Algebra I

September 28, 2023

Recommended Text

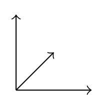
Abstract Algebra (3e) - Dummit and Foote
Finite Groups: An Introduction (2nd revised) - Jean-Pierre Serre
Robert Boltje's Lecture Notes - (`https://boltje.math.ucsc.edu/courses/f17/f17m200notes.pdf`)

Definition: Binary Operation

Let S be a set. A binary operation on S is a function $f : S \times S \to S$. We will almost never use f for the binary operation $(f(s,t))$.
The usual notation for binary operations is $s * t$.

Example

1. $S = \mathbb{R}^3$, define $f : S \times S \to S$ as $(\vec{x}, \vec{y}) \rightsquigarrow \vec{x} + \vec{y}$.
2. $S = \mathbb{R}^3$, define $S \times S \xrightarrow{f} S$ as $(\vec{x}, \vec{y}) \rightsquigarrow \vec{x} + \vec{y}$.
    - Note that $(\vec{x}, \vec{y}) \rightsquigarrow \vec{x} \cdot \vec{y}$ is not a binary operation.
3. $S = \mathbb{Z}$ as $(m, n) \mapsto m \cdot n$.
4. $S = \mathbb{R}^3$ as $(\vec{x}, \vec{y}) \rightsquigarrow \frac{\vec{x}+\vec{y}}{2}$



5. Let $n \geq 1$ be an interger and $S = M_{n \times n}(\mathbb{R}) = \{n \times n \text{ real matricies}\}$. Then $(A, B) \rightsquigarrow AB$.

Observations

Examples 1,3,5 are associative; examples 2,4 are not.
Examples 1-4 are commutative; example 5 commutes only when $n = 1$.
$\vec{0}$ for example 1, 1 for example 3, and I_n for example 5.

Q: What is a Group?

A group is a set equipped with a binary operation which satisfies three axioms.
Let $*$ be a binary operation on a set S.

1. Say $*$ is associative if $\forall a, b, c \in S$, $(a * b) * c = a * (b * c)$.
2. Say $*$ is commutative if $\forall a, b \in S$, $a * b = b * a$.
3. An element $e \in S$ is a neutral element (with respect to $*$) if $\forall a \in S$, $a * e = a = e * a$.
    - If there exists a neutral element, then it is unique.

4. Suppose $(S,*)$ has a neutral element e. Let $a \in S$. Then $b \in S$ is called an inverse of a (with respect to $*$) if $a * b = e = b * a$.

Definition: Group

A group is a set G equipped with a binary operation $*$ such that

1. $*$ is associative.
2. $*$ has a neutral element e.
3. Every $g \in G$ has an inverse.

If, in addition, $*$ is commutative, we say $(G,*)$ is an abelian or commutative group.

Examples

$(\mathbb{R}^3,+)$ is a commutative group.
$(\mathbb{R}^3,\times)$ has no neutral element.
$(\mathbb{Z},\cdot)$ has no inverse (except ± 1).
$(\mathbb{R}^3,\text{mid})$ is not associative. (the midpoint)
$(M_{n\times n}(\mathbb{R}),\cdot)$ has no inverse of $0_{n\times n}$.
For $n \geq 1$, $(\mathbb{R}^n,+)$ and $(\mathbb{C}^n,+)$ are abelian groups.

Proof that the Neutral Element is unique.

Let e, e' be neutral eements. Then $e' = e * e' = e$. ■

Proof that the Inverse is unique.

Left to the reader.

Definition: Subgroup

Let G be a group, and let H be a subset of G. We say that H is a subgroup of G if

1. $\forall h_1, h_2 \in H$, $h_1 * h_2 \in H$.
2. $e \in H$.
3. $\forall h \in H$, $h^{-1} \in H$.

Examples

$\mathbb{Z}^n \subseteq \mathbb{R}^n$ is a subgroup ($* = +$).
$G = \{A \in M_{n\times n} : \det(A) \neq 0\}$. Then $(G,\cdot)$ is a group.

- This is the General Linear Group on $\mathbb{R}$: $\mathrm{GL}_n(\mathbb{R})$.
- Recall $A^{-1} = \frac{1}{\det(A)}\left((-1)^{itj}\det(M_{\alpha_i})\right)$.

Definition: General Linear Subgroups

$S = \{A \in \mathrm{GL}_n(\mathbb{R}) : a_{ij} \in \mathbb{Z},\ \forall 1 \leq i, j \leq n\}$.
S is closed under $\cdot$ and $I_n \in S$, but for example

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^{-1} = \frac{1}{1 \cdot 4 - 2 \cdot 3} \begin{pmatrix} 4 & -2 \\ -3 & 1 \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{pmatrix}$$

so S is not a subgroup.
However, $T = \{A \in S : \det(A) = \pm 1\} \subseteq \mathrm{GL}_n(\mathbb{R})$.

- Note that if $AA' = I_n$ then $\det(A)\det(A') = 1$.

Definition: Additive Groups

For groups like $\mathbb{Z}^n$, $\mathbb{R}^n$ and $\mathbb{C}^n$, we will use $+$ for the binary operation and say that they are additive groups.
The Neutral Element is denoted as 0.
The inverse is denoted as $-g$.
For $m \geq 1$ and $g \in G$, $mg = g + \overset{m}{\cdots} + g$ and $(-m)g = -(mg)$.

Definition: Multiplicative Groups

For groups like $\mathrm{GL}_n(\mathbb{C})$ or $\mathrm{GL}_n(\mathbb{Z})$, we say that the group is multiplicative.
Denote the neutral element as 1.
Denote the inverse of g as g^{-1}.
For $m \geq 1$, $g^m = g \overset{m}{\cdots} g$.
$g^0 = 1$.
$g^{-m} = (g^m)^{-1}$.

Definition: Group Element Order

Let G be a group, $g \in G$, and $m \geq 1$.
Say g has order m if $g^m = 1$ and $g^k \neq 1,\ \forall k$ such that $1 \leq k \leq m$.
An element has infinite order if $g^m \neq 1,\ \forall m \in \mathbb{Z}^+$.

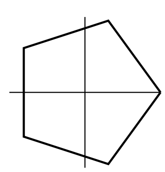
Examples

In D_{10}, I_2 has order 1, rotations have order 5 and reflections have order 2.

Groups from Geometry

Pentagon

Consider the regular pentagon P.



$H = \{T \in \mathrm{GL}_2(\mathbb{R}) : T(P) = P\}$.
This is the symmetry group of P or D_{10} (sometimes D_5)
$H \leq \mathrm{GL}_2(\mathbb{R})$.

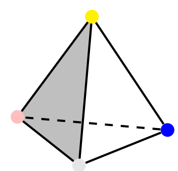
- Proof of closure.
  Suppose $T_1, T_2 \in H$. Then $T_1(P) = P$, $T_2(P) = P$ and $(T_1 \circ T_2)(P) = T_1(T_2(P)) = T_1(P) = P$.
  Therefore H is closed under $\circ$.

- Proof of identity.
  $\mathrm{Id}_{\mathrm{GL}_2} = I_2$ does satisfy $I_2(P)$.

- Proof of inverse.
  If $T \in H$ (i.e. $T \in \mathrm{GL}_2(\mathbb{R})$ and $T(P) = P$, apply T^{-1} and get $T^{-1}(T(P)) = T^{-1}(P)$. Therefore $P = T^{-1}(P)$.

Tetrahedron

Let X be the regular tetrahedron and $A = \{\text{rotational symmetries of } X\}$.



Then A contains

- The identity: 1.

- $2 \cdot 4 = 8$ rotations by 120°.

- 3 rotations of 180°.

So we have a bijection $r : \{B, P, W, Y\} \to \{B, P, W, Y\}$ where

$$
\begin{tikzcd}[row sep=tiny]
\mathrm{B} \arrow[r] & \mathrm{B} \\
\mathrm{P} \arrow[rdd] & \mathrm{P} \\
\mathrm{W} \arrow[ru] & \mathrm{W} \\
\mathrm{Y} \arrow[ru] & \mathrm{Y}
\end{tikzcd}
$$

Definition: Symmetric Group

Let S be a set (e.g. $E = \{B, P, W, Y\}$). The Symmetric Group $\mathrm{Sym}(E)$ is the set of bijections $f : E \to E$ equipped with the binary operation $\circ$ (composition).

October 3, 2023

Propositions: Symmetric Group

Let X be a set.
When $|X| = n$ denote the elements $\{1, 2, \ldots, n\}$.
$\mathrm{Sym}(X) = \{f : X \to X | f \text{ is bijective}\}$.
With $\circ$ (composition of functions) as a binary operation, $\mathrm{Sym}(X)$ is a group.

Symmetric Group Order

If $|X| = n$, then $|\mathrm{Sym}(X)| = n!$

- Proof
  Let $X = \{1, 2, \ldots, n\}$. A bijection f consists of $f(1), f(2), \ldots, f(n)$.
  For $f(1)$, we have n choices; for $f(2)$ we have $n-1$ choices. This continues until only 1 choice remains for $f(n)$.
  Therefore the choices are $(n)(n-1)\cdots(1) = n!$

Example

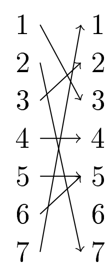
For the symmetric group on four letters $\{a, b, c, d\}$, $|\mathrm{Sym}(4)| = 4! = 24$

Definition: Cycles

Let $x = \{1, \ldots, n\}$, $m \geq 1$ be an integer and $a_1, a_2, \ldots, a_m$ distinct elements in X.
Then the m-cycle denoted by $(a_1\ a_2\ \cdots\ a_m)$ is the element of $\mathrm{Sym}(X)$ which maps a_1 to a_2, a_2 to a_3,..., a_{m-1} to a_m, and a_m to a_1.

Example

Let $n = 7$ and $m = 4$. Then $(2\ 7\ 1\ 3)$ is a bijection.



Degenerate Case

$m = 1$ gives Id_X.

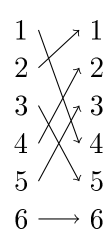
First Non-Degenerate Case

A transposition is, by definition a 2-cycle: $(a_1\ a_2)$.

Proposition: Symmetric Group as Cycle Composition

Every elenent in $\mathrm{Sym}(X)$ is the product (using $\circ$) of m-cycles, where m can vary.

- Proof
  Consider $\mathrm{Sym}(6)$.



This gives a bijection $\pi = (1\ 4\ 2)(3\ 5)(6)$ which is the composition of cycles.
We say that this π has cycle type $3 + 2 + 1$.

- Cycle Type
  If instead $\pi = (1\ 4\ 2)(3\ 5\ 6)$ then the cycle type is given as $3 + 3$.

Finite Symmetric Groups

For $n = 2$, $\mathrm{Sym}(X) = \{\mathrm{Id}, (1\ 2)\}$.
This gives cylce types $1 + 1$ and 2.
For $n = 3$, $\mathrm{Sym}(X) = \{\mathrm{Id}, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$.
This gives cycle types $1 + 1$, $2 + 1$ and 3.

Symmetric Group for Tetrahedron

For $n = 4$ let $X = \{B, P, W, Y\}$.
Partitions of $n = 4$ are

$$
\begin{array}{lllllllll}
4 = 4 & 6 & (B\ P\ W\ Y) & \cdots & & & & & \text{sign} = -1 \\
\ \ = 3 + 1 & 4 \cdot 2 = 8 & (P\ W\ Y) & \cdots & & & & & \text{sign} = +1 \\
\ \ = 2 + 2 & \frac{\binom{4}{2}}{2} = 3 & (B\ P)(W\ Y) & (B\ W)(P\ Y) & (B\ Y)(P\ W) & & & & \text{sign} = +1 \\
\ \ = 2 + 1 + 1 & \binom{4}{2} = 6 & (B\ P) & (B\ W) & (B\ Y) & (P\ W) & (P\ Y) & (W\ Y) & \text{sign} = -1 \\
\ \ = 1 + 1 + 1 + 1 & 1 & \mathrm{Id}_X & & & & & & \text{sign} = +1
\end{array}
$$

Rotation Group for Tetrahedron

$$
\begin{aligned}
A &= \{\text{Rotational Symmetries}\} \\
&= \{\mathrm{Id}_X, 8 \text{ 3-cycles}, 3 \text{ of type } 2{+}2\}
\end{aligned}
$$

Note, from the sign, that $A \leq \mathrm{Sym}(4)$.

Symmetries Not in Rotation

Why, for example, is $(B\ P)$ not in the rotation group?
If it were, it should be possible to swap vertices and then undo the switch with only rotation.
However, the two tetrahedra are mirror images across a plane.
Observe that the right hand rule with respect to P, W and Y will give opposite, orthogonal vectors.

Rotation as a Subgroup of Symmetry

Q: Is A a subgroup of $\mathrm{Sym}(4)$?
Following the definition, it would be necessary to veryify

- $\mathrm{Id} \in A$
- A is closed under inverse.
- A is closed under composition.

Group Homomorphism

Let G and H be groups (whose binary operations are denoted by $g_1 \cdot g_2$).
A (group) homomorphism from G to H is a function $\phi : G \to H$ such that

- $\phi(g_1 \underset{G}{\cdot} g_2) = \phi(g_1) \underset{H}{\cdot} \phi(g_2)$

Properties of Group Homomorphism

1. $\phi(1_G) = 1_H$
2. $\phi(g^{-1}) = [\phi(g)]^{-1}, \ \forall g \in G$

- Proof
  By definition, $\phi(1_G \cdot 1_G) = \phi(1_G) \cdot \phi(1_G)$.
  Letting $e = \phi(1_G)$, we get $e = e \cdot e$.
  By multiplying both sides by e^{-1}, we get $1_H = e$.
  Part two is left as an exercise.

Example 1

Let $n \geq 1$ and $G = \mathrm{GL}_n(\mathbb{R}) = \{A \in M_{n \times n}(\mathbb{R}) | \det(A) \neq 0\}$.
In particular, when $n = 1$, $\mathrm{GL}_1(\mathbb{R}) = \mathbb{R}^* = \{r \in \mathbb{R} | r \neq 0\}$ (with multiplication as the binary operation).
Then $\det : G \to H$ is a group homomorphism.
That is $\det(AB) = \det(A)\det(B)$ (as learned in MATH 21).

Example 2

Let $n \geq 1$, $G = \mathrm{Sym}(n)$, $H = \mathrm{GL}_n(\mathbb{R})$.
Construct a group homomorphism $\rho : G \to H$.
Recall that a linear transformation $A \in H$ is completely determined by $Ae_1, \ Ae_2, \ \ldots \ , Ae_n$
where $e_1 = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \ldots, e_n = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}$.
For $\pi \in G = \mathrm{Sym}(n)$, $\rho(\pi)$ is the linear transformation that maps e_i to e_j whenever π maps i to j.
This is a surjective linear transformation on a vector space and, therefore, invertible.

- Example
  For $n = 4$ and $\pi = (2\ 3\ 4)$

$$\begin{tikzcd}
1 \arrow[r] & 1 \\
2 \arrow[dr] & 2 \\
3 \arrow[dr] & 3 \\
4 \arrow[uur] & 4
\end{tikzcd}$$

  $\rho(\pi)$

$$\begin{tikzcd}[row sep=small]
e_1 \arrow[r] & e_1 \\
e_2 \arrow[dr] & e_2 \\
e_3 \arrow[dr] & e_3 \\
e_4 \arrow[uur] & e_4
\end{tikzcd}$$

Therefore

$$\rho(\pi) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

– Is this a group homomorphism?
  Let $\pi_1, \pi_2 \in G$ be arbitrary elements.
  Need to show: $\rho(\pi_1 \circ \pi_2) = \rho(\pi_1) \circ \rho(\pi_2)$.
  Both sides are linear transformations and, hence, determined by their actions on e_i for $i = 1, \dots, n$.

$$\begin{aligned} \rho(\pi_1 \circ \pi_2)e_i &= e_{\pi(i)} \\ &= e_{\pi_1(\pi_2(i))} \\ \rho(\pi_1)(\rho(\pi_2)e_i) &= \rho(\pi_1)(e_{\pi_2(i)}) \end{aligned}$$

Composition of Group Homomorphisms

Let G, H and K be groups and $G \xrightarrow{\phi} H$ and $H \xrightarrow{\psi} K$ be homomorphisms.
Then the composite $\psi \circ \phi : G \to K$ is a group homomorphism.

Proof

Let $g_1, g_2 \in G$ be arbitrary.

$$\begin{aligned} (\psi \circ \phi)(g_1 g_2) &= \psi(\phi(g_1 g_2)) && \text{by definition of } \circ \\ &= \psi(\phi(g_1 \phi(g_2)) && \text{since } \phi \text{ is a group homomorphism} \\ &= \psi(\phi(g_1))\psi(\phi(g_2)) && \text{since } \psi \text{ is a group homomorphism} \\ &= (\psi \circ \phi)(g_1) \circ (\psi \circ \phi)(g_2) && \text{by definition of } \circ \end{aligned}$$

Definition: Sign Homomorphism

Let $n \geq 1$ and $G = \mathrm{Sym}(n)$.
Ths sign homomorphism is the composition sign: $G \xrightarrow{\rho} \mathrm{GL}_n(\mathbb{R}) \xrightarrow{\det} \mathbb{R}^*$

Sign of Symmetric Group

$\mathrm{sign}(\mathrm{sym}(n)) \subseteq \{1, -1\} \leq \mathbb{R}^*$

- Lemma
  Let $a_1, \dots, a_m$ be distinct numbers between 1 and n.
  Then $(a_1 \cdots a_m)$ is equal to $(a_1 \cdots a_{m-1})(a_{m-1}\ a_m)$.
  This will be proven on homework.

- Corollary
  Any m cycle is the composition of $m-1$ transpositions.
  Namely, $(a_1, \ \dots \ , a_m) = (a_1 \ a_2)(a_2 \ a_3)\cdots(a_{m-1} \ a_m)$.
  Easily check: $\mathrm{sign}((a_i \ a_{i+1})) = -1$.
  Now any $g \in \mathrm{Sym}(n)$ allows a cycle decomposition.

Definition: Kernel of a Homomorphism

Let $G \xrightarrow{\phi} H$ be a group homomorphism.
The kernel of ϕ is $\ker(\phi) := \{g \in G | \phi(g) = 1_H\}$.

The Kernel is a Subgroup

Let $g_1, g_2 \in \ker(\phi)$. Then

$$\begin{aligned} \phi(g_1 g_2) &= \phi(g_1)\phi(g_2) && \phi \text{ is a homomorphism} \\ &= 1_H 1_H && g_1, g_2 \in \ker(\phi) \\ &= 1_H && g_1, g_2 \in \ker(\phi) \end{aligned}$$

Similarly, $1_G \in \ker(\phi)$ and $g^{-1} \in \ker(\phi)$ if $g \in \ker(\phi)$. ■

Definition: Alternating Group

Let X be a set, $|X| = n \leq \infty$.
The alternating group on X is the $\mathrm{Alt}(X) = \ker(\mathrm{sign} : \mathrm{Sym}(X) \to \{\pm 1\})$.

October 5, 2023

Definition: Group Action

Let G be a group and X a set.
A (left) action of G on X is a function $\alpha : G \times X \to X$ which satisfies two conditions:

1. $\alpha(1_G, x) = x$ for all $x \in X$.

2. $\alpha(g_1, \alpha(g_2, x)) = \alpha(g_1 g_2, x)$ for all $g_1, g_2 \in G$ and $x \in X$.

Notation

Write $\alpha(g, x) = g * x = g \cdot x = gx$.

Example A

Let X be any set, and let $G = \mathrm{Sym}(X) = \{f : X \to X \text{ bijections}\}$ where the group operation $\circ$ is the composition of functions.
Then G acts (on the left) on X by $f * x \underset{\text{def}}{=} f(x)$.
Then the features

1. $\mathrm{Id}_X(x) = x, \ \forall x \in X$

2. $g_1 * (g_2 * x) = (g_1 \circ g_2) * x,\ \forall g_1, g_2 \in G,\ \forall x \in X$

   - Or $g_1(g_2(x)) = (g_1 \circ g_2)(x)$

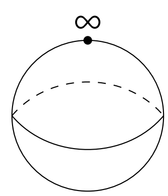
are satisfied.

Example B

Let $G = \mathrm{Sym}(\{B,\ P,\ W,\ Y\})$ which acts on $X = \{B,\ P,\ W,\ Y\}$.
If $H \leq G$, then H acts on X as well, define $h * x = \dot{h} * x$ (where $\dot{h}$ is regarded as in the alternating group of G).
In particular, $\mathrm{Alt}(\{B,\ P,\ W,\ Y\})$ acts on X by rotations.

Example C*

This example is not required for this class.
From complex Analysis we have the Riemann sphere $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$.



Let $G = \mathrm{SL}_2(\mathbb{C})$.
Define G-action on $X = \mathbb{P}^1(\mathbb{C})$ by

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} z := \frac{\alpha z + \beta}{\gamma z + \delta} \qquad (\infty \text{ if } \gamma z + \delta = 0)$$

This is called the Möbius group action on $\mathbb{P}^1(\mathbb{C})$.
Exercise: show that 1. and 2. are satisfied.

Definitions

Let G act on X. (Say X is a (left) G-set)

Stabilizer

Let $x \in X$. The stabilizer of x in G is $\mathrm{Stab}_G(x) = \{g \in G | g * x = x\} \subseteq G$.

- Example 1
  Let G be any group and X a G-set.
  Then for any $x \in X$, $\mathrm{Stab}_G(x) \leq G$.

  - Proof
    1. $1_G \in \mathrm{Stab}_G(x)$ since, by definition, $1_G * x = x$.
       Therefore the identity is present.

    2. If $g_1, g_2 \in \mathrm{Stab}_G(x)$ are such that $g_1 * x = x$ and $g_2 * x = x$, then $(g_1 g_2) * x \underset{\text{2nd Axiom}}{=} g_1 * (g_2 * x) = g_1 * x = x$.
       Therefore the stabilizer is closed under composition.

3. Say $g \in \mathrm{Stab}_G(x)$ and $g * x = x$. Apply g^{-1} to both sdies to get

$$x \underset{\text{1st Axiom}}{=} 1_G * x = (g^{-1}g) * x \underset{\text{2nd Axiom}}{=} g^{-1} * (g * x) = g^{-1} * x$$

Therefore the stabilizer is closed under inverse.

- Example 2
  Let $G = \mathrm{Alt}(\{B,\ P,\ W,\ Y\})$ and consider $H = \mathrm{Stab}_G(W) = \{\mathrm{Id}, (B\ P\ Y), (B\ Y\ P)$.
  Fact: H does not act transitively on X, since W is fixed and no element $g \in H$ satisfies $g * W = B$.

Orbit

Let $x \in X$. The G-orbit of x in X is $G \cdot x = \{g * x | g \in G\} \subseteq X$.
Let G act on X and $x, y \in X$. Either $G \cdot x = G \cdot Y$ or $G \cdot x \cap G \cdot y = \varnothing$.
So X is the disjoint union of G-orbits.
e.g. $\{B,\ P,\ W,\ Y\} = \{W\} \coprod \{B,\ P,\ Y\}$ gives the $\mathrm{Stab}_G(W)$-orbits.

- Example 1
  When $G = \mathrm{Alt}(X)$, for $X = \{B,\ P,\ W,\ Y\}$, there is only one orbit since $\forall x \in X$, $G \cdot x = X$.

- Example 2
  When $G = \mathrm{Stab}_G(W)$, for $X = \{B,\ P,\ W,\ Y\}$, then $G \cdot W = \{W\}$ while

$$\begin{aligned} G \cdot B &= \{\mathrm{Id}(B),\ (B\ P\ Y)(B),\ (B\ Y\ P)(B)\} = \{B,\ P,\ Y\} \\ &= G \cdot P = \{\mathrm{Id}(P),\ (B\ P\ Y)(P),\ (B\ Y\ P)(P)\} = \{P,\ Y,\ B\} \\ &= G \cdot Y \end{aligned}$$

Transitivity

Say G acts transitively on X (or the action is transitive) if, for any pair $x, y \in X$, there exists $g \in G$ (depending on x and y) such that $g * x = y$.

- Example
  $G = \mathrm{Alt}(\{B,\ P,\ W,\ Y\}) \circlearrowright \{B,\ P,\ W,\ Y\}$ is transitive.

  - Proof
    Let $x, y \in X$ be arbitrary.
    If $x = y$, then take $g = \mathrm{Id}_X$ and we have $g * x = y$.
    Suppose $x \neq y$, then write $X = \{x,\ y,\ z,\ w\}$ and take $g = (x\ y)(z\ w)$. We have $g * x = y$.
    e.g. $x = P$, $y = Y$, $z = B$ and $w = W$ gives $g = (P\ Y)(B\ W)$.

- Exercise *
  This exercise is not required for the course.
  Prove that $\mathrm{SL}_2(\mathbb{C})$ acts transitively on $\mathbb{P}^1(\mathbb{C})$.
  Say $\mathbb{P}^1(\mathbb{C})$ is a homogeneous space under $\mathrm{SL}_2(\mathbb{C})$.

Proposition: Group Action Gives Group Homomorphisms

($\longrightarrow$) Let G act on X. Then

1. For any $g \in G$, the function $\pi_g : X \to X$ defined by $\pi_g(x) = g * x$ is a bijection of X, hence $\pi_G \in \mathrm{Sym}(X)$.

2. The function $G \xrightarrow{\phi} \mathrm{Sym}(X)$ given by $\phi(g) = \pi_g$ is a group homomorphism.

Proof of 1

Need to show that π_g is injective and surjective.
(Inj) Let $x, y \in X$ and assume $\pi_g(x) = \pi_g(y)$ (i.e. $g * x = g * y$).
Apply $g^{-1} *$ on both sides, such that $x = g^{-1} * (g * x) = g^{-1} * (g * y) = y$.
(Sur) Let $x \in X$ be arbitrary. Need to find $y \in X$ such that $\pi_g(y) = x$.
Take $y = g^{-1} * x$, and $\pi_g(y) = g * (g^{-1} * x) = x$.

Proof of 2

Need to show that $\forall g_1, g_2 \in G$, $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$.
$\phi(g_1 g_2) \in \mathrm{Sym}(X)$ is characterized by $[\phi(g_1 g_2)](x) = \pi_{g_1 g_2}(x) = (g_1 g_2) * x$.
On the other hand, $\phi(g_1)\phi(g_2) \in \mathrm{Sym}(X)$ is characterized by $[\phi(g_1)\phi(g_2)](x) = \phi(g_1)[\phi(g_2)(x)] = g_1 * (g_2 * x)$.
By the second group action axiom, these must be the same.

Proposition: Group Homomorphism Admits Group Action

($\longleftarrow$) Let $G \xrightarrow{\rho} \mathrm{Sym}(X)$ be a group homomorphism.
Then, by letting $g * x = \rho(g)(x) \in X$ we get a left G-action on X.

Proof

1. $1_G * x = \rho(1_G)(x) = \mathrm{Id}_X(x) = x$.

2. Let $g_1, g_2 \in G$ and $x \in X$. Then $(g_1 g_2) * x = [\rho(g_1 g_2)](x) = [\rho(g_1) \circ \rho(g_2)](x) = \rho(g_1)[\rho(g_2)(x)] = g_1 * (g_2 * x)$.

Definition: Right Group Actions

Let G be a group and X be a set. A right G-action on X is a function $\beta : X \times G \to X$ such that

1. $\beta(x, 1_G) = x,\ \forall x \in X$.

2. $\beta(x, g_1 g_2) = \beta(\beta(x, g_1), g_2),\ \forall g_1, g_2 \in G,\ \forall x \in X$.

Notation

$\beta(x, g) = x * g = x \cdot g = xg$

Remark

If $\alpha : G \times X \to X$ is a left action, we get a right action $\beta : X \times G \to X$ by $\beta(x, g) = \alpha(g^{-1}, x)$ and vice versa.
That is $x * g = g^{-1} * x$.
Proof recommended as an exercise.

Analogues

Stability, orbit and transitivty all have analogues which can be demonstrated by converting to left actions.

Definition: Cosets

Let $H \leq G$, and let $X = G$.
We have left action $H \times X \to X$ and $h * x = hx$ (taken in G).
As well as right action $X \times H \to X$ where $x * h = xh$.
A (left) H-coset is an orbit xH for some $x \in X$.
A (right) H-coset is an orbit Hx for some $x \in X$.

Example

Let $G = \text{Alt}(4)$, $H = \text{Stab}_G(W) = \{\text{Id}, (B\ P\ Y), (B\ Y\ P)\}$.

1. Take any $x \in H$, $xH = H$.
2. Take $x = (B\ P)(W\ Y)$, and $xH = \{(B\ P)(W\ Y), (B\ P)(W\ Y)(B\ P\ Y) = (P\ W\ Y), (B\ P)(W\ Y)(B\ Y\ P) = (B\ W\ Y)\}$.
3. There are two more; what are they?

October 10, 2023

Cosets Revisited

Let G be a group, $H \leq G$. Then a (left) H-coset in G is a set of the form

$$gH = \{gh | h \in H\}$$

, where $g \in G$

Coset Space

G/H is the set of H-cosets.

- Example
  For $G = \text{Alt}(4)$, given $C_1 = H = \text{Stab}_G(B) = \{1, (P\ W\ Y), (P\ Y\ W)\}$, we have
  $C_2 = (B\ P\ W)H = \{(B\ P\ W), (B\ P\ )(W\ Y), (B\ P\ Y)\}$
  $(B\ P\ W) \circ (P\ W\ Y) = (B\ P)(W\ Y)$

$$\begin{array}{c} \text{P} \longleftarrow \text{B} \longleftarrow \text{B} \\ \text{B} \longleftarrow \text{W} \longleftarrow \text{P} \\ \text{Y} \longleftarrow \text{Y} \longleftarrow \text{W} \\ \text{W} \longleftarrow \text{P} \longleftarrow \text{Y} \end{array}$$

  $(B\ P\ W) \circ (P\ Y\ W) = (B\ P\ Y)$

$$\begin{aligned} P &\longleftarrow B \longleftarrow B \\ Y &\longleftarrow Y \longleftarrow P \\ W &\longleftarrow P \longleftarrow W \\ B &\longleftarrow W \longleftarrow Y \end{aligned}$$

$C_3 = (B\ W\ P)H = \{(B\ W\ P), (B\ W\ Y), (B\ W)(P\ Y)\}$
$C_4 = (B\ Y\ P)H = \{(B\ Y\ P), (B\ Y\ )(P\ W), (B\ Y\ W)\}$
Then $G/H = \{C_1, C_2, C_3, C_4\}$.

- Q: What do the 3 elements in C3 have in common in geometric terms?
  C_3 sends B to W.
  Similarly, the cosets send B to all other vertices (including to itself).

Definition: Transporter

Let G be a group and X a G-set.
For two points, $x, y \in X$, the transporter $\mathrm{Trsp}_G(x, y) = \{g \in G | gx = y\}$.

Example

$G/H = \{\mathrm{Trsp}_G(B, B), \mathrm{Trsp}_G(B, P), \mathrm{Trsp}_G(B, W), \mathrm{Trsp}_G(B, Y)\}$

Note

When $x = y$, we recover $\mathrm{Trsp}_G(x, x) = \mathrm{Stab}_G(x)$.
For general G and H, there may not be a nice geometric action associated with it.
But G/H is still a G-set since $g'(gH) = (g'g)H$.

Proposition (B)

Let $H \leq G$ be a subgroup and let $g \in G$.
Then the map $H \xrightarrow{f} gH$ defined by $h \mapsto f(h) = gh$ is a bijection.

Proof

(Surjective) Any element x in gH is, by definition, of the form gh for some $h \in H$. So $x = f(h)$.
(Injective) Say $h_1, h_2 \in H$ satisfy $f(h_1) = f(h_2)$. That is $gh_1 = gh_2$. Multiplying g^{-1} on the left, we get $h_1 = h_2$.

Proposition (C)

Let G act on X, $x \in X$, and $g \in G$.
Take $y := gx$ and $H = \mathrm{Stab}_G(x)$. Then $gH = \mathrm{Trsp}_G(x, y)$.

Proof

($\subseteq$) Let $gh \in gH$ be arbitrary. Then

$$(gh) * x \underset{\text{Axiom 2}}{=} g * (h * x) \underset{h \in \mathrm{Stab}_G(x)}{=} g * x \underset{y = g*x}{=} y$$

Therefore $gh \in \mathrm{Trsp}_G(x, y)$.
($\supseteq$) Suppose $g' \in \mathrm{Trsp}_G(x, y)$. Consider $g^{-1}g'$. Then

$$(g^{-1}g')*x = g^{-1}*(g'*x) \underset{g'\in \mathrm{Trsp}_G(x,y)}{=} g^{-1}(y) = x$$

Therefore $(g^{-1}g') \in \mathrm{Stab}_G(x)$. Setting $g^{-1}g' := h$, so $g' = gh \in gH$.

Theorem: Orbit-Stabilizer Theorem (OST)

Let G act transitively on a set X (so that there is only one orbit in X, namely X itself).
If $|G| < \infty$, then for any $x \in X$ we have

$$|X| \cdot |\mathrm{Stab}_G(x)| = |G|$$

Proof

Let us count $|G|$ by partitioning G into transporters.

$$G = \coprod_{y\in X} \mathrm{Trsp}_G(x,y)$$

Therefore

$$|G| = \sum_{y\in X} |\mathrm{Trsp}_G(x,y)| \underset{B+C}{=} \sum_{y\in X} |\mathrm{Stab}_G(x)| = |X||\mathrm{Stab}_G(x)| \quad \blacksquare$$

Theorem: Lagrange's Theorem

If G is a finite group and $H \leq G$, then $|G| = |H| \cdot |G/H|$.

Proof (Sketch)

Apply the Orbit-Stabilizer Theorem to $X = G/H$.
This action is transitive as $g(1H) = gH$.
Note $gH = H \iff g \in H$ and $g1 \in H$.
Therefore $\mathrm{Stab}_G(1H) = \{g \in G \mid g(1H) = 1H\} = H$.

Corollary

If $H \leq G$ and $|G| < \infty$, then $|H| \mid |G|$.
The converse is not true. No subgroup of order 6 in $\mathrm{Alt}(4)$ (where $|\mathrm{Alt}(4)| = 12$).

Definition: Conjugate

Let G be a group, $H \leq G$, $g \in G$.

1. For $x \in G$ the g-conjugate of x is $gxg^{-1} = {}^{g}x$.

2. The g-conjugate of H is $gHg^{-1} = {}^{g}H = \{gxg^{-1} \mid x \in H\}$.

Example

Let $G = \text{Alt}(4)$ and $H = \text{Stab}_G(B) = \{1, (P\ W\ Y), (P\ Y\ W)\}$. Then, for $g = (B\ Y\ P)$

$$gHg^{-1} = \{1, (B\ W\ P), (B\ P\ W)\} = \text{Stab}_G(Y)$$

$(B\ Y\ P)1(B\ P\ Y) = 1$
$(B\ Y\ P)(P\ W\ Y)(B\ P\ Y) = (B\ W\ P)$

$$\begin{array}{c}
\text{W} \leftarrow \text{W} \longleftarrow \text{P} \longleftarrow \text{B} \\
\text{B} \longleftarrow \text{P} \longleftarrow \text{Y} \longleftarrow \text{P} \\
\text{P} \longleftarrow \text{Y} \leftarrow \text{W} \leftarrow \text{W} \\
\text{Y} \longleftarrow \text{B} \longleftarrow \text{B} \longleftarrow \text{Y}
\end{array}$$

- Note: Shortcut
  $(gxg^{-1})^{-1} = (g^{-1})^{-1}x^{-1}g^{-1} = gx^{-1}g^{-1}$.
  Applying this to $g = (B\ Y\ P)$ with $x = (P\ W\ Y)$
  Therefore, from the previous calculation, $gx^{-1}g^{-1} = (gxg^{-1})^{-1} = (B\ P\ W)$.

Proposition: Geometric Meaning of Conjugate

Let G act on a set X, $x \in X$, $g \in G$, and define $y := g * x$.
Then for $H = \text{Stab}_G(x)$, we have

$$gHg^{-1} = \text{Stab}_G(y)$$

That is, the conjugate of a stabilizer is a stabilizer.

Proof

($\subseteq$) Let $ghg^{-1} \in gHg^{-1}$ be arbitrary.
Then

$$(ghg^{-1}) * y = g * (h * (g^{-1} * y)) = g * (h * x) = g * x = y$$

Therefore $ghg^{-1} \subseteq \text{Stab}_G(y)$.
($\supseteq$) Let $g' \in \text{Stab}_G(y)$ be arbitrary.
Consider $g^{-1}g'g$. Then

$$(g^{-1}g'g) * x = g^{-1} * (g' * (g * x)) = g^{-1} * (g' * y) = g^{-1} * y = x$$

Therefore $h := g^{-1}g'g \in H$. Then by multiplying g on the left and g^{-1} on the right, we get

$$g' = ghg^{-1} \in gHg^{-1}$$

Orbit-Stablizer Theorem and Lagrange

1. If G acts transitively on X, then all the stabilizers have the same cardinality because they are all conjugates. So the Orbit-Stabilizer Theorem is consistent.

2. If $X = G/H$, then $\text{Stab}_G(1H) = H$. What about $\text{Stab}_G(gH) = gHg^{-1}$?

October 12, 2023

Recall: Conjugate

$h \in G,\ H \le G, g \in G$
The conjugates $ghg^{-1} = {}^{g}h,\ gHg^{-1} = \{ghg^{-1} \mid h \in H\}$.

Meaning

If G acts on $X,\ x \in X,\ g \in G,\ g * x =: y,\ H = \mathrm{Stab}_G(x)$, then $gHg^{-1} = \mathrm{Stab}_G(y)$.

- Example
  $G = \mathrm{Alt}(4),\ x = B,\ H = \{1, (P\ W\ Y), (P\ Y\ W)\},\ g = (B\ P)(Y\ W)$
  gives $gHg^{-1} = \mathrm{Stab}_G(P) = \{1, (B\ W\ Y), (B\ Y\ W)\}$.

Definition: Cyclic Subgroup

The cyclic subgroup generated by g is given as $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\} = \{\ldots, g^{-2}, g^{-1}, 1, g, g^1, g^2, \ldots\}$.

Definition: Normal Subgroup

Let $H \le G$.
Say H is normal in G and write $H \trianglelefteq G$ if for all $g \in G,\ gHg^{-1} = H$.
Equivalently, $gH = Hg$ for all $g \in G$.

Trivial Example

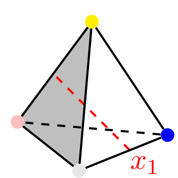
If $H = \{1\}$ ir $H = G$, then $H \trianglelefteq G$.

Example 1: Non-Normal Subgroup

$G = \mathrm{Alt}(4),\ H = \mathrm{Stab}_G(B)$ is not normal.

Example 2: Alternating Group

Consider $G = \mathrm{Alt}(4),\ X = \{x_1, x_2, x_3\}, H = \mathrm{Stab}_G(x_1)$.



Then we have the following facts.

- First: Transitivity
  G acts transitively.

- Second: Order of H
  By the Orbit-Stabilizer Theorem,

$$|H||X| = |G| \implies |H| \cdot 3 = 12 \implies |H| = 4$$

- Third: Description of G
  We know

$$G = \left\{1, \begin{pmatrix} 8 \\ \text{3-cycles} \end{pmatrix}, \begin{pmatrix} 3 \\ 2+\text{2-cycles} \end{pmatrix}\right\}$$

- Q: Can a 3-cycle belong to H?
  A: No. Lagrange's Theorem.
  Suppose a 3-cycle $g \in H$. Then the cyclic subgroup $\langle g \rangle = \{1, g, g^2\}$, but $\langle g \rangle \le H$ and $3 \nmid 4$.

- Fourth: Description of H
  By Lagrange's Theorem, $H \subseteq \left\{1, \binom{3}{\text{2+2-cycles}}\right\} \implies H = \left\{1, \binom{3}{\text{2+2-cycles}}\right\}$.

- Fifth: H is a Normal Subgroup
  Run the argument with x_1 replaced with x_2, then $\mathrm{Stab}_G(x_2) = H = \mathrm{Stab}_G(x_3)$.
  Therefore, $H \trianglelefteq G$.

Example 3: Non-Normal

From Homework 1, $\mathbb{P}_1(1)$, $H = \{A \in \mathrm{SL}_2\mathbb{C} \mid A^\dagger A = I_2\}$ is not normal.
$\mathbb{P}_1(2)$, $S = \{A = A^\dagger\} \ntrianglelefteq G$.

Example 4: SL As Kernel

$\mathrm{SL}_n(\mathbb{R}) = \ker(\det \mid \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^\times) \trianglelefteq \mathrm{GL}_n(\mathbb{R})$

Example 5: Alternating Group As Kernel

$\mathrm{Alt}(n) = \ker(\mathrm{sign} \mid \mathrm{Sym}(n) \to \{\pm 1\}) \trianglelefteq \mathrm{Sym}(n)$

- Proof
  Let $g \in G$ and $k \in K$ be arbitrary.
  We need to show that $gkg^{-1} \in K$.
  $\phi(gkg^{-1}) \underset{\phi \text{ homomorphism}}{=} \phi(g)\phi(k)\phi(g^{-1}) \underset{k \in K}{=} \phi(g)[\phi(g)]^{-1} = 1_H$.

Exercise 1

$\mathrm{Stab}_{\mathrm{Alt}(4)}(1 \text{ of the 6 edges}) \overset{?}{\trianglelefteq} \mathrm{Alt}(4)$.

Exercise 2

Can you have a subset closed under conjugation?
On Homework 2 we will examine conjugate classes.

Theorem: Quotient Group

Let $N \trianglelefteq G$. Then on G/N, we have a structure of a group, the quotient group, with the binary operation $g_1 N * g_2 N := (g_1 g_2)N$.
The identity element $1N = N$.
The inverse $(gN)^{-1} = g^{-1}N$.

Proof

The main difficulty is in demonstrating that $*$ is well-defined.
That is, if g_1', g_2' are other elements such that (1) $g_1'N = g_1N$ and (2) $g_2' = g_2N$, then we need to show that $(g_1g_2)N = (g_1'g_2')N$.
But (1) means that $g_1' = g_1n_1$ for some $n_1 \in N$, while (2) similarly means $g_2' = g_2n_2$ for $n_2 \in N$.
It follows that $g_1'g_2' = g_1n_1g_2n_2$.
Recall that $N \trianglelefteq G$ implies $Ng_2 = g_2N$, so $n_1g_2 = g_2n_3$ for some $n_3 \in N$.
Therefore $g_1n_1g_2n_2 = g_1g_2n_3n_2 \in N$.
Finally, multiplying N on the right side gives $(g_1g_2)N = (g_1'g_2')N$.

- Associativity
  Proof of associativity is left as an exercise.

Remark

If $H \leq G$ and $g_1H * g_2H \underset{\text{def}}{=} g_1g_2H$ defines (well) a group, then $H \trianglelefteq G$.

Proposition: Kernal Is Normal

Let $G \xrightarrow{\phi} H$ be a group homomorphism, then $K := \ker(\phi) = \{g \in G \mid \phi(g) = 1_H\}$ is a normal subgroup of G.

Proposition: Abelian Subgroups are Normal

If G is abelian, and $H \leq G$, then $H \trianglelefteq G$.

Proof

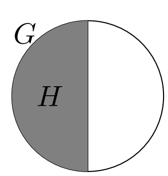
$ghg^{-1} = h$

Proposition: Subgroup of Index 2

Let $H \leq G$ of index 2 (i.e. $[G : H] = |G/H| = 2$), then $H \trianglelefteq G$.

Proof

Let $g \in G$ be arbitrary.
Need to show that o$gHg^{-1} = H$ or, equivalently, $gH = Hg$.
If $g \in H$, there is nothing to prove. So assume $g \notin H$.
But both gH and Hg are the (set) complement of H in G.



- Example
  $\mathrm{Alt}(n) \trianglelefteq \mathrm{Sym}(n)$
  If $n = 1$, there is nothing to prove.
  If $n \geq 2$, then $|\mathrm{Alt}(n)| = \frac{n!}{2} = \frac{|\mathrm{Sym}(n)|}{2}$.

Definition: Simple Group

A group G is simple if G has exactly 2 normal subgroups, namely $\{1\} \neq G$.

Non-Example

$G = \mathrm{Alt}(4) \trianglerighteq H = \mathrm{Stab}_G(x_1),\ H \neq \{1\}$ or G
So G is not simple.

Proposition: Group of Prime Order

Let p be a prime number.
Any group G of order p is both cyclic and simple.
$\mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{p-1}\}$ with $+$.

- Proof
  Suppose $g \in G$ is not the identity.
  Form $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\} =: H \leq G$.
  By Lagrange's Theorem, $|H||G| = p$. Since the only positive divisors of p are 1 and p, $\langle g \rangle = H = G$ for any $g \neq 1_G$.
  If $H \leq G$ is any normal subgroup, $|H| \mid |G|$ so $H = \{1\}$ or $H = G$.

Remarks*

For all $n \geq 5$, $\mathrm{Alt}(n)$ is a simple group.
This may be asked as a homework exercise.
If $p \geq 5$ is a prime, then $\mathrm{SL}_2(\mathbb{F}_p)/\{\pm I_2\}$ is a simple group.
Relatedly, if $n \geq 4$ then $\mathrm{SL}_n(\mathbb{F}_p)/Z(\mathrm{SL}_n(\mathbb{F}_p))$ is simple.
The point is that there are infinitely many finite simple groups.
Circa 1980, classification of finite simple groups was announced.
Requires $\sim 10^4$ pages (not everyone has been convinced).

Definition: Center

Let G be a group.
The center $Z(G) = \{z \in G \mid zg = gz,\ \forall g \in G\}$ is a normal subgroup ($gzg^{-1} = z, \forall g, z$).

More Group Action Terminology

Let G act on a set X.
Recall that this corresponds to a group homomorphism $G \xrightarrow{\rho} \mathrm{Sym}(x)$.

Definition: Faithful

Say the action is faifthful if $\ker(\rho) = \{1_G\}$.
$\forall g \in G:\ gx = x,\ \forall x \in X \implies g = 1_G$

Definition: Free

Say the action is free if $\forall g \in G,\ \forall x \in X,\ gx = x \implies g = 1_G$.
$\mathrm{Stab}_G(x) = \{1_G\},\ \forall x \in X$

Example 1

Let G act on $X = G$ by left multiplication. Then this is free.

Example 2

$G = \mathrm{Alt}(4)$
$X_1 = \{B, P, W, Y\}$ is faifthful but not free.
$X_2 = \{6 \text{ edges}\}$ is faifthful but not free.
$X_3 = \{3 \text{ strings}\}$ is not faithful.

October 17, 2023

Recall: Normal Subgroup

A subgroup $N \leq G$ is normal & $N \trianglelefteq G$, if $gNg^{-1} = N$ for all $g \in G$.

Notation

$G \xrightarrow{\pi} G/N$
$g \mapsto gN$

Recall: Quotient Group

We have constructed, for $N \trianglelefteq G$, the quotient group G/N, with $g_1N * g_2N = g_1g_2N$.

Definition: Group Homomorphisms

For groups G, K, $\mathrm{Hom}(G, K) = \{G \to K \mid \text{group homomorphisms}\}$.

Theorem: Universal Mapping Property of the Quotient Group

Let H be any group.

Part 1

For any group homomorphism $\overline{f} : G/N \to H$, by composing, we get a homomorphism

$$\overline{f} \circ \pi = f : G \xrightarrow{\pi} G/N \xrightarrow{\overline{f}} H$$

such that $f(N) = \{1_H\}$.

- Proof
  Let $\overline{f} \in \mathrm{Hom}(G/N, H)$ and $f := \overline{f} \circ \pi \in \mathrm{Hom}(G, H)$.
  Then

$$f(n) = \overline{f}(\pi(n)) = \overline{f}(nN) = \overline{f}(N) \underset{N \in G/N \text{ is the identity}}{=} 1_H$$

Part 2

Conversely, for any group homomorphism $f : G \to H$ such that $f(N) = \{1_H\}$ we get a unique homomorphism $\overline{f} : G/N \to H$ such that $f = \overline{f} \circ \pi$.

- Proof
  - Well Defined
    Let $f \in \text{Hom}(G,H)$ satisfy $f(N) = \{1_H\}$.
    Define $\overline{f}(gN) = f(g)$ for every $g \in G$.
    Need to Show: If $g_1N = g_2N$, then $f(g_1) = f(g_2)$.
    But $g_1N = g_2N$ implies, since $g_1 1_G \in g_1N$, that $g_1 = g_2 n$ for some $n \in N$.
    Since f is a group homomorphism, we have

    $$f(g_1) = f(g_2)f(n) \underset{f(N)=\{1_H\}}{=} f(g_2)1_H = f(g_2)$$

  - Homomorphism
    $\overline{f}$ is a homomorphism since for any $g_1N_1, g_2N_2 \in G/N$, we have

    $$\overline{f}(g_1N * g_2N) \underset{\text{definition of } *}{=} \overline{f}(g_1g_2N) \underset{\text{definition of } \overline{f}}{=} f(g_1g_2) \underset{f \text{ is homomorphism}}{=} f(g_1)f(g_2) \underset{\text{definition of } \overline{f}}{=} \overline{f}(g_1N)\overline{f}(g_2N$$

  - Uniqueness
    Suppose $l \in \text{Hom}(G/N,H)$ is any element satisfying $f = l \circ \pi$.
    Then for any $g \in G$, we have

    $$\overline{f}(gN) = f(g) = l(\pi(g)) = l(gN)$$

    Therefore $\overline{f} = l$.

Rephrase: Universal Mapping Property of Quotient Group

$\text{Hom}(G/N,H) \overset{1}{\underset{2}{\rightleftarrows}} \{f \in \text{Hom}(G,H) \mid f(N) = \{1_H\}\}$
Equivalently, $f(N) = \{1_H\} \iff N \leq \ker(f)$.
Note: $f(N) = \{1_H\} \iff N \subseteq f^{-1}(\{1_H\}) = \ker(f)$

Loosely: Universal Mapping Property of Quotient Group

Giving a homomorphism $G/N \to H$ is the same as giving a homomorphism $G \to H$ that kills N.

Definition: Group Generators

Let G be a group and let $S \subseteq G$.

Definition: Word

A word in S of length $l \geq 1$ is an expression $x_1x_2\cdots x_l$ where $x_i \in \{s, s^{-1}\}$ for some $s \in S$ and $i = 1, \ldots, l$.
The word of length zero is, by convention, 1_G.

Definition: Generated Subgroup

The subgroup generated by S, $\langle S \rangle$ is the subset of G consisting of all the words in S of all possible lengths.
Fact: $\langle S \rangle \leq G$.

- Example
  $S = \{A, C, I, T, L\}$.

One word in S of length 3 is $CA^{-1}T$.
Inverse: $(CA^{-1}T) = T^{-1}AC^{-1}$.
Composition: $CA^{-1}T * T^{-1}A^{-1}IL = CA^{-1}TT^{-1}A^{-1}IL = CA^{-2}IL$. (Note that, strictly, $A^{-2} \notin S$ but rather $A^{-2} \equiv A^{-1}A^{-1}$).

Common Usage

We usually do not use the bare definition to describe what $\langle S \rangle$.

- Example
  Let $G = \mathrm{Sym}(n)$ and let $S = \{\text{transpositions } (a\ b) \mid 1 \le a < b \le n\}$.
  Then $\langle S \rangle = G$.

  - Proof
    Step 1: Any $\pi \in G$ has a cycle decomposition. So $\pi = \gamma_1\gamma_2\cdots\gamma_k$, where γ_i is an l_i-cycle for some $l_i \ge 1$.
    Step 2: If γ is an l-cycle, $l \ge 2$, say $\gamma = (a_1\ a_2\ \cdots\ a_l)$, then $\gamma \overset{\text{HW1}}{=} (a_1\ a_2)(a_2\ a_3)\cdots(a_{l-1}\ a_l)$.

Definition: Commutator

A commutator in G is an element of the form $[g, h] := ghg^{-1}h^{-1}$ for some $g, h \in G$.

Definition: Commutator Subgroup

The commutator subgroup (or derived subgroup) $D(G)$ (sometimes $[G, G]$) is the subgroup of G generated by all the commutators.
That is, a typical element in $D(G)$ is $C_1C_2\cdots C_l$ where $C_i = [g_i, h_i]$ for some $g_i, h_i \in G, \forall i$.
Note that $[g, h]^{-1} = (ghg^{-1}h^{-1})^{-1} = hgh^{-1}g^{-1} = [h, g]$.

Proposition: Commutator Subgroup Is Normal

$D(G) \trianglelefteq G$.

Lemma:

Let $g_0 \in G$ be fixed.
The map $G \to G$ defined as $g \mapsto g_0gg_0^{-1}$ – called the inner homomorphism and denoted $\mathrm{Int}(g_0)$ – is a group homormorphism.

- Proof

$$\mathrm{Int}(g_0)(g_1g_2) = g_0g_1g_2g_0^{-1} = g_0g_1g_0^{-1}g_0g_2g_0^{1} = [\mathrm{Int}(g_0)(g_1)][\mathrm{Int}(g_0)(g_2)]$$

Proof

Let $g_0 \in G$ and $C_1\cdots C_l \in D(G)$ be arbitrary.

$$g_0(C_1\cdots C_l)g_0^{-1} = \mathrm{Int}(g_0)(C_1\cdots C_l) = \underset{\text{lemma}}{=} [\mathrm{Int}(g_0)(C_1)]\cdots[\mathrm{Int}(g_0)(C_l)]$$

It suffices to prove that $\mathrm{Int}(g_0)(C)$ is a commutator for any commutator C.

$$\mathrm{Int}(g_0)(C) = \mathrm{Int}(g_0)(ghg^{-1}h^{-1}) = [\mathrm{Int}(g_0)(g), \mathrm{Int}(g_0)(h)] \quad \blacksquare$$

Definition: Abelianization

The quotient group $G/D(G)$ is called the Abelianization G^{ab} of G.

Property: Commutativity

G^{ab} is commutative.

- Proof
  Let $D = D(G)$ and let $gD, hD \in G^{\text{ab}}$ be arbitrary.
  Then

$$[gD, hD] = (gD)(hD)(gD)^{-1}(hD)^{-1} = ghg^{-1}h^{-1}D = D = 1_{G^{\text{ab}}}$$

  Therefore, by multiplying on the right by $(hD)(gD)$, we get

$$(gD)(hD) = (hD)(gD)$$

  So G^{ab} is Abelian.

Note: Abelian Groups

G is Abelian if and only if $D(G) = \{1_G\}$.

Proposition: Minimal Normal Subgroup with Commutative Quotient

$D(G)$ is the smallest normal subgroup $N \trianglelefteq G$ such that G/N is commutative.

Proof

Suppose $N \trianglelefteq G$ has Abelian G/N.
Need to Show: $D(G) \leq N$.
So let $g, h \in G$ be arbitrary and let $C = ghg^{-1}h^{-1}$.
Then in G/N, $[gN, hN] = 1_{G/N} = N$.
Therefore $[g, h] \in N$ and $[G, G] \leq N$. ■

Remark*: Homology in Algebraic Topology

Let X be a connected manifold, say
IMAGE HERE - DOUBLE TORUS WITH CHUNK BEING REMOVED
In Algebraic Topology, we study loops up to homotopy $G = \pi_1(X, x_0)$.
Then $G^{\text{ab}} \underset{Hurewicz}{=} H_1(X; \mathbb{Z})$ is a homology.

Theorem: Universal Mapping Property of Abelianization

Let G be any group and H be any Abeian group.
Then we have a bijection $\text{Hom}(G, H) \rightleftarrows \text{Hom}(G^{\text{ab}}, H)$.

Proof

Since H is Abelian, any homomorphism $f : G \to H$ will satisfy $f([G, G]) = \{1_H\}$.
So use UMP for quotient G/N. ■

October 19, 2023

Review: Commutator

Let G be a group.
A commutator is an element of the form $[g, h] = ghg^{-1}h^{-1}$.
The derived (or commutator) subgroup $DG = [G, G]$ is the subgroup generated by all the commutators.

Properties of Commutators

$DG \trianglelefteq G$
$G^{\text{ab}} := G/DG$ is abelian.
G^{ab} satisfies the universal mapping property. That is, for all abelian H.

$$\mathrm{Hom}(G, H) \leftrightarrows \mathrm{Hom}(G^{\text{ab}}, H)$$

Example: G Abelian

If G is abelian, then $D(G) = \{1_g\}$ and $G \xrightarrow{\sim} G^{\text{ab}} = G/\{1_G\}$ (usually written $G = G^{\text{ab}}$).
Conversely, $DG = \{1_G\}$ implies G is abelian.

Example: G Simple and Non-abelian

If G is simple and non-abelian, then $DG = G$.

Definition: Perfect Group

A group G is called perfect if $D(G) = G$.
cf. Poincaré Conjecture (Perelmon circa 2002: Every closed 3-manifold M with $\pi_1(M) = \{1\}$ is homeomorphic to S^3.

Example: G Symmetric Group 3

Let $G = \mathrm{Sym}(3)$.
By Lagrange, if $H \leq G$, then $|H| \mid |G| = 3! = 6$. Consider

$$|H| = 1, 2, 3, \text{ or } 6$$

Then

$$\begin{tikzcd}[column sep=small]
 & & \mathrm{Sym}(3) \arrow[dll, dash] \arrow[dl, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
\langle(1\ 2)\rangle & \langle(2\ 3)\rangle & & \langle(1\ 3)\rangle & \langle(1\ 2\ 3)\rangle \\
 & & \{1\} \arrow[ull, dash] \arrow[ul, dash] \arrow[ur, dash] \arrow[urr, dash] & &
\end{tikzcd}$$

Which one is DG?
It cannot be $\{1\}$ since $G \neq G^{\text{ab}}$.
It cannot be $\langle\tau\rangle, \tau^2 = 1$, since they are not normal.
$G/\langle(1\ 2\ 3)\rangle$ is a group of order 2 and, therefore, abelian.

Recall

DG is the smallest normal subgroup N of G such that G/N is abelian.

Therefore, $DG = D(\mathrm{Sym}(3)) = \langle (1\ 2\ 3) \rangle$.

Note

For $G = \mathrm{Sym}(3)$,

$$G \underset{\neq}{>} D(G) = \langle (1\ 2\ 3) \rangle \underset{\neq}{>} D(D(G)) = \{1\}$$

Definition: Solvable Group

Suppose G is a group such that

$$D(D(D(\cdots D(G)\cdots) = \{1\}$$

Then G is solvable (or soluble).

Definition: Conjugacy Class

The conjugacy class of $\in G$ is the set of elements in G that are conjugate to $\overline{x}$.
Let G act on (the set) $G = X$ by conjugation: $g * x = gxg^{-1}$.
Then the conjugacy class of x is the G-orbit of $x \in X$.

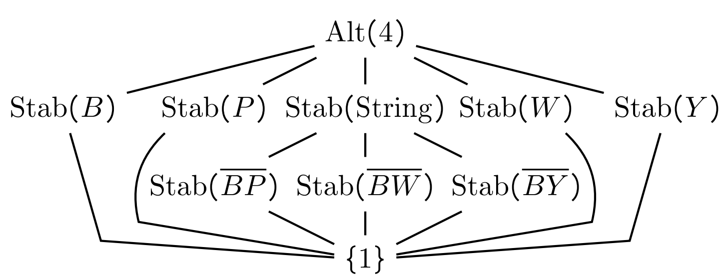
Definition: Centralizer

The centralizer $x \in G$ is the stabilizer of x in this conjugation cation.

$$C_G(x) = \{g \in G \mid gxg^{-1} = x\} \iff gx = xg$$

Example: G Alternating Group 4

Let $G = \mathrm{Alt}(4)$.
Then, by Lagrange, $H \leq G \implies |H| \mid |G| = 12$.
So $|H| = 1, 2, 3, 4, 6,$ or 12



Note: Stab(String) refers to the stabilizer of x_1 as depicted in Example 2 on page 19.

Proposition: No Order 6 Subgroup

No subgroup H of order 6 in AAlt(4).

- Proof
  Suppose $H \leq G$ has order six.
  Then $[G : H] = \frac{12}{6} = 2$ and, therefore, $H \trianglelefteq G$.
  So H must be a union of certain conjugacy classes.
  From Homework 1, G acts transitively on {6 edges}, so Stab($\overline{BP}$), Stab($\overline{BW}$),and Stab($\overline{BY}$) are conjugate to each other (HW2 P1(b)).
  Therefore the 3 elements of order 2, $T = \{(B\ P)(W\ Y), (B\ W)(P\ Y), (B\ Y)(P\ W)\}$ form a conjugacy class in G
  It follows that $G = \{1\} \coprod T \coprod$ {8 elments of order 3}.
  By the following lemma, this resolves to

$$G = \{1\} \coprod T \coprod \{p\}^{\#} \coprod \{p^2\}^{\#}$$

- Lemma (Key)
  Every element p of order 3 in $G = \mathrm{Alt}(4)$ has conjugacy class of size 4.

  - Proof
    |(conjugacy class of $p| \geq 4$ since G acts transitively on $\{B, P, W, Y\}$ and $\exists p \in \mathrm{Stab}(P)$ such that, without loss of generality, $gpg^{-1} = \mathrm{Stab}(B)$.
    Since $p = 1$ implies $gpg^{-1} = 1$, each g sends non-trivial p to either $(P\ W\ Y)$ or $(P\ Y\ W)$ in Stab(B).
    Then, also

$$|(\text{conjugacy class of } p| = |\text{orbit of } p \text{ under the conjugation action}| = |G|/|C_G(p)| \leq 12/3 = 4$$

    Therefore no normal group of order 6 is in $G = \mathrm{Alt}(4)$.

Example Continued: 6 Alternating Group 4

{1} is non-abelian.
Stab($\overline{BP}$) inhabits a conjugate class.
Because $|G/\,\mathrm{Stab(String)}| = 3$ it is cyclic and $DG = \{1\} \coprod T$
Observe that DG is abelian.

Proof

What to Show: For $t = (B\ P)(W\ Y)$ and every $t \in T$, $C_G(t) \supseteq DG$.
Then

$$|C_G(T)| \underset{OST}{=} \frac{|G|}{|T|} = \frac{12}{3} = 4$$

Therefore, $C_G(t) = DG$.

Remark: Enumerability of Subgroups

There are very few groups G such that we can enumerate all the subgroups of G.

Theorem: Product of Integers is a Subgroup

Let $G = (\mathbb{Z}, +)$.

1. For any $a \in \mathbb{Z}$, the subset $a\mathbb{Z} = \{an \mid n \in \mathbb{Z}\}$ is a subgroup of G.

2. Conversely, any subgroup $H \leq \mathbb{Z}$ is of the form $H = a\mathbb{Z}$ for some $a \in G$.

Proof of 1

Need to Show: $a\mathbb{Z}$ contains 0, is closed under + and is closed under (additive) inverse.
But, $0 = a0$, and $an + am = a(n+m)$ and $-(an) = a(-n)$, for $n, m \in \mathbb{Z}$.

Proof of 2

Suppose $H \leq (\mathbb{Z}, +)$.
Since + is commutative, all subgroups will be normal.
If $H = \{0\}$, then $h = 0\mathbb{Z}$, and we're done.
If not, say $H \ni x \neq 0$, then $h \ni -x$.
Therefore $S = \{x \in H \mid x > 0\}$ must be non-empty.
Let a be the smallest element in S.
Then we claim $H = a\mathbb{Z}$.

- Proof of the Claim
  ($\supseteq$) Since $H \ni a$ and $H \leq G$.
  ($\subseteq$) Let $x \in H$ be arbitrary. Apply Division Algorithm and get

  $$x = aq + r$$

  where $q, r \in \mathbb{Z}$ and $0 \leq r \leq a$.
  If $r > 0$, then

  $$r = x - aq \in H$$

  so $r \in S$.
  However, since $r < a$, this contradicts the very choice of a as the smallest element.
  So $r = 0$.
  But then $x = aq \in a\mathbb{Z}$.
  Therefore $H \subseteq a\mathbb{Z}$. ■

Homework 2 Question

If $H \leq G$, then $gHg^{-1} \leq G$.
Consider the set X_G of all the subgroups H of G.
The group G acts on X_G by conjugation: $g * H := gHg^{-1}$.

Definition: Normalizer

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

October 24, 2023

Isomorphism Theorems

Definition: Isomorphism

An isomorphism between two groups, G and H, is a group homomorphism $f : G \to H$ that is bijective.
Two groups are said to be isomorphic if there is an isomorphism between them.

Example

Let G be any group, $N = \{1_G\}$, and let $\pi : G \to G/N$ be the canonical projetion.
Then $gN = \{g\}, \forall g \in G$.
So π is an isomorphism.
e.g. for $G = \{1, a, b, c\}$
$G/\{1_G\} = \{\{1\}, \{a\}, \{b\}, \{c\}\}$
1 - {1}
a - {a}
b - {b}
c - {c}
Here we will write $G = G/\{1_G\}$.

Lemma:

Let $G \xrightarrow{\phi} H$ be a group homomorphism.
Suppose ϕ is surjective. Form $K = \ker(\phi) \leq G$.
Then we have an isomorphism, induced by ϕ:

$$\overline{\phi} : G/K \to H$$

Proof

Giving $\overline{\phi}$ is the same as giving a homomorphism $G \xrightarrow{\psi} H$ such that $\psi(K) = \{1_H\}$ by the Universal Mapping Property.
So take $\psi = \phi$.
So have a group homomorphism $\overline{\phi}(gK) = \phi(g), \forall g \in G$.

$$\begin{tikzcd}
G \arrow[rr, "\phi"] \arrow[dr, "\pi"'] & & H \\
& K \arrow[ur, "\overline{\phi}"'] &
\end{tikzcd}$$

Set Theory

ϕ surjective $\implies \overline{\phi}$ surjective.
Remains to show: $\overline{\phi}$ is injective.
Let $g_1K, g_2K \in G/K$such that $\overline{\phi}(g_1K) = \overline{\phi}(g_2K)$.
Then, by definition of $\overline{\phi}$,

$$\phi(g_1) = \phi(g_2)$$

So

$$\phi(g_1 g_2^{-1}) \underset{\phi \text{ homomorphism}}{=} \phi(g_1\phi(g_2^{-1}) = 1_H.$$

Therefore $g_1 g_2^{-1} \in \ker(\phi) = K$ and $g_1K = g_2K$. ■

Definition: Normalizer (Revisited)

Let $H \leq G$. The normalizer $N_G(H)$ is $\{g \in G \mid gHg^{-1} = H\}$.

Note: Normalizer is a Stabilizer

It is the stabilizer of H in the conjugation action of G on the set of all subgroups of G.
Since $\forall h \in H$, we have $hHh^{-1} = H$, we have $H \leq N_G(H)$.
Since $N_G(H)$ is a stabilizer, $N_G(G) \leq G$.
Therefore $H \leq N_G(H) \leq G$.
$H \leq N_G(H) \leq G$.

Note: H is Normal If the Normalizer of H is G

$H \trianglelefteq G \iff N_G(H) = G$.

Example 1

Let $G = \mathrm{Alt}(4)$, $K_1 = \mathrm{Stab}_G(B) = \langle (P\ W\ Y)\rangle$, and $H_1 = \langle (B\ P)(W\ Y)\rangle$.
Question: What are $N_G(H_1)$ and $N_G(K_1)$?

- H1
  H_1 is not normal in G, so $N_G(H_1) \neq G$.
  Since $H_1 \leq N_G(H_1) \leq G$.
  Recall that $H_1 \leq \mathrm{Stab}_G(\text{String}) \leq G$ and $\mathrm{Stab}_G(\text{String})$ is abelian.
  Therefore $N_G(H_1) = \mathrm{Stab}_G(\text{String})$.
  Note also: $N_G(\mathrm{Stab}_G(\text{String})) = G$.

- K1
  From homework, $\forall g \in G$, $gK_1g^{-1} = \mathrm{Stab}_G(gB)$ and, if $gB \neq B$, then $\mathrm{Stab}_G(gB) \neq K_1$.
  So $K_1 \leq N_G(K_1) \subseteq \mathrm{Stab}_G(B) = K_1$.
  That is, $N_G(K_1) = K_1$. It is a "self-normalizer."

Example 2

Let $G = \mathrm{GL}_2(\mathbb{R})$, $H = \left\{\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \mid x \in \mathbb{R}\right\}$.
What is $N_G(H)$?
Say $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ belongs to $N_G(H)$.
Then $g\begin{pmatrix} 1 & 3 \\ 0 & -1 \end{pmatrix}g^{-1} \in H$. Say

$$g\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}g^{-1} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$

for some $x \in \mathbb{R}$. Then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$\begin{pmatrix} a & b+3a \\ c & d+3c \end{pmatrix} = \begin{pmatrix} a+xc & b+xd \\ c & d \end{pmatrix}$$

Therefore, $c = 0$ (and $x = \frac{3a}{d}$). So

$$N_G(H) \le \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, d \in \mathbb{R}^+, b \in \mathbb{R} \right\}$$

Are they equal?

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}^{-1} = \begin{pmatrix} a & b+ax \\ 0 & d \end{pmatrix}\frac{1}{ad}\begin{pmatrix} d & -b \\ 0 & a \end{pmatrix} = \begin{pmatrix} 1 & ? \\ 0 & 1 \end{pmatrix} \in H$$

Therefore, for $g = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, $gHg^{-1} \in H$.

Now, apply the same argument to $g^{-1} = \begin{pmatrix} 1/a & -b/ad \\ 0 & 1/d \end{pmatrix}$ and get $g^{-1}Hg \subseteq H$.

That is to say, $H \subseteq gHg^{-1}$.
It follows that $(A) + (B) \implies g \in N_G(H)$, and

$$N_{\mathrm{GL}_2(\mathbb{R})}\left(\left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \mid x \in \mathbb{R} \right\} \right) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, d \in \mathbb{R}^+, b \in \mathbb{R} \right\}$$

Definition: Product

Let $H, K \le G$.
Then $HK := \{hk \mid h \in H, k \in K\}$
HK need not be a subgroup, and may differ from KH.

Example

Let $G = \mathrm{Alt}(4)$, $H = \langle (B\ P)(W\ Y) \rangle$, and $K = \langle (P\ W\ Y) \rangle$.
Note $|H| = 2$ and $|K| = 3$. Then

$$HK = \{1 \cdot 1, 1(P\ W\ Y), 1(P\ Y\ W), (B\ P)(W\ Y)1, (B\ P)(W\ Y)(P\ W\ Y), (B\ P)(W\ Y)(P\ Y\ W)\}$$

Fact

If $H, K \le G$ such that $H \cap K = \{1_G\}$ and $h_1, h_2 \in H$ and $k_1, k_2 \in K$, then

$$h_1 k_1 = h_2 k_2 \implies h_1 = h_2 \text{ and } k_1 = k_2$$

Proof

Multiply h_2^{-1} on the left and k_1^{-1} on the right. Then

$$H \ni h_2^{-1} h_1 = k_2 k_1^{-1} \in H \quad \blacksquare$$

Therefore $|HK| = 6$.
Since G contains no subgroup of order 6, $HK \not\le G$.

Theoren: First Isomorphism Theorem

Note: Dummit and Foote lists this as the Second Isomorphism Theorem.
Let $H, K \leq G$ and assume that $H \leq N_G(K)$,

1. $HK = KH$ is a subgroup of G,
2. $K \trianglelefteq HK$ and $H \cap K \trianglelefteq H$, and
3. $HK/K \xleftarrow{\sim} H/H \cap K$ is an isomorphism of (quotient) groups.

Proof of 1

- Equality
  Need to prove $HK \subseteq KH$ and $KH \subseteq HK$.
  $(\Longrightarrow)$ Let $h \in H$ and $k \in K$. We want $hk \in KH$.
  Since $h \in \mathbb{N}_G(K)$, $hKh^{-1} = K$.
  So, in particular, $hkh^{-1} \in k_2$ for some $k_2 \in K$. Multiplying by h on the right,
  $$hk = k_2h \in KH$$
  $(\Longleftarrow)$ Let $kh \in HK$.
  Since $H \in N_G(K)$ and $N_G(K)$ is a subgroup, $h^{-1} \in N_G(K)$.
  So $h^{-1}K(h^{-1})^{-1} = K$.
  In particular, $h^{-1}kh = k_3$ for some $k_3 \in K$. So
  $$kh = h_{k3} \in HK$$
- Subgroup
  Identity: $1 = 1 \cdot 1 \in HK$
  Product: Let h_1k_1 and h_2k_2 be arbitrary. Then for some $h_4 \in H, k_4 \in K$
  $$(h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2 \underset{KH=HK}{=} h_1(h_4k_4)k_2 = (\overset{\in H}{h_1k_4})(\overset{\in K}{k_4k_2}) \in HK$$
  So HK is closed under the group operation.
  Inverse: $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$.

Proof of 2

- K is Normal in HK
  Let $hk \in HK$ be arbitrary.
  Since $h \in H \leq N_G(K)$, $k \in K \leq N_G(K)$, and $N_G(K)$ is a subgroup,
  $$hk \in N_G(K)$$
  Therefore $HK \leq N_G(K)$ and K is normal in HK.
- H Meet K is Normal in H
  For $h \in H$, $hKh^{-1} = K$ by assumption, and $hHh^{-1} = H$.
  Therefore $h(H \cap K)h^{-1} = H \cap K$, and $K \cap H$ is normal in H.

Proof of 3

Let us start with the inclusion homomorphism

$$
\begin{tikzcd}
h \arrow[r, mapsto] & h \cdot 1 \arrow[r, mapsto] & hK \\
H \arrow[r] \arrow[rr, bend right, "\phi"'] & HK \arrow[r] & HK/K
\end{tikzcd}
$$

ϕ is surjective.
A typical element in HK/K is $hkK = hK$ which is the image of $h \in H$ under ϕ.
Then $\ker(\phi) = \{h \in H \mid hK = 1_K\} \iff h \in K$. This is $H \cap K$.
Therefore, by lemma, $H/H \cap K \xrightarrow[\sim]{\overline{\phi}} HK/K$.

Example

Let $G = \mathrm{GL}_3(\mathbb{R})$ and $H = \left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \mid x, y, z \in \mathbb{R} \right\}$.$H \leq G$ called the Heisenberg group of dimension .

October 26, 2023

Heisenberg Groups

$$G = \mathrm{Heis}_3(\mathbb{R}) = \left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \mid x, y, z \in \mathbb{R} \right\} \leq \mathrm{GL}_3(\mathbb{R})$$

Subgroup

1. $I_3 \in G$ since we can take $x = y = z = 0$.

2. (Empty elements are read as zeros.)

$$\underbrace{\begin{pmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{pmatrix}}_{=g} \underbrace{\begin{pmatrix} 1 & a & c \\ & 1 & b \\ & & 1 \end{pmatrix}}_{=h} \begin{pmatrix} 1 & x+a & z+c+xb \\ & 1 & y+b \\ & & 1 \end{pmatrix}$$

So closed under matrix multiplication.
Note: (the $(1,2)$-component of gh) = (the $(1,2)$-component of g) + (the $(1,2)$-component of h).
Ditto for the $(2,3)$-component.

1. G is closed under inverse.

Let $a = -x$, $b = -y$ and $c = -z + xy$. Then

$$\begin{pmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -x & xy - x \\ & 1 & -y \\ & & 1 \end{pmatrix} \in G$$

Example

Identify $\mathbb{R}^3 = \left\{ \begin{bmatrix} x \\ y \\ z \end{bmatrix} \right\}$ with G and let G act on $\mathbb{R}^3 = X$ by left multiplication. i.e.

$$g = \begin{pmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} x \\ y \\ z \end{pmatrix} \rightsquigarrow g * \vec{v} = \begin{pmatrix} 1 & a & c \\ & 1 & b \\ & & 1 \end{pmatrix} \begin{pmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{pmatrix} = \cdots$$

For example, if

$$\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \leftrightarrow I_3 \quad \text{and} \quad g = \begin{pmatrix} 1 & 0 & 0 \\ & 1 & z \\ & & 1 \end{pmatrix}$$

then g maps $\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ to $\begin{pmatrix} 0 \\ 2 \\ 0 \end{pmatrix}$ while

$$h = \begin{pmatrix} 1 & 3 & 0 \\ & 1 & 0 \\ & & 1 \end{pmatrix} \quad \text{maps} \quad \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \quad \text{to} \quad \begin{pmatrix} 3 \\ 0 \\ 0 \end{pmatrix}.$$

However, since this is a noncommutative group

$$gh = \begin{pmatrix} 1 & 3 & 0 \\ & 1 & 2 \\ & & 1 \end{pmatrix} \quad \text{maps} \quad \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \quad \text{to} \quad \begin{pmatrix} 3 \\ 2 \\ 0 \end{pmatrix}$$

$$hg = \begin{pmatrix} 1 & 3 & 0 \\ & 1 & 0 \\ & & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ & 1 & 2 \\ & & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 6 \\ & 1 & 2 \\ & & 1 \end{pmatrix}$$

So hg maps $\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ to $\begin{pmatrix} 3 \\ 2 \\ 6 \end{pmatrix}$.

So G acts on $\mathbb{R}^3$ transitively and freely.

This is one of the eight "model geometries" of William Thurston.

Heisenberg Group Center and Derived Group

Recall

The center

$$Z(G) = \{ g \in G \mid gh = hg, \forall h \in G \}$$

and the derived group

$$D(G) = \langle \{ [g, h] \mid g, h \in G \} \rangle.$$

Center of Heisenberg Group

If

$$g = \begin{pmatrix} 1 & a & c \\ & 1 & b \\ & & 1 \end{pmatrix} \in Z(G),$$

then for any $x, y, z \in \mathbb{R}$, we have

$$\begin{pmatrix} 1 & a & c \\ & 1 & b \\ & & 1 \end{pmatrix} \overbrace{\begin{pmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{pmatrix}}^{=h} = \begin{pmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{pmatrix} \begin{pmatrix} 1 & a & c \\ & 1 & b \\ & & 1 \end{pmatrix}$$
$$\begin{pmatrix} 1 & a+x & c+z+ay \\ & 1 & b+y \\ & & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+a & z+c+xb \\ & 1 & y+b \\ & & 1 \end{pmatrix}$$

Therefore $ay = xb$ for all $x, y, z \in \mathbb{R}$.
Take $(x, y) = (1, 0)$, and we get $0 = b$.
Take $(x, y) = (0, 1)$, and we get $a = 0$.
It follows that

$$Z(G) = \left\{ \begin{pmatrix} 1 & 0 & c \\ & 1 & 0 \\ & & 1 \end{pmatrix} \mid c \in \mathbb{R} \right\}$$

Derived Group of Heisenberg Group

$[g, h] = ghg^{-1}h^{-1}$ has

$$(1,2) - \text{component} = a + x + (-a) + (-x) = 0$$
$$(2,3) - \text{component} = b + y + (-b) + (-y) = 0$$

So $D(G) \leq Z(G)$ for this G.

- Q: Is the center a subgroup of the derived group?
  Form

  $$G/Z(G) \xleftarrow[\phi]{\sim} (R^2, +)$$
  $$\begin{pmatrix} 1 & a & 0 \\ & 1 & b \\ & & 1 \end{pmatrix} Z(G) \longleftarrow (a, b)$$

  ϕ is a group homomorphism since the $(1,2)$-component and $(2,3)$ component of gh are the sum of those components in g and h.
  ϕ is surjective, since

$$\begin{pmatrix} 1 & a & c \\ & 1 & b \\ & & 1 \end{pmatrix} Z(G) = \begin{pmatrix} 1 & a & 0 \\ & 1 & b \\ & & 1 \end{pmatrix} Z(G)$$

where the matrix on either side differ by only an element in $Z(G)$.
ϕ is injective, since if

$$\phi(a,b) = \begin{pmatrix} 1 & a & o \\ & 1 & b \\ & & 1 \end{pmatrix} \in Z(G)$$

, then $a = b = 0$. So $(a,b) = 0$ in $\mathbb{R}^2$.
This is a cool isomorphism, but it only demonstrates $D(G) \le Z(G)$.

- Q: Is the center a subgroup of the derived group? (Take Two)

$$\begin{aligned} \begin{pmatrix} 1 & 1 & \\ & 1 & \\ & & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & \\ & 1 & c \\ & & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 & \\ & 1 & \\ & & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & \\ & 1 & \\ & & -c \end{pmatrix} &= \begin{pmatrix} 1 & 1 & c \\ & 1 & c \\ & & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 & c \\ & 1 & -c \\ & & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & c \\ & 1 & 0 \\ & & 1 \end{pmatrix} \end{aligned}$$

Therefore $Z(G) = D(G)$.

Theorem: Correspondence + 2nd Isomorphism Theorem

Let $N \trianglelefteq G$, $E_1 = \{H \le G \mid H \ge N\}$ (subgroup of G containing N), $E_2 = \{K \le G/N\}$ (subgroups of the quotient group).
Further, let $\pi : G \to G/N$ be the canonical projection homomorphism.
Then E_1 and E_2 are in bijection by

$$\Phi : E_1 \to E_2 \text{ given by } \Phi(H) = \pi(H)$$
$$\Psi : E_2 \to E_1 \text{ given by } \Psi(K) = \pi^{-1}(K)$$

1. Φ and Ψ preserve inclusion (i.e. $H_1 \le H_2$ in E_1 implies $H_1/N \le H_2/N$, and vice versa).

2. Φ and Ψ preserve normality (i.e. $H \trianglelefteq G$ in E_1 implies $H/N \trianglelefteq G/N$).

3. For any $H \in E_1$ that is normal in G, $G/H \cong (G/N)/(H/N)$ as groups.

General Fact

If $\phi : G_1 \to G_2$ is any homomorphism of groups, then $\begin{cases} H_1 \le G_1 \implies \phi(H_1) \le G_2 \\ H_2 \le G_2 \implies \phi^{-1}(H_2) \le G_1 \end{cases}$.

So Φ and Ψ are well-defined.

- Proof of Second Fact
  1. $1_{G_1} \in \phi^{-1}(H_2)$, since $\phi(1_{G_1}) = 1_{G_2} \in H$.
  2. If $g_1, g_1' \in \phi^{-1}(H_2)$, then $\phi(g_1 g_1') = \phi(g_1)\phi(g_1') \in H_2$ since H_2 is closed under product.
  3. If $g_1 \in \phi^{-1}(H_2)$, then $g_1^{-1} \in \phi^{-1}(H_2)$ similarly.

Proof of 1

Say $H_1, H_2 \in E_1$ such that $H_1 \leq H_2$.
Then $\Phi(H_1) = \{h_1 N \mid h_1 \in H_1\} \subseteq \{h_2 N \mid h_2 \in H_2\} = \phi(H_2)$.
Similarly, $K_1 \leq K_2 \in H_2$ implies $\Psi(K_1) \leq \Psi(K_2)$.

Proof of 2

Suppose $H \in E_1$ and $H \trianglelefteq G$. We want to prove that $\Phi(H) = H/N$ is normal in G/N.
So let gN be an arbitrary element in G/N, then $\forall h \in H$ we have

$$(gN)(hN)(gN)^{-1} = ghg^{-1}N \leq H/N = \Phi(H)$$

Let $h \in H$ vary, and we get

$$(gN)(H/N)(gN)^{-1} \subseteq H/N$$

Run the argument with g replaced by g^{-1},

$$(g^{-1}N)(H/N)(g^{-1}N)^{-1} = (gN)^{-1}(H/N)(gN) \subseteq H/N$$

hence

$$H/N \subseteq (gN)(h/N)(gN)^{-1}.$$

Therefore, gN normalizes $H/N = \Phi(H)$.

Proof of 3

1.

Start with $G \xrightarrow{\pi'} G/H$. As a canonical projection, π' is surjective.
That is $g \longmapsto \pi'(g) = gH$, and $\pi'(N) = \{1_{G/H}\}$ since for all $n \in N$, $n \in H$ so $nH = H$.

1.

By the Universal Mapping Property of G/N, we get a unique homomorphism

$$\begin{tikzcd} & G \arrow[dl, "\pi"'] \arrow[dr, "\pi'"] & \\ G/N \arrow[rr, "\pi''"] & & G/H \\ gN \arrow[rr, mapsto] & & gH \end{tikzcd}$$

where π'' is surjective.

- Recall: 0th Isomorphism Theorem

If $\phi : G_1 \to G_2$ is a surjective homomorphism of groups, then $\overline{\phi} : G_1/\ker(\phi) \xrightarrow{\sim} G_2$ is an isomorphism. Apply this to $\pi'' = \phi$.

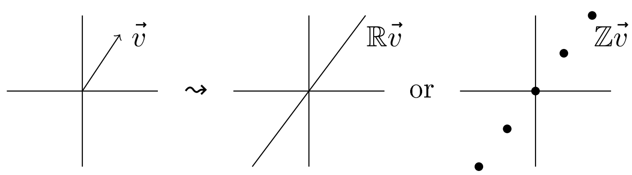
$$\begin{aligned}\ker(\pi'') &= \{gN \in G/N \mid gH = H\} \iff g \in H \\ &= \{hN \mid h \in H\} \\ &= H/N\end{aligned}$$

Therefore $(G/N)/(H/N) \xrightarrow{\sim} G/H$.

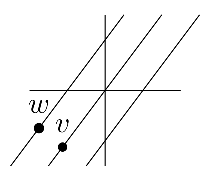
Example 1

Let $G = \mathrm{Heis}_3(\mathbb{R})$ and $N = Z(G) = D(G)$.
Some interesting subgroups of $(\mathbb{R}^2, +)$ are

1. $\{0\}$
2. $\vec{v} \neq \vec{0} \rightsquigarrow \mathbb{R}\vec{v}$ and $\mathbb{Z}\vec{v}$ are subgroups.



3. Say $\vec{v}, \vec{w}$ are linear independent. $\mathbb{Z}\vec{v} + \mathbb{R}\vec{w}$.



4. IMAGE HERE - LEGIT NO IDEA. Collection of vertical lines in $\mathbb{R}^3$ that form inverse of example 2?

October 31, 2023

Definition: Subnormal Series

Let G be a group.
A subnormal series (or filtration) of G is a series

$$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_l = \{1\}$$

of subgroups of G, such that $G_i \trianglerighteq G_{i+1}$ for all $i = 0, \ldots, l-1$.
The length of the filtration is l.

Definition: Normal Series

If each G_i is normal in G, we say the the series is normal.

Definition: Factor Group

The quotient group G_i/G_{i+1} is called the ith factor group of the filtration.
This is often denoted $\mathrm{gr}_i(G.)$ meaning "graded."

Definition: Composition Series

If, for each $i = 0, \ldots, l-1$, $\mathrm{gr}_i(G.)$ is simple, then we say the filtration is a composition series (or a Jordan-Hölder series).

Example 1

Let $G = \mathrm{Alt}(4)$.
Take $G_1 = D(G) = \mathrm{Stab}_G(\mathrm{String})$. (Recall $|G_1| = 4$.
Take $G_2 = \{1\}$.
Then $G = G_0 = G_1 \trianglerighteq G_2$ is a filtration.
It is a normal series.
G_0/G_1 is a cyclic group of order 3 and, hence, simple.
$G_1/G_2 = G_1$ (strictly isomorphic; this is an abuse of notation) has order 4, is abelian, and contains $\langle (B\ P)(W\ Y) \rangle$ as a proper subgroup. So $G.$ is not a JH series (composition series).

Example 2

Let $G = \mathrm{Alt}(4)$, $H_1 = G_1 = D(G)$, $H_2 = \langle (B\ P)(W\ Y) \rangle$ and $H_3 = \{1\}$.
Then,

$$G = H_0 \trianglerighteq H_1 \trianglerighteq H_2 \trianglerighteq H_3$$

is a subnormal series.
It is not a normal series, since H_2 is not normal in G.
It is a JH series, since H_0/H_1, H_1/H_2, and H_2/H_3 have orders 3, 2 and 2 respectively and, therefore, are all simple.

Proposition:

Every finite group G has at least one Jordan-Hölder Series.

Proof

By induction on $|G|$.
If $|G| = 1$, then, by convention, (G) is a JH series of length 0.
Suppose $|G| > 1$.
If G is simple (i.e. G has exactly 2 normal subgroups, namely $\{1\}$ and G), then

$$(\ G = G_0 \trianglerighteq \{1\} = G_1\ )$$

is a JH series of length 1.
Suppose G is not simple.
Then G contains a normal subgroup N, $N \neq \{1\}$ and $G \neq G$.
Among all such nontrivial proper normal $N \trianglelefteq G$, choose the one with maximal $|N|$.
Then $Q := G/N$ is simple since, by the 2nd isomorphism theorem, if Q were not simple, it would contain a

nontrivial proper normal subgroup $Q_1 \underset{\neq}{\lhd} Q$, which would correspond to a normal subgroup $N \underset{\neq}{\lhd} N_1 \underset{\neq}{\lhd} G$, but then $|N_1| > |N|$, which would contradict the choice of N.
By induction hypothesis, $|N| < |G|$, we have a JH series for N, say

$$N = N_0 \trianglerighteq N_1 \trianglerighteq \cdots \trianglerighteq N_l = \{1\}$$

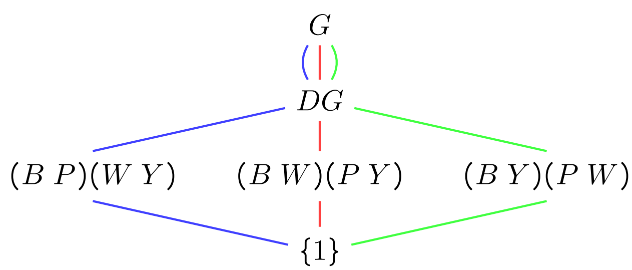
Then take $G_0 = G$ and $G_{i+1} = N_i$ for $i = 0, 1, 2, \ldots, l$ to get

$$G = \underbrace{G_0 \trianglerighteq N_0}_{Q} \trianglerighteq N_1 \trianglerighteq \cdots \trianglerighteq N_l = \{1\}$$

which have simple factors.
Therefore, $N.$ is a JH series. ■

Example 1

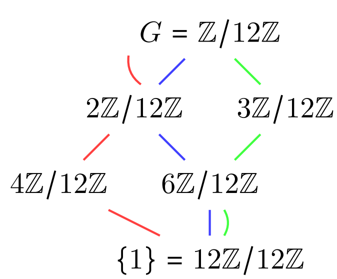
For $G = \mathrm{Alt}(4)$,



has 3 JH series.

Example 2

For $G = \mathbb{Z}/12\mathbb{Z}$.
Fact: by the 2nd isomorphism theorem, subgroups of G are exactly $a\mathbb{Z}/12\mathbb{Z}$ where $a \mid 12$.
($\iff$ subgroup $a\mathbb{Z}$ of $\mathbb{Z}$ containing $12\mathbb{Z}$)
12 has factors 1,2,3,4,6,12. Then



there are 3 JH series.

Definition: Product Group

Let G and H be groups.
The product group $G \times H$ is the cartesian product equipped with the component wise group operation.

$$(g_1, h_1) * (g_2, h_2) = (g_1 * g_2, h_1 * h_2)$$

Example

Let p be a prime number.
Take $G = H = \mathbb{Z}/p\mathbb{Z}$. Then

$$(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z}) \underset{notation}{=} (\mathbb{Z}/p\mathbb{Z})^2$$

where $|(\mathbb{Z}/p\mathbb{Z})^2| = p^2$ and

$$(a, b) + (a', b') = (a + a', b + b')$$

for $a, a', b, b' \in \mathbb{Z}$.
A subgroup K of $\tilde{G} = (\mathbb{Z}/p\mathbb{Z})^2$, by Lagrange's Theorem, must have order 1, p or p^2.
We know $|\{1\}| = 1$ and $|\tilde{G}| = p^2$.
If $|K| = p$, then K is cyclic and generated by (a, b).
If $k \in \{1, 2, \ldots, p-1\}$, then note that for $(a, b) \neq (0, 0)$

$$\langle (a, b) \rangle = \langle (ka, kb) \rangle$$

Because both have order p.
Conversely, if $(a, b) \neq (0, 0)$ and $(a', b') \neq (0, 0)$ satisfy

$$\langle (a, b) \rangle = \langle (a', b') \rangle$$

then for some $k \in \{1, 2, \ldots, p-1\}$ we have $(a', b') = (ka, kb)$.

- Upshot
  There are exactly $\frac{p^2-1}{p-1} = p + 1$ subgroups K of order p in $\tilde{G}$.
  - Example
    For $p = 3$,

$$\begin{tikzcd}[column sep=tiny]
 & & (\mathbb{Z}/3\mathbb{Z})^2 \arrow[dll, dash] \arrow[dl, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
\langle (1,0) \rangle = \langle (2,0) \rangle & \langle (1,1) \rangle = \langle (2,2) \rangle & & \langle (1,2) \rangle = \langle (2,1) \rangle & \langle (0,1) \rangle = \langle (0,2) \rangle \\
 & & \{(0,0)\} \arrow[ull, dash] \arrow[ul, dash] \arrow[ur, dash] \arrow[urr, dash] & &
\end{tikzcd}$$

    there are 4 JH series.

Definition: Automorphism

Let G be a group.
A (group) automorphism of G is a bijective group homomorphism

$$\phi : G \to G$$

$\mathrm{Aut}(G) = \{\phi : G \to G \mid \text{automorphisms}\}$.
Fact: $\mathrm{Aut}(G)$ equipped with composition (of functions) is a group.
Justification: $\phi \circ \psi \in \mathrm{Aut}(G)$ if $\phi, \psi \in \mathrm{Aut}(G)$; $\phi^{-1} = \phi^{-1}$ and $1_{\mathrm{Aut}(G)} = \mathrm{Id}_G$.

Example 1

Let $G = (\mathbb{Z}, +)$.
A homomorphism $G \xrightarrow{\phi} G$ is completely determined by $\phi(1) = a_\phi$.
Since $\phi(n) \underset{\phi \text{ homomorphism}}{=} n\phi(1) = na_\phi$.
Thus {group homomorphisms $\phi : G \to G$} $\leftrightarrow (\mathbb{Z}, \times)$ and $\phi \leftrightarrow a_\phi$.
If $(\phi(1) = a_\phi$ and $\psi(1) = a_\psi$, then note that

$$(\phi \circ \psi)(1) = \phi(\psi(1)) = \phi(a_\psi) = a_\phi a_\psi$$

So if $\phi \in \mathrm{Aut}(G)$, then $a_\phi \in \mathbb{Z}$ must have a multiplicative inverse in $\mathbb{Z}$.
Hence $a_\phi = 1$ or $a_\phi = -1$.
Conversely $\begin{cases} \phi_1(n) = n \\ \phi_{-1}(n) = -n \end{cases}$, $\forall n \in \mathbb{Z}$ are in $\mathrm{Aut}(G)$.
Therefore $\mathrm{Aut}\left((\mathbb{Z}, +)\right) = \{\pm 1\}, x \ \backslash)$.

Example 2

Let p be a prime and $G = (\mathbb{Z}/p\mathbb{Z}, +)$.
A group homomorphism $\phi : G \to G$ is (again) determined by $\phi(1) = a_\phi$.
So {group homomorphisms $\phi : G \to G$} $\leftrightarrow \mathbb{Z}/p\mathbb{Z}$, $\phi \leftrightarrow a_\phi$ and $\phi \circ \psi \leftrightarrow a_\phi a_\psi$.
So if ϕ is bijective, then a_ϕ must have a multiplicative inverse in $\mathbb{Z}/p\mathbb{Z}$.
Fact: Any nonzero element $a \in \mathbb{Z}/p\mathbb{Z}$ has a multiplicative inverse.

- Proof
  Look at $\langle a \rangle = \{ka \mid k \in \mathbb{Z}\}$.
  Since $\mathbb{Z}/p\mathbb{Z}$ is simple, $\langle a \rangle = \mathbb{Z}/p\mathbb{Z}$.
  Hence $\langle a \rangle \ni 1$, so $\exists k \in \mathbb{Z}$ such that $ka = 1$ in $\mathbb{Z}/p\mathbb{Z}$.
  Take $b := k \pmod{p}$, and we have $ba = 1$. ∎

Conclusion

$\mathrm{Aut}\left((\mathbb{Z}/p\mathbb{Z}, +)\right) = (\mathbb{Z}/p\mathbb{Z})^x = ((\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}, x)$

Example

Take $G = (\mathbb{Z}/p\mathbb{Z})^2$.
Compute $|\mathrm{Aut}(G)|$.
$Aut(G)$ is also called $\mathrm{GL}_2(\mathbb{F}_p)$.

Definition: Semidirect Product (Left)

Let H and N be groups and

$$\psi : H \to \mathrm{Aut}(N)$$

be a group homomorphism.
The semidirect product $H \underset{\psi}{\ltimes} N$, as a set is (simply) the cartesian product $H \times N$ equipped with the binary operation

$$(h_1, n_1) * (h_2, n_2) = \left(h_1 h_2, n_1 \cdot \overbrace{(\underbrace{\psi(h_1)}_{\in \mathrm{Aut}(N)}\ n_2)}^{\in N} \right)$$

This is a group.
$(1_H, 1_N)$ is the identity.

November 2, 2023

Definition: Semidirect Product (Right)

Let H and N be groups, and let

$$\phi : H \to \mathrm{Aut}(N)$$

be a group homomorphism.
The semidirect product of H by N via ϕ is

$$N \rtimes_{\phi} H \underset{\text{as a set}}{=} N \times H$$

equipped with the binary operation

$$(n_1, h_1) * (n_2, h_2) = (n_1 \cdot \overbrace{\underbrace{\phi(h_1)}_{\in \mathrm{Aut}(N)}\ n_2}^{\in N}, h_1 h_2)$$

Associativity

Given $(n_1, h_1), (n_2, h_2), (n_3, h_3)$, need to prove that

$$\underbrace{((n_1, h_1) * (n_2, h_2))}_{n_1 \cdot [\phi(h_1) n_2], h_1 h_2)} * (n_3, h_3) = (n_1, h_1) \underbrace{(*(n_2, h_2) * (n_3, h_3))}_{(n_2[\phi(h_2) n_3], h_2 h_3)}$$

Left Hand Side:

$$(n_1[\phi(h_1) n_2][\phi(h_1 h_2) n_3], h_1 h_2 h_3)$$

Since $\phi(h_1)$ is a homomorphism,

$$\phi(h_1)(n_2[\phi(h_2) n_3] = [\phi(h_1) n_2][\phi(h_1)(\phi(h_2) n_3)]$$

and

$$\phi(h_1)(\phi(h_2) n_3) = \phi(h_1 h_2) n_3.$$

Right Hand Side:

$$(n_1\ \underbrace{\phi(h_1)(n_2[\phi(h_2) n_3])}_{[\phi(h_1) n_2] \underbrace{[\phi(h_1)(\phi(h_2) n_3)]}_{\phi(h_1 h_2) n_3}}, h_1 h_2 h_3) = (n_1[\phi(h_1) n_2][\phi(h_1 h_2) n_3], h_1 h_2 h_3)$$

Identity

Use $(1_N, 1_H)$.

Inverse

Given (n_1, h_1), want to find (n_2, h_2) that is 2-sided inverse.
Use

$$(\phi(h_1^{-1})n_1^{-1}, h_1^{-1})$$

Need $n_2 \in N$, such that

$$\begin{aligned} n_1\phi(h_1)n_2 &= 1_N \\ \phi(h_1)n_2 &= n_1^{-1} \\ n_2 &= \phi(h_1^{-1})n_1^{-1} \end{aligned}$$

Left hand proof left as an exercise.

Upshot

The external semidirect product produces a new group out of the old group.
If we take ϕ to be $\phi(h) = \mathrm{Id}_N$, we get the direct product $N \times H$.

Proposition: Internal Semidirect Product

Let G be a group, $H \leq G$, $N \trianglelefteq G$, so that we have a group homomorphism

$$\begin{aligned} H \leq G &\xrightarrow{\phi} \mathrm{Aut}(N) \\ g &\rightsquigarrow \phi(g)n \underset{\text{defn.}}{=} gng^{-1} \end{aligned}$$

Assume that $H \cap N = \{1\}$ and $HN(\underset{\text{1st isomorphism}}{=} NH) \underset{\text{assumption}}{=} G$.
Then we have an isomorphism of groups

$$\begin{aligned} N \underset{\phi}{\rtimes} H &\xrightarrow{f} G \\ (n, h) &\rightsquigarrow nh \end{aligned}$$

Remark

In this situation, we asy that G is the (internal) semidirect product of H and N.

Proof

- f is a group homomorphism.

$$\begin{aligned} f((n_1, h_1) * (n_2, h_2)) &= f(n_1\phi(h_1)n_2, h_1h_2) \\ &= n_1\phi(h_1)n_2h_1h_2 \\ &= n_1(h_1n_2h_1^{-1})h_1h_2 \\ &= n_1h_1n_2h_2 \\ &= f(n_1, h_1)f(n_2, h_2) \end{aligned}$$

- f is injective.

If $f(n,h) = 1$, then $nh = 1$. So

$$\underbrace{n}_{\in N} = \underbrace{h^{-1}}_{\in H}.$$

Therefore $n = 1$ and $h = 1$.

- f is surjective

  Since $NH = G$. ■

Example 1

Let $N = \text{Stab(String)}$, of order 4, and $H = \text{Stab}_G(P)$, of order 3.
Then $H \cap N = \{1\}$ and $HN = G$ gives $|G| = 12$.

Example 2

Let $\widetilde{G} = \text{GL}_2(\mathbb{R})$ and

$$K = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \mid x \in \mathbb{R} \right\}$$

Then

$$G = N_{\widetilde{G}}(K) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, d \in \mathbb{R}^\times, b \in \mathbb{R} \right\},$$

$N = K$, and

$$H = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \in \mathbb{R}^\times \right\}$$

Observe

$$HN = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & ax \\ 0 & d \end{pmatrix} \mid a, d \in \mathbb{R}^\times, x \in \mathbb{R} \right\}$$

This is the "Borel subgroup."

Definition: Group Extension

Let H and N be groups.
An extension of H by N is the data of

1. A group G.

2. An injective homomorphism of $N \overset{\iota}{\hookrightarrow} G$ such that $\iota(N) \trianglelefteq G$.

3. An isomorphism of groups $G/\iota(N) \xrightarrow[\sim]{\pi} H$.

Example

All the semidirect products give extensions of H by N.

Notation

$$1 \longrightarrow N \xrightarrow{\sim} G \xrightarrow{\tilde{\pi}} H \longrightarrow 1$$

(This is an exact sequence.)

Recall: Derived Group

If G is a group, the derived group $DG = \langle [g,h] \mid g_1 h \in G \rangle \trianglelefteq G$ is the smallest normal subgroup of G such that G/N is abelian.
We can apply D repeatedly.

$$\begin{array}{ccccccccc} G & \trianglerighteq & DG & \trianglerighteq & D(DG) & \trianglerighteq & D(D(DG)) & \trianglerighteq & \cdots \\ \parallel & & \parallel & & \parallel & & \parallel & & \\ G^{(0)} & & G^{(1)} & & G^{(2)} = D(G^{(1)}) & & G^{(3)} = D(G^{(2)}) = D(D(G^{(1)})) & & \end{array}$$

Inductive Definition: $G^{(i+1)} = D(G^{(i)}, i \geq 0, G^{(0)} = G$.

Proposition:

Let G be a group.
$[\exists N \geq 0 \ G^{n} = \{1\}]$ if and only if there exists some filtration $G.$ of length l with $G_0 = G$, $G_l = \{1\}$ such that G_i/G_{i+1} is abelian.

Definition: Solvable Group (Again)

A group G is solvable (or soluble) if the 2 equivalent conditions are satisfied.

Proof

$(\Longrightarrow)$ Suppose $G^{(n)} = \{1\}$.
Then take $G_i := G^{(i)}$ for $i = 0, 1, \ldots, N$ and $G_i/G_{i+1} = G^{(i)}/D(G^{(i)})$ is abelian.
Hence a filtration required in the second condition.
$(\Longleftarrow)$ Suppose we have a filtration

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_l = \{1\}$$

such that G_i/G_{i+1} is abelian $\forall i = 0, \ldots, l-1$.
Claim: for all $i = 0, \ldots, l-1$, we have

$$G_i \supseteq G^{(i)}$$

If this is true, it finishes the proposition since $G^{(l)} \subseteq G_l = \{1\}$.

- Proof of Claim
  By induction on i,

$$i = 0 \quad G^{(0)} = G = G_0$$

Suppose, for $i \geq 0$, that $G_i \supseteq G^{(i)}$.
Then, since G_i/G_{i+1} is abelian, by the definition of DG, $G_{i+1} \supseteq D((G_i)$.
Apply D to $G_i \supseteq G^{(i)}$ and we get $D(G_i) \supseteq D(G^{(i)})$.
Since, in general, if $G \geq H \geq K$, then $D(H) \geq D(K) = \langle k_1 k_2 k_1^{-1} k_2^{-1} \rangle$.
Therefore, $G_{i+1} \geq D(G^{(i)}) \underset{defn.}{=} G^{(i+1)}$. ■

Example 1

$G = \mathrm{Alt}(4)$ is solvable.
$D(G) = N$ of size 4, $D(N) = \{1\}$ and $D(DG) = \{1\}$.

Example 2

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, d \in \mathbb{R}^\times, b \in \mathbb{R} \right\}$$

is solvable since if

$$(\mathbb{R}, +) \cong N = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \mid x \in \mathbb{R} \right\}$$

then

$$G \underset{\neq}{\trianglerighteq} N \underset{\neq}{\trianglerighteq} \{1\}$$

Meets the condition that $G_0 = G$, $G_l = \{1\}$ such that G_i/G_{i+1} is abelian. So

$$G/N \cong H = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \in \mathbb{R}^\times \right\} \text{ is abelian } \cong R^\times \times \mathbb{R}^\times$$

Nonexample

$G = \mathrm{GL}_2(\mathbb{R})$.
Say $A, B \in \mathrm{GL}_2(\mathbb{R})$. Then $[A, B] = ABA^{-1}B^{-1}$ and $\det(ABA^{-1}B^{-1}) = 1$.
Therefore $DG = \mathrm{SL}_2(\mathbb{R})$, but since $\mathrm{SL}_2(\mathbb{R})$ is perfect, $D(\mathrm{SL}_2(\mathbb{R})) = \mathrm{SL}_2(\mathbb{R})$.
Proof left as an exercise.

Example 3

Let p be a prime. The Heisenberg group of order p^3 is given as

$$\mathrm{Heis}_p = \left\{ \begin{pmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{pmatrix} \mid x, y, z \in \mathbb{Z}/p\mathbb{Z} \right\} \qquad |\mathrm{Heis}_p| = p^3$$

(uses the same formula as with $\mathbb{R}$)
The exact same computation for $\mathbb{R}$ gives:

$$D(\mathrm{Heis}_p) = \mathbb{Z}(\mathrm{Heis}_p) = \left\{ \begin{pmatrix} 1 & 0 & z \\ & 1 & 0 \\ & & 1 \end{pmatrix} \mid z \in \mathbb{Z}/p\mathbb{Z} \right\}$$

Therefore $D(D(\mathrm{Heis}_p)) = \{1\}$.
So Heis_p is solvable as is $\mathrm{Heis}_3(\mathbb{R})$.

To Read: Theorem

Let G be a finite group. Then the factor group in the JH series of G are the same as multisets independent of the choice of the JH series.

Example

Let $G = \mathbb{Z}/12\mathbb{Z}$

$$\begin{tikzcd}
& & G = \mathbb{Z}/12\mathbb{Z} & \\
& 2\mathbb{Z}/12\mathbb{Z} \arrow[ur, dash, "C_2"] & & 3\mathbb{Z}/12\mathbb{Z} \arrow[ul, dash, "C_3"'] \\
4\mathbb{Z}/12\mathbb{Z} \arrow[ur, dash, "C_2"] & & 6\mathbb{Z}/12\mathbb{Z} \arrow[ul, dash] \arrow[ur, dash, "C_2"'] & \\
& & \{1\} = 12\mathbb{Z}/12\mathbb{Z} \arrow[ull, dash, "C_3"] \arrow[u, dash, "C_2"'] &
\end{tikzcd}$$

November 7, 2023

Definition/Proposition: Solvable

A group G solvable if and only if it satisfies 2 equivalent conditions:

1. $\exists N \geq 1, D^N(G) = \underbrace{D(D(\cdots D}_{N}(G)\cdots) = \{1\}$.
2. There exists a filtration $G. = (G_0 \trianglerighteq \cdots \trianglerighteq G_l)$ with $G_0 = G$ and $G_l = \{1\}$ such that G_i/G_{i+1} is abelian $\forall i = 0, \ldots, l-1$.

Definition: Extension

If $N \trianglelefteq G$, we say G is an extension of G/N by N.

Proposition: Solvability is Compatible with Extensions

Let $N \trianglelefteq G$, then

1. If N is solvable and G/N is solvable, then G is solvable.

2. If G is solvable, then so are N and G/N.

Proof of 1

Let $N. = (N_0 \trianglerighteq \cdots \trianglerighteq N_l)$ and $Q. = (Q_0 \trianglerighteq \cdots \trianglerighteq Q_m)$ (where $G/N = Q$) be filtrations as in the definition of solvability. Then we "graft" the two filtrations into one.

$$\underbrace{\pi^{-1}(Q_0) \trianglerighteq \cdots \trianglerighteq \pi^{-1}(Q_{m-1}) \trianglerighteq \pi^{-1}(Q_m)}_{\text{factors are abelian}} = \underbrace{N_0 \trianglerighteq \cdots \trianglerighteq N_{l-1} \trianglerighteq N_l}_{\text{factors are abelian}}$$

Where $G \xrightarrow{\pi} Q = G/N$.
Since

$$\pi^{-1}(Q_i)/\pi^{-1}(Q_{i+1}) \underset{\text{2nd isomorphism theorem}}{\overset{\text{correlation theorem}}{\cong}} Q_i/Q_{i+1}$$

is abelian.

Proof of 2

- Lemma

  1. If $H \leq G$, then $D(H) \leq D(G)$.

  2. If $N \trianglelefteq G$, then $\pi(D(G)) = D(Q)$.

     – Proof of a

     $$\begin{aligned} D(H) &= \langle hh'h^{-1}h'^{-1} \mid h, h' \in H \rangle \\ &\subseteq \langle gg'g^{-1}g'^{-1} \mid g, g' \in G \rangle = D(G) \end{aligned}$$

     – Proof of b

     $$\pi(gg'g^{-1}g'^{-1}) = \pi(g)\pi(g')\pi(g)^{-1}\pi(g')^{-1}$$

     So $\pi(D(G)) \subseteq D(Q)$.
     Conversely, any commutator like the right hand side is in the image of π, hence $\pi(D(G)) \supseteq D(Q)$.

- Back to the proof of 2

  Suppose $D^k(G) = \{1\}$.
  Note, by the above lemma and with an application of induction,

$$\begin{gathered} D(N) \subseteq D(G) \\ D(D(N)) \subseteq D(D(G)) \\ \vdots \\ D^k(N) \leq D^k(G) = \{1\} \end{gathered}$$

So N is solvable.
Then also

$$D(Q) = \pi(D(G))$$
$$D(D(Q)) = \pi(D(D(G)))$$
$$\vdots$$
$$D^k(Q) = \pi(D^k(G))$$

So Q is solvable.

Corrollary

If A and B are solvable groups, then any semidirect product of A by B is solvable.

Definition: Conjugacy Class

The conjugacy class of $x \in G$

$$x^{\#}\{gxg^{-1} \mid g \in G\}$$

Recall that, by the orbit stabilizer theorem, $|x^{\#}| = \frac{|G|}{|C_G(x)|}$. So

$$C_G(X) = \{h \in G \mid hx = xh,\ hxh^{-1} = x\}$$

Example 1

Let $G = \mathrm{Alt}(4)$. Then

$$1^{\#} = \{1\}$$
$$|(B\ P)(W\ Y)^{\#}| = 3 \quad \text{all the } 2 + 2 \text{ cycles}$$

Consider $g = (B\ P\ W)$. Then $\langle g \rangle = \mathrm{Stab}_G(Y)$, $\pi\,\mathrm{Stab}(y)\pi^{-1} = \mathrm{Stab}(\pi(y))$, and

$$N_G(\langle g \rangle) = \langle g \rangle \underbrace{\geq}_{=} C_G(g)$$

Therefore $|C_G(g)| = 3$ and $|(B\ P\ W)^{\#}| = 4$.
Since $\pi(B\ P\ W)\pi^{-1} = (\pi(B)\pi(P)\pi(W))$,

$$\begin{aligned} \pi = (B\ P)(W\ Y) &\implies \pi(B\ P\ W)\pi^{-1} = (P\ B\ Y) = (B\ Y\ P) \\ \pi = (B\ P\ Y) &\implies \pi(B\ P\ W)\pi^{-1} = (P\ Y\ W) \\ \pi = (P\ W\ Y) &\implies \pi(B\ P\ W)\pi^{-1} = (B\ W\ Y) \end{aligned}$$

So

$$(B\ P\ W)^{\#} = \{(B\ P\ W), (B\ Y\ P), (P\ Y\ W), (B\ W\ Y)\}$$

Therefore

$$\begin{array}{llll} \mathrm{Alt}(4) = 1 & (B\ P)(W\ Y) & (B\ P\ W) & (B\ W\ P) \\ & (B\ W)(P\ Y) & (B\ Y\ P) & (B\ P\ Y) \\ & (B\ Y)(P\ W) & (P\ Y\ W) & (P\ W\ Y) \\ & & (B\ W\ Y) & (B\ Y\ W) \end{array}$$

The class equation

$$12 = 1 + 3 + 4 + 4$$

Consider $\mathrm{Sym}(4) = \widetilde{G}$, which has conjugacy class and cycle types

$$\begin{array}{ccccccccccc} \widetilde{G} & = & 1 & & 3 & & 8 & & \binom{4}{2} = 6 & & \frac{4!}{4} = 6 \\ & & & & \text{2+2-cycles} & & \text{3-cycles} & & \text{2-cycles} & & \text{4-cycles} \\ 24 & = & 1 & + & 3 & + & 8 & + & 6 & + & 6 \end{array}$$

Note that the 3 cycles in Alt(4) fuse into the same conjugacy class in Sym(4).

Definition: Fusion

Different conjugacy classes in G merge into 1 in $\widetilde{G}$.

More Generally

If $G = \coprod_{i=1}^{h} K_i$ into disjoint conjugacy classes, the class equation

$$|G| = \sum_{i=1}^{h} |K_i|$$

Example 1

Let p be a prime and $G = \mathrm{Heis}_3(p) = \left\{ \begin{pmatrix} 1 & x & z \\ & 1 & y \\ & & z \end{pmatrix} \mid x, y, z \in \mathbb{Z}/p\mathbb{Z} \right\}$.

Recall

$$Z(G) = \left\{ \begin{pmatrix} 1 & 0 & z \\ & 1 & 0 \\ & & 1 \end{pmatrix} \mid z \in \mathbb{Z}/p\mathbb{Z} \right\}$$

and, for any $g \in Z(G)$, $g^{\#} = \{g\}$.
So we have p conjugacy classes of size 1.
Let $(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2 \setminus \{(0,0)\}$ and $g := \begin{pmatrix} 1 & x & 0 \\ & 1 & y \\ & & 1 \end{pmatrix}$.
Consider the centralizer, $C_G(g) \geq Z(G)$ and $C_G(g) \geq \langle g \rangle$.
So $|C_G(g)| \geq p + 1$ and, by Lagrange, $|C_G(g)| \mid p^3$.
Therefore $|C_G(g)| = p^2$ and, by the orbit stabilizer theorem, $|g^{\#}| = p^3/p^2 = p$.
It follows that the class equation for $\mathrm{Heis}_3(p)$ is

$$p^3 = \underbrace{1 + \cdots + 1}_{\substack{p \\ Z(G)}} + \underbrace{p + \cdots + p}_{\substack{p^2 - 1 \\ \text{one for each } (x,y)}}$$

- Question

If $(x,y) \neq (x',y')$, then

$$\begin{pmatrix} 1 & x & \\ & 1 & y \\ & & 1 \end{pmatrix}^{\#} \neq \begin{pmatrix} 1 & x' & \\ & 1 & y' \\ & & 1 \end{pmatrix}^{\#}$$

Observe that

$$\begin{aligned} \begin{pmatrix} 1 & -a & ? \\ & 1 & -b \\ & & 1 \end{pmatrix}\begin{pmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{pmatrix}\begin{pmatrix} 1 & a & c \\ & 1 & b \\ & & 1 \end{pmatrix} &= \begin{pmatrix} 0 & -a & ? \\ & 0 & -b \\ & & \end{pmatrix}\begin{pmatrix} 1 & x+a & ? \\ & 1 & y+b \\ & & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & x & ? \\ & 1 & y \\ & & 1 \end{pmatrix} \end{aligned}$$

That is, $G \to G/Z(G) \cong (\mathbb{Z}/p\mathbb{Z})^2$.
In particular,

$$\begin{pmatrix} 1 & 1 & \\ & 1 & \\ & & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & & \\ & 1 & 1 \\ & & 1 \end{pmatrix}$$

are not conjugate.
But they become conjugate in $\mathrm{GL}_3(\mathbb{Z}/p\mathbb{Z})$, another instance of fusion.

Definition: p-Group

Let p be a prime number.
A finite group G is called a p-group if $|G| = p^n$ for some interger n.

Examples

- $\mathbb{Z}/p^n\mathbb{Z}$ (the cyclic group of p^n.
- $\mathrm{Heis}_3(p)$.
- Any repeated semi-direct products thereof.

Theorem: Solvability of p-Groups.

Any p-group $G \neq \{1\}$ has a nontrivial center $Z(G)$ and, therefore, is solvable.

Proof

Let $g \in G$.
If $g \in Z(G)$, then $g^{\#} = \{g\}$.
If $g \notin Z(G)$, then $C_G(g) \underset{\neq}{<} G$, so $|g^{\#}| = \frac{|G|}{|C_G(g)|}$ is divisible by p.
But then

$$p^n = |G| = \underbrace{1 + \cdots + 1}_{|Z(G)|} + (\text{integers disible by } p)$$

Therefore $p \mid |Z(G)|$ and $|Z(G)| \geq p$.
By induction on n, we may assume that any group of order p^m $(0 \leq m \leq n-1)$ is solvable.
But then

$$\underbrace{Z(G)}_{\text{order } \geq p} \trianglelefteq G \twoheadrightarrow \underbrace{G/Z(G)}_{\text{has order } p^m,\, m<n}$$

By the above proposition, G is solvable.

Remark:

In some ways, solvable groups are easier to understand.
So given a finite group G, one attempts to understand G by first studying solvable subgroups of G.

Definition: p-Sylow Subgroups

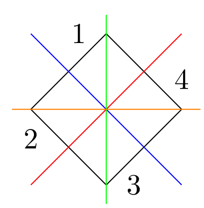
Let G be a finite group and p be prime.
Write $|G| = p^n \cdot m$ where $n \geq 0$, $m \geq 1$ are integers and $p \nmid m$.
A p-Sylow subgroup H of G, is a subgroup of order $|H| = p^n$.

Example 1

Let $G = \text{Alt}(4)$.
$|G| = 12 = 2^2 \cdot 3$, so the 2-Sylow subgroup of G is $H = \text{Stab(String)}$.
$|G| = 12 = 3^1 \cdot 4$, so the 3-Sylow subgroups of G are the vertext stabilizers.

Example 2

Let $G = \text{Sym}(4)$.
$|G| = 4! = 24 = 2^3 \cdot 3 = 3^1 \cdot 8$.
3-Sylows are the cyclic groups generated by (1 of the 8) 3-cycles, so there are 4 of them.



$$\begin{aligned} D_8 &\leq \text{Sym}(4) \\ &= \begin{cases} 4 \text{ rotations} \\ 4 \text{ reflections} \end{cases} \\ &= \{(1\ 2)(3\ 4), (2\ 4), (1\ 4)(2\ 3), (1\ 3), (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (4\ 3\ 2\ 1), 1\} \end{aligned}$$

November 9, 2023

Jean-Paul Serre

The proofs of Sylow Theorems below are taken from Serre's Finite Groups, an Introduction.

Definition: p-Sylow Subgroups

Let G be a finite group, p be prime, and write $|G| = p^n \cdot m$ where $n \geq 0$ and $m \geq 1$ are integers such that $p \nmid m$.
A p-Sylow subgroup of G is a subgroup $S \leq G$ such that $|S| = p^n = q$.

Theorem: First p-Sylow Theorem

There exist p-Sylow subgroups.

Recall:

By Lagrange, $H \le G \iff |H| \,\Big|\, |G|$.
However, the converse is false.
For example, $G = \mathrm{Alt}(4)$ has no subgroup of order 6, even though $6 \big| 12$.

Proof

Let $X = \{S \subseteq G \mid |S| = p^n\}$.
Note $|X| = \binom{q\cdot m}{q}$.
If $p^n = 1$, there is nothing to prove. So assume $n \ge 1$, $q \ge p$.

- Lemma

  $\binom{q\cdot m}{q} \equiv m \pmod p$; in particular, $p \nmid |X|$.

  - Proof

    $R = (\mathbb{Z}/p\mathbb{Z})[T] = \{\text{polynomials in } T \text{ with } \mathbb{Z}\text{-coefficients } \pmod p\}$ is (going to be) a ring.
    Consider $(1+T)^{q\cdot m}$.
    First, by the Binomial Theorem,

    $$(1+T)^p = \sum_{j=0}^{p} \binom{p}{j} T^j$$

    If $1 \le j \le p-1$, then $\binom{p}{j} = \frac{p!}{(p-j)!j!}$ is divisible by p. So

    $$(1+T)^p \equiv 1 + T^P \pmod p$$

    Repeating the process,

    $$(1+T)^{p^2} \equiv ((1+T)^p)^p \equiv (1+T^P)^P \equiv 1 + T^{p^2} \pmod p$$

    By induction,

    $$(1+T)^q \equiv 1 + T^q \pmod p$$

    Using the Binomial Theorem again,

    $$(\star) \quad (1+T)^{q\cdot m} \equiv (1+T^q)^m \equiv 1 + \binom{m}{1} T^Q + \cdot \pmod p$$

    On the other hand, by applying the Binomial Theorem directly,

    $$(*) \quad (1+T)^{q\cdot m} = \sum_{j=0}^{q\cdot m} \binom{q\cdot m}{j} T^j$$

Compare the coefficients of T^q, and we get $m \equiv \binom{q \cdot m}{q} \pmod p$.

Consider the (translation) action of G on X:

$$g * S := \{gs \mid s \in S\}$$

Now decompose X into disjoint G-orbits:

$$X = \coprod_{j=1}^{N} O_j$$

Then

$$|X| = \sum_{j=1}^{N} |O_j|$$

So at least 1 orbit, say $O_j = G \cdot S_0$ must have $|O_j| \not\equiv 0 \pmod p$.
Take $H := \mathrm{Stab}_G(S_0) = \{g \in G \mid gS_0 = S_0\}$.

1. By Orbit Stabilizer Theorem, $|H| = \frac{|G|}{|O_j|} = \frac{q \cdot m}{|O_j|} = q\frac{m}{|O_j|} \geq q$.

2. On the other hand, we fix $\sigma_0 \in S_0$ and we have a map

$$\begin{aligned} H &\xrightarrow{f} S_0 \\ h &\longmapsto h\sigma_0 \end{aligned}$$

f is injective, since $h_1\sigma_0 = h_2\sigma_0$, then $h_1 = h_2$.
Therefore $|H| \leq |S_0| = q$. ■

Theorem: Second Sylow Theorem

Notation as before, let S_0 be a p-Sylow subgroup.

1. Any p-subgroup, P, is contained in a conjugate of S_0.

   $$P \leq gS_0g^{-1}$$

   for some $g \in G$.

2. Any (other) p-Sylow subgroup S of G is conjugate to S_0.

   $$S = gS_0g^{-1}$$

   for some $g \in G$.

3. Let $n_p(G) = \#\{p\text{-Sylow subgroups of } G\}$. Then

$$n_p(G) \equiv 1 \pmod p$$

(This is sometimes listed as the third Sylow theorem)

- Lemma 2

  Let P be a p-group acting on a finite set Y.
  Define $Y^P = \{y \in Y \mid gy = y, \forall g \in P\}$, the set of fixed points. Then

  $$|Y^P| \equiv |Y| \pmod p$$

  – Remark (*): in Algebraic Topology this leads to Smith Theory.

  – Proof

    Decompose Y into P-orbits.

    $$Y = \underbrace{\{*_1\} \coprod \cdot \coprod \{*_a\}}_{Y^P} \coprod_{j=1}^{M} O_j$$

    Therefore $|O_j| = \frac{|P|}{|\mathrm{Stab}_j|}$ is a power of p and $\geq p$.
    It follows that

    $$|Y| = |Y^P| + \underbrace{\sum_{j=1}^{M} |O_j|}_{\text{divide by } p} \equiv |Y^p| \pmod p$$

Proof (Second Sylow Theorem)

- Part 1
  $y = G/S_0$, the coset space, is not necessarily a group.
  G acts on y by translation: $g * (g' S_0) = gg' S_0$.
  Restrict the action to P, and

  $$|y^P| \equiv |y| \pmod p) = \frac{|G|}{|S_0|} = \frac{q \cdot m}{q} = m \not\equiv 0 \pmod p$$

  Therefore $y^P \neq \varnothing$. Say $gS_0 \in y^P$ or $P \subseteq \mathrm{Stab}_G(gS_0)$.
  For any $\pi \in P$, $\pi \cdot gS_0 = gS_0$, and

  $$g^{-1}\pi g \underbrace{S_0}_{\ni 1} = S_0$$
  $$g^{-1}\pi g \in S_0$$
  $$\pi \in gS_0 g^{-1}$$

  Thus, $P \leq gS_0 g^{-1}$. ■

- Part 2
  If S is a p-Sylow and, by (1), $S \subseteq gS_0g^{-1}$, then, since both have q elements,

$$S = gS_0g^{-1} \quad \blacksquare$$

- Part 3
  Write $\mathcal{S} = \{p-\text{Sylows } S \text{ of } G\}$
  Let G act on $\mathcal{S}$ by conjugation.

$$g * S = gSg^{-1}$$

  By (2), the action is transitive.
  Note: $\mathrm{Stab}_G(S) = N_G(S)$.

  - Lemma 3

    Suppose $S, S' \in \mathcal{S}$.
    If $S' \in N_G(S)$, then $S' = S$.

    - Proof

      Note that $|N_G(S)| \mid |G| = q \cdot m$, and $S \subseteq N_G(S)$ where $|S| = q$.
      Therefore S is a p-Sylow of $N_G(S)$.
      Now, if $S' \leq N_G(S)$, S' is a p-Sylow of $N_G(S)$.
      So, by (2) applied to $N_G(S)$ replacing G,

$$\exists n \in N_G(S): \quad S' = nS'n^{-1} = S \quad \blacksquare$$

      - Remark

        $n_p(G) = \frac{|G|}{|\mathrm{Stab}_G(S)|} = \frac{|G|}{|N_G(S)|}$ for any p-Sylow S.

  Choose any $S_0 \in \mathcal{S}$, and let S_0 act on $\mathcal{S}$ by conjugation.
  Then, by Lemma 2, $|\mathcal{S}^{S_0}| \equiv |\mathcal{S}| \pmod{p}$, and

$$\mathcal{S}^{S_0} = \{S' \in \mathcal{S} \mid S_0 \in \underbrace{\mathrm{Stab}_G(S')}_{\underbrace{=N_G(S')}_{\iff S_0 = S'}}\} = \{S_0\} \quad \blacksquare$$

Sylow Examples

Example 1

Let $G = \mathrm{Alt}(4)$, $|G| = 2^2 \cdot 3^1$.

$$n_2(G) = 1 \equiv 1 \pmod{2}$$
$$n_3(G) = 4 \equiv 1 \pmod{3}$$

Example 2

Let p be a prime.
Denote $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

$$M_{2\times 2}(\mathbb{F}_p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{F}_p \right\}$$

has addition and multiplication (not commutative).

$$|M_{2\times 2}(\mathbb{F}_p)| = p^4$$

And $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2\times 2}(\mathbb{F}_p)$ if and only if $\det(A) = ad - bc$ is nonzero.

$$\left(A^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \right)$$

Definition: General Linear Group Over Finite Field

$$\mathrm{GL}_2(\mathbb{F}_p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2\times 2}(\mathbb{F}_p) \mid ad - bc \neq 0 \text{ in } \mathbb{F}_p \right\}$$

equipped with matrix multipication, is a group.

- Question: $|\mathrm{GL}_2(\mathbb{F}_p)| = ?$
  Conceptual answer will be given in Math 201.
  An ad hoc answer is

  $$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc = 0 \text{ in } \mathbb{F}_p \right\}$$

  If $a = 0$ (in $\mathbb{F}_p$), then $bc = 0$ so $b = 0$ or $c = 0$. So consider

  $$\underbrace{\{a = 0 \text{ and } b = 0\}}_{p^2} \cup \underbrace{\{a = 0 \text{ and } c = 0\}}_{p^2} : \cap \text{ has } p \text{ elements}$$

If $a \neq 0$ (