightarrow{\mathrm{id}} R$ satisfies the universal property. ☒

Euclidean Domains "Elementary"

fix commutative ring R.

Def: a norm on R is a function $R \to \mathbb{N}$ with $0 \mapsto 0$.
A norm N is positive if $N(a) > 0 \ \forall a \neq 0$.

A domain R is Euclidean if there exists a norm $N: R \to \mathbb{N}$ such that $a, b \in R$ with $b \neq 0$.

$\Rightarrow \exists\, q, r \in R$
(quotient, remainder)
satisfying
$a = qb + r$ with $r = 0$ or $N(r) < N(b)$

E.g. • $\mathbb{K}$ = field N = anything-ish!
• $R = \mathbb{Z}$, $N = |\cdot|$

Theorem: $R = \mathbb{K}[x]$ is Euclidean (if $\mathbb{K}$ field) with $N = \deg$.
Moreover, q, r unique.

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

$\deg a = n \geq 1$: use induction.

field $\subsetneq$ Euclidean $\subsetneq$ PID $\subsetneq$ UFD $\subsetneq$ domain $\subsetneq$ commutative $\subsetneq$ ring.

Let $a = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ with $a_n \neq 0 \neq b_m$.
$b = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_0$

Case: $m > n$: $q = 0$ and $r = a$ ✓
Case: $m \leq n$: set $a' = a - \frac{a_n}{b_m} x^{n-m} b$
then $\deg a' < n$ so $a' = q'b + r$ by induction hypothesis
with $r = 0$ or $\deg r < m$
set $q = q' + \frac{a_n}{b_m} x^{n-m}$. Then $qb + r = \left(q' + \frac{a_n}{b_m} x^{n-m}\right) b + r$

$= \left(q'b + \frac{a_n}{b_m} x^{n-m} b + r\right)$ a'
$= a - \frac{a_n}{b_m} x^{n-m} b + \frac{a_n}{b_m} x^{n-m} b$
$= a$.

Consider $a = \hat{q}b + \hat{r} \Rightarrow (\hat{q}-q)b = r - \hat{r}$ has degree $< m$.
$= qb + r$

$(\hat{q}-q)b$ has degree $\deg(\hat{q}-q) + m$
if $\hat{q}-q \neq 0$. But this contradicts equality above so
$\hat{q}-q = 0 = \hat{r}-r$.

Lemma: R euclidean $\Rightarrow$ PID
and $(0) \neq I \leq R$ ideal $\Rightarrow I = (d)$ for any $d \neq 0$ of minimal norm.

Proof: fix such $d \in I$.
$a \in I \Rightarrow a = qd + r$ with $r = a - qd \in I$.
$N(r) < N(d) \Rightarrow r = 0$. ∎

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

Q: Is $\mathbb{k}[x,y]$?

A: Nope.

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

Proof: $a \in \langle p \rangle \Rightarrow \langle a, p \rangle = d$ for some $d = \gcd(a,p)$.
But $p \nmid d$ since $a \notin \langle p \rangle$.
$\mathcal{U}$ $\Rightarrow d \in R^\times$. ∎

Why? If $R[y]$ PID then R field
because $R[y]/\langle y \rangle \cong R$ is a domain $\Rightarrow \langle y \rangle$ prime!
$\Rightarrow \langle y \rangle$ maximal (b/c R PID)
$\Rightarrow R$ field.

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

Euclidean Algorithm

Input: $a, b \in R$, $b \neq 0$
Output: $\gcd(a,b)$

Init: q_0, r_0 with $a = q_0 b + r_0$ (0)
q_1, r_1 $b = q_1 r_0 + r_1$ (1)
$i = 1$ $r_0 = q_2 r_1 + r_2$ (2)

While: $r_i \neq 0$
Do: write $r_{i-1} = q_{i+1} r_i + r_{i+1}$
$i \leftarrow i+1$

Return: r_{i-1} (call it r_n)

Ending:
$r_{n-3} = q_{n-1} r_{n-2} + r_{n-1}$ $(n-1)$
$r_{n-2} = q_n r_{n-1} + r_n$ (n)
$r_{n-1} = q_{n+1} r_n$ $(n+1)$

Example: $\overset{a}{168} = 3 \cdot \overset{b}{30} + 18$

$30 = 1 \cdot 18 + 12$

$18 = 1 \cdot 12 + 6$

$12 = 2 \cdot 6$

Thm: $\langle a, b \rangle = \langle r_n \rangle$

Proof: $(0) \Rightarrow r_0 \in \langle a, b \rangle$

$(1) \Rightarrow r_1 \in \langle b, r_0 \rangle \subseteq \langle a, b \rangle$

$(i) \Rightarrow r_i \in \langle r_{i-2}, r_{i-1} \rangle \subseteq \langle a, b \rangle$ by induction.

$(n+1) \Rightarrow r_n \mid r_{n-1}$.

$(n) \Rightarrow r_n \mid r_{n-2}$

$(i) \Rightarrow r_n \mid r_{i-2}$ $i \geq 2$ by induction on $n-i$.

$(1) \Rightarrow r_n \mid b$
$(0) \Rightarrow r_n \mid a$
$\Rightarrow \langle r_n \rangle = \langle a, b \rangle$ ∎

Modules

Fix a ring A.

Def: M is a left module over A ($/A$) or a left A-module if M is

- an abelian group with monoid action
- a left action of $(A, \cdot)$ that is distributive:
  - $(x+y)m = xm + ym$ $\forall x, y \in A$
  - $x(m+n) = xm + xn$ $m, n \in M$

Eg. $A = \overset{\text{field}}{\mathbb{K}}$, M = vector space

Ex: $-m = (-1) \cdot m$

$x(-m) = -(xm)$

$0m = 0$

$\vdots$

Action: $(x, m) \mapsto xm$

$(y, xm) \overset{\text{left}}{\mapsto} yxm$

$\overset{\text{right}}{\mapsto} xym$

Assume "module" = left module

right module is analogous

bi-module is left & right

Def $N \overset{\text{subgroup}}{\subseteq} M$ submodule if $AN \subseteq N$.

E.g.
- $I \subseteq A$ left ideal $\iff$ submodule
- A is a free A-module with basis $1 \in A$.
- A/I cyclic A-module generated by $\bar{1} \in A/I$. (I left ideal) (I 2-sided $\Rightarrow$ quotient ring; I 1-sided $\Rightarrow$ quotient module)
  $a \cdot \bar{I} = \overline{a(1)}$
- $\mathbb{Z}$-module = abelian group ;;
- V = vector space/$\mathbb{K}$ and $T: V \to V$ linear
  $\Rightarrow$ V is a $\mathbb{K}[x]$-module via $x \cdot v = Tv$
  $f(x) \cdot v = f(T)v$
- $A = R^{n\times n}$ = $n\times n$ matrices/R $\Rightarrow$ $R^n = \left\{ \begin{bmatrix} * \\ \vdots \\ * \end{bmatrix} \right\}$ left A-module
  $\cong$ left ideal $\subseteq A$.
  $\left\{ \begin{bmatrix} 0 & * & \cdots & * \\ \vdots & \vdots & & \vdots \\ 0 & * & \cdots & * \end{bmatrix} \right\} \subseteq A$ analogous w/ rows for right ideal.
- Set S, (left) A-module M.
  $\Rightarrow$ maps$(S \to M)$ 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 $m \in M \Rightarrow$
$m = \sum_{\lambda \in \Lambda} x_\lambda m_\lambda$ ← linear combination for $\{x_\lambda \mid \lambda \in \Lambda\}$ almost all 0. (finite number)

E.g. $\mathbb{Z}\times\mathbb{Z}$ (lattice points in the plane) is generated by $\left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}$
or by $\left\{ \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}$. But $\left\{ \begin{bmatrix} 3 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}$ generates $2\mathbb{Z}\times\mathbb{Z} \subsetneq \mathbb{Z}\times\mathbb{Z}$
$\det \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = 1 \in \mathbb{Z}^*$ $\det \begin{bmatrix} 3 & 0 \\ 0 & 1 \end{bmatrix} = 2 \notin \mathbb{Z}^*$

Lemma: $N \subseteq M$ submodule
$\Rightarrow$ group M/N naturally a module.

Proof: $xm \equiv xm' \pmod N$ if $m - m' \in N$ because $x(m-m') = xm - xm' \in N$. ☐

E.g. $\mathbb{Z}\times\mathbb{Z} \xleftarrow{\begin{bmatrix} 3 \\ 6 \end{bmatrix}} \mathbb{Z}$ has image $N \cong \mathbb{Z}$
$N = \left\langle \begin{bmatrix} 3 \\ 6 \end{bmatrix} \right\rangle$ $M/N \cong \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}$ (choose generating set as $\left\{ \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}$)

Def: fix R a commutative domain. Then the torsion submodule of M is $M_{tor} = \{m \in M \mid rm = 0 \text{ some } r \in R \setminus \{0\}\}$
E.g. $(M/N)_{tor} = \mathbb{Z}/3\mathbb{Z} \times 0$.

Def: $I \subseteq A$ left ideal $\Rightarrow IM = \{$linear combinations of elements of M with coefficients in $I\}$

Ex. $IM \subseteq M$ submodule.

$(IJ)M = I(JM)$

$(I+J)M = IM + JM$.

Def: $\varphi: M \to M'$ is a module homomorphism

if φ is a group hom $(M,+) \to (M',+)$ with

$\varphi(xm) = x\varphi(m)$ $\forall x \in A$ and $m \in M$. φ is A-linear.

Note: A-mod is a category:

objects M

morphisms $\varphi: M \to M'$ (A-linear)

With:

- $1_M: M \to M$ identity
- $\varphi: M \to M'$ and $\gamma: M' \to M''$
  $\Rightarrow \gamma \circ \varphi: M \to M''$
  - Associative
  - $1_M \circ \varphi = \varphi = \varphi \circ 1_{M'}$

For fun:

A-mod has initial object 0. $0 \to M$ $\forall M$.

terminal object 0. $M \to 0$ $\forall M$.

free modules

fix ring $A \neq 0$, M a left A-module.

Def. M is free if it has a generating linearly independent subset (basis)

S any set $\rightsquigarrow$ free module with basis S is $\bigoplus_{s \in S} A \overset{\text{def}}{=} A^{\oplus S} \cong$ finitely supported functions $S \to A$ (all but finitely many elements go to 0)

E.g. $A = k$ field. (B/c all vector spaces have a basis)

M = vector space.

$A = \mathbb{Z}$ M = free abelian group $\mathbb{Z}^{\oplus s}$

Theorem: $\{x_\lambda\}_{\lambda \in \Lambda}$ basis of M and

$\{y_\lambda\}_{\lambda \in \Lambda}$ any elements of N.

$\Rightarrow \exists!$ homomorphism $\varphi: M \to N$ with $\varphi(x_\lambda) = y_\lambda \quad \forall \lambda \in \Lambda$

Proof: Unique because $\{x_\lambda\}$ generates M.

Exists because $M = \bigoplus_\lambda A x_\lambda$ and $A x_\lambda \cong A$.

universal prop of $\oplus \Rightarrow \exists$ ☑

Def: for a module M a (free) presentation is a morphism

$F_1 \to F_0$

With cokernel $F_0 \twoheadrightarrow M$ (with both F_i free).

$F_0 / \mathrm{im}(F_1 \to F_0)$

$F_0 \twoheadrightarrow M$ has kernel K ("subgroup of relations") (syzygy module)

basis ⟶ generating set

$$0 \to K \to F_0 \to M \to 0$$

$F_1 \twoheadrightarrow K$.

Eg. $\mathbb{Z} \oplus \mathbb{Z} \xrightarrow{\begin{bmatrix} 0 & 0 \\ 0 & 2 \end{bmatrix}} \mathbb{Z} \oplus \mathbb{Z}$ presentation of $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

$(1,0) \longmapsto (0,0)$

$(0,1) \longmapsto (0,2)$

E.g. $T: V \to V$ vector space/$\mathbb{K}$ dim = d.

$\Rightarrow V$ is a $\mathbb{K}[t]$-module.

$t: V \to V$ is $T: V \to V$

$V = \langle v \rangle$ cyclic

$\iff V = \mathrm{span}_{\mathbb{K}} \{v, Tv, \ldots, T^{d-1}v\}$

$\iff \mathbb{K}[t] \twoheadrightarrow V$ $\quad \ker = \langle \text{min. polynomial of } T \rangle$ $\quad m_p(t)$

$1 \mapsto v$

$t \mapsto tv = Tv$

$t^2 \mapsto t^2 v = T^2 v$

$\vdots$

Want $p(t)$ so that $p(T) = 0$.

$\iff \mathbb{K}[t] \xrightarrow{m_p(t)} \mathbb{K}[t]$ is a presentation of V.

A ring, M A-module

$M = \langle x \rangle$ cyclic $\iff A \twoheadrightarrow M$

$1 \mapsto x$

$A = R =$ PID $\Rightarrow \ker$ is (a)

Q. IF $m_p(t) = (t-\alpha)^d$, what is V?

A. a Jordan block!

↑ understand this by next lecture!

Def: An exact sequence

$0 \to K \xrightarrow{\varphi} M \xrightarrow{\psi} N \to 0$

Splits if it has a section σ

Satisfying $\psi\sigma = id_N$.

Note: sequence short exact $\Rightarrow$

$M = K + \sigma(N)$ by Midterm 2 #5

but $K \cap \sigma(N) = 0$ since $\sigma(N) \hookrightarrow N$.

Then $\iff M = K \oplus \sigma(N)$.

$M \cong K \oplus N$

↑ not equal

Corollary: N free $\Rightarrow$ sequence splits.

Proof: If $\{x_\lambda\}_{\lambda \in \Lambda}$ in M maps to a basis $\{y_\lambda\}_{\lambda \in \Lambda}$ of N, then use Thm to construct $\sigma : y_\lambda \to x_\lambda \ \forall \lambda \in \Lambda$. ☐

Free Modules over a PID

Def: The rank of a free module F over a nonzero commutative ring is $\operatorname{rank} F := |\text{basis of } F|$ (analogous to dimension)

Lemma: doesn't depend on the basis

Proof: Suppose $F \cong \bigoplus_{s \in S} R$.
Let $\mathfrak{p} \subseteq R$ be maximal.
Then $F/\mathfrak{p}F \cong \bigoplus_{s \in S} R/\mathfrak{p}$ is a vector space over $R/\mathfrak{p}$ of dimension $|S|$.

Thm: Fix F free over PID R and a submodule $M \subseteq F$. Then M is free of rank $\leq \operatorname{rank} F$.

(non) **Ex.** $R = \mathbb{K}[x,y] \supseteq \langle x, y \rangle$

Proof: $F = \bigoplus_{\lambda \in \Lambda} R x_\lambda$ for a basis $\{x_\lambda\}_{\lambda \in \Lambda}$.
$J \subseteq \Lambda \Rightarrow M_J \overset{\text{def}}{=} M \cap \bigoplus_{j \in J} R x_j$.
(*)
and $M_J = \bigoplus_{j \in J} R y_j$ for some $y_j \in M_J$ 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:

$$\{y_j\}_{j \in J} \subseteq \{y'_j\}_{j \in J'} \text{ if } J \subseteq J' \text{ and } y_j = y'_j \ \forall j \in J.$$

WARNING: some y_i can be 0.

If $\mathcal{C}$ is a chain in Y then

$\bigcup_{C \in \mathcal{C}} C \in Y$ since any dependence relation involves only finitely many of the y_j's.

Hence $\exists$ a family $\{y_j\}_{j\in J}$ maximal in Y

Want $J=\Lambda$. Suffices: $k\in\Lambda\setminus J \Rightarrow \leftarrow$

Let $K=J\cup\{k\}$ and $M\hookrightarrow F\xrightarrow{\pi_k} Rx_k\subseteq R$.

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 $\langle a\rangle x_k$

$0\to M_J\to M_K\to \pi_k(M_K)\to 0$

is exact. It splits because $\langle a\rangle x_k$ is free!

Thus $\{y_j\}_{j\in K}\in Y$ if $y_k=a(ax_k)$

$M_K\cong M_J\oplus\langle a\rangle x_k$.

So $J=\Lambda$ ∎.

Structure Theorem for modules over PID R

fix finitely generated M over PID R. Then $\exists!$ proper ideals $\langle q_1\rangle\subseteq\cdots\subseteq\langle q_\ell\rangle$ with $M\cong R/\langle q_1\rangle\oplus\cdots\oplus R/\langle q_\ell\rangle$

invariants of R

E.g. $R=\mathbb{Z}\Rightarrow M\cong \underbrace{\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}}_{\text{rank}}\oplus \mathbb{Z}/n_1\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/n_k\mathbb{Z}$

With $n_k\mid\cdots\mid 1$

$\mathbb{Z}/n_1\mathbb{Z}=\bigoplus_p \mathbb{Z}/p^{e_1(p)}\mathbb{Z}$ $\quad$ $\mathbb{Z}/n_k\mathbb{Z}=\bigoplus_p \mathbb{Z}/p^{e_k(p)}\mathbb{Z}$

$e_1(p)\geq\cdots\geq e_k(p)$ $\forall p$ all 0 for almost all p.

E.g. $\mathbb{Z}^3\oplus$ (Sylow 2: $\mathbb{Z}/32\mathbb{Z}\oplus\mathbb{Z}/32\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$; Sylow 3: $\mathbb{Z}/81\mathbb{Z}\oplus\mathbb{Z}/27\mathbb{Z}\oplus\mathbb{Z}/3\mathbb{Z}$; Sylow 5: $\mathbb{Z}/125\mathbb{Z}\oplus\mathbb{Z}/25\mathbb{Z}\oplus\mathbb{Z}/5\mathbb{Z}$)

CRT

$\mathbb{Z}/162000\mathbb{Z}^\times\times\mathbb{Z}/1800\mathbb{Z}^\times\times\mathbb{Z}/20\mathbb{Z}^\times\times\mathbb{Z}/10\mathbb{Z}^\times\times\mathbb{Z}/2\mathbb{Z}^\times\times\mathbb{Z}/2\mathbb{Z}^\times$

$q_1\ q_2\ q_3$ $\quad$ q_4 $\quad$ q_5 $\quad$ q_6 $\quad$ q_7 $\quad$ q_8 $\quad$ q_9

Eg. $R = \mathbb{K}[x] \Rightarrow$ module V is a vector space over $\mathbb{K}$ with $x \cdot v = Tv$ for some $T: V \to V$.

Thm $\Rightarrow V \cong \mathbb{K}[x]^{\lceil} \oplus (\dim < \infty)$ (easy, so assume $\dim V < \infty$)

Thm $\Rightarrow V \cong \bigoplus_p \mathbb{K}[x]/\langle p^{e_1(p)} \rangle \oplus \cdots \oplus \bigoplus_p \mathbb{K}[x]/\langle p^{e_k(p)} \rangle$

$e_1(p) \geq \cdots \geq e_k(p)$ for all primes p and almost all $e_i(p) = 0$.

Q. What is $\{p\}$?

A. Irreducible polynomials (up to scalars $\mathbb{K}^*$)

Q. What if $\mathbb{K} = \mathbb{C}$?

A. $x - \alpha$ for some $\alpha \in \mathbb{C}$

Q. What is $\mathbb{K}[x]/\langle (x-\alpha)^e \rangle$?

A. Cyclic with minimal polynomial $(x-\alpha)^e$
= Jordan block of size e for eigenvalue α. (cf. Lec 23)

$R = \mathbb{K}[x] \Rightarrow$ thm is Jordan form.

Thm fix a f.g. nonzero module M / PID R (nonzero).
$\exists!$ proper ideals $\langle q_1 \rangle \subseteq \cdots \subseteq \langle q_n \rangle$ with

$$M \cong R/\langle q_1 \rangle \oplus \cdots \oplus R/\langle q_n \rangle$$

Def $\operatorname{Rank} M = \#\{i \mid q_i = 0\}$

Proof overview

(Recall if M module / commutative domain R has torsion submodule

$$M_{tor} = \{m \in M \mid rm = 0 \text{ for some } r \in R \setminus \{0\}\}$$

$M = M_{tor}$: "M is torsion")

fix M finitely generated / PID R.

Prop 1: $M = M_{tor} \oplus F$ with F free. Then $\operatorname{rank} M \overset{\text{def}}{=} \operatorname{rank} F < \infty$ well defined.

Prop 2: If $M = M_{tor}$, then $M = \bigoplus_p M(p)$ where

p: set of prime elements such that $\langle p \rangle$ are the prime ideals

- $p^e M(p) = 0$ for some $e \in \mathbb{N}$
- $M(p) = 0$ for almost all p $\Rightarrow$ finite direct sum

$M(p) = \{m \in M \mid p^e m = 0 \text{ for } e \gg 0\}$ analog of Sylow p-subgroup

Prop 3: $M = M(p) \Rightarrow M \cong R/\langle p^{e_1} \rangle \oplus \cdots \oplus R/\langle p^{e_n} \rangle$

$\exists$: Props $\Rightarrow M \cong R^\ell \oplus \bigoplus_{p}^{\text{finite}} \left(R/\langle p^{e_{\ell+1}(p)} \rangle \oplus \cdots \oplus R/\langle p^{e_{\ell+k}(p)} \rangle \right)$

with $e_{\ell+1}(p) \geq \cdots \geq e_{\ell+k}(p)$

Set $q_1 = \cdots = q_\ell = 0$ and

$q_i = \prod_p p^{e_i(p)}$ for $i > \ell$ where $e_i(p) = 0$ for $i > \ell + k$

Then

- $\cdots \mid q_n \mid q_{n-1} \mid \cdots \mid q_2 \mid q_1$ for all n by construction

so $\langle q_1 \rangle \subseteq \langle q_2 \rangle \subseteq \cdots \subseteq \langle q_n \rangle \subseteq \cdots$

Take $n = \max_{e_i(p) \neq 0} i$.

and • $\bigoplus_p R/\langle p^{e_i(p)} \rangle \cong R/\langle q_i \rangle$ by Chinese remainder theorem. ✓

!: $\#\{i \mid q_i = 0\} = \operatorname{rank} M$.

Henceforth assume $M = M_{tor}$. Suppose $q_1, \ldots, q_n$ satisfy thm.

Uniqueness is trivial when $q_1 \cdots q_n = p$ is prime:

$n = 1$ and $q_1 = p$

If $M = R/\langle q_1 \rangle \oplus \cdots \oplus R/\langle q_n \rangle$ with $q_1, \ldots, q_n = pa$ with $a \notin R^\times$ then $R \to R/\langle p \rangle \subset M$

$\#\{i \mid p \mid q_i\} = \dim_{R/\langle p \rangle} M/pM$.

↑ field! b/c R PID

Since $pR/\langle q \rangle = \begin{cases} R/\langle q \rangle & \text{if } p \nmid q \ (\langle p, q \rangle = R) \\ R/\langle q/p \rangle & \text{if } p \mid q. \end{cases}$

Induction on # of prime factors of $q_1 \cdots q_n \Rightarrow$ uniqueness for pM.

$\operatorname{ord}_p\left(\frac{q_i}{\gcd(p, q_i)}\right)$ is well defined hence $\operatorname{ord}_p(q_i)$ is well defined. ∎

Proof of prop 1: $M = M_{tor} \oplus F$.

$M_{tor} = \ker(M \to M_{(0)})$

where $M_p = S^{-1}M$ for $S = R \setminus p$

$x \cdot m = 0 \iff \frac{m}{1} = 0$ in $M[x^{-1}]$

Suffices: $E = \mathrm{im}(M \to M_{(0)})$ is free since then we have an exact sequence $0 \to M_{tor} \to M \to E \to 0$ which splits

Q: Why does this show rank M is well-defined?
A: $E \cong M/M_{tor}$!

$\ker(N \oplus N' \to N') = N \Rightarrow N' \cong N \oplus N'/N$

Will prove $E \subseteq$ f.g. free submodule of $M_{(0)}$ so then p72 of lecture notes applies... will prove next time!

$E = \mathrm{im}(M \to M_{(0)})$

↑ invert nonzero elements of R

Need: $E = \mathrm{im}(M \to M_{(0)}) \subseteq$ f.g. free submodule of $M_{(0)}$.

$M = \langle m_1, \dots, m_k \rangle$

$\Rightarrow M_{(0)} = \langle \frac{m_1}{1}, \dots, \frac{m_k}{1} \rangle$ over $R_{(0)} = K(R)$ (field of fractions)

$E = \langle \frac{m_1}{1}, \dots, \frac{m_k}{1} \rangle$ over R.

"An integral domain maps injectively to its fraction field"

Choose basis $x_1, \dots, x_n$ for $M_{(0)}$ over $K(R)$.

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 $E \subseteq R\frac{x_1}{a} \oplus \cdots \oplus R\frac{x_n}{a}$. ☒

Ex: prove rank $M = n$.

Proof of prop 2. $M = M_{tor} \Rightarrow M = \bigoplus_p M(p)$

Lemma $M(p) \overset{\text{def}}{=} \{m \in M \mid p^e m = 0 \text{ for } e \gg 0 m\}$
$= \ker(M \to M[p^{-1}])$ ☒

Lemma: If $M = M_{tor}$ then $M(p) \hookrightarrow M$ induces an isomorphism of $R_{\langle p \rangle}$-mods $M(p)_{\langle p \rangle} \xrightarrow{\simeq} M_{\langle p \rangle}$.

Proof: Need surjection by HW5 #9b.
Direct check ☑.

Lemma: If $p^n N = 0 \Rightarrow N \xrightarrow{\simeq} N_{\langle p \rangle}$ as R-mods.
(p-module; $n \mapsto \frac{n}{1}$)

Proof: $p^n N = 0 \Rightarrow N$ is a module over $R/\langle p^n \rangle$
Then for $r \in R$, $\bar{r} \in \left(R/\langle p^n \rangle\right)^*$ if $r \notin \langle p \rangle$
since $\langle r, p^n \rangle = 1$.
Hence if $S = R \setminus \langle p \rangle$ then

$$\begin{aligned} N_{\langle p \rangle} &= S^{-1} N \\ &= S^{-1} R N \\ &= S^{-1} R/\langle p^n \rangle N \\ &\cong R/\langle p^n \rangle N \\ &= N \end{aligned}$$

☑

Proof of Prop 2: $M = M_{tor} \Rightarrow M = \bigoplus_p M(p)$

$M(p) \neq 0 \Rightarrow \exists\, x_p \in M(p)$ with $p^{\overset{\circ}{\#}} x_p = 0$
Thus $\langle x_p \mid M(p) \neq 0 \rangle$ f.g. by Cor p.(47)
so $M(p) = 0$ for almost all p.
Hence $\bigoplus_p M(p) = \prod_p M(p)$
Lemmas $\Rightarrow M(p) \to M_{\langle p \rangle} = M(p)_{\langle p \rangle} = M(p)$

$\Rightarrow M(p) \xrightarrow{\simeq} M_{\langle p \rangle}$ $\forall p$.
But $M(q)_{\langle p \rangle} = 0$ $\forall \langle q \rangle \neq \langle p \rangle$. Thus

$$\begin{aligned} M \to \prod_p M_{\langle p \rangle} &= \prod_p M(p) \\ &= \bigoplus_p M(p) \end{aligned}$$

becomes an isomorphism locally at every $\langle p \rangle$.
$\Rightarrow$ isomorphism $M \xrightarrow{\simeq} \bigoplus_p M(p)$

Proof of Prop 3 $M = M(p) \Rightarrow M \cong R/\langle p^{e_1}\rangle \oplus \cdots \oplus R/\langle p^{e_n}\rangle$

$$\frac{R \oplus \cdots \oplus R}{\langle p^{e_1}\rangle \oplus \cdots \oplus \langle p^{e_n}\rangle} = \operatorname{coker}\left(\begin{bmatrix} p^{e_1} & & 0 \\ & \ddots & \\ 0 & & p^{e_n} \end{bmatrix}\right)$$

Nakayama's Lemma:

fix local ring A (unique max ideal) with max ideal $\mathfrak{p}$ and f.g. N, then $N = \mathfrak{p}N \Rightarrow N = 0$.

Proof: $N = \langle x_1, \dots, x_n\rangle \Rightarrow x_1 = \sum_{i=1}^{n} a_i x_i$ with $a_i \in \mathfrak{p}$ (including)

$\Rightarrow (1 - a_1) x_1 = \sum_{i=2}^{n} a_i x_i$ with $a_i \in \mathfrak{p}\ \forall i$

$1 - a_1 \in A \setminus \{\mathfrak{p}\} = A^*$

$\Rightarrow x_1 \in \langle x_2, \dots, x_n\rangle$

done by induction on n.

Nakayama's Lemma (the second):

fix $(A, \mathfrak{p})$ local with M f.g. write $M \to M/\mathfrak{p}M$, $x \mapsto \bar{x}$.

Assume $M/\mathfrak{p}M = \langle \bar{x}_1, \dots, \bar{x}_n\rangle$

Then $M = \langle x_1, \dots, x_n\rangle$

Proof: part 1 with $N = M/\langle x_1, \dots, x_n\rangle$ ☑

Ex $x_1, \dots, x_n$ basis of free module F $\Leftrightarrow$ $\bar{x}_1, \dots, \bar{x}_n$ basis of $F/\mathfrak{p}F$ (vector space).

Proof of Prop 3: Apply Nakayama to R (a local PID), $R = R_{\langle p\rangle}$

$K \hookrightarrow F \twoheadrightarrow M$

free

Details in lecture notes ☑ ✓ WE SURVIVED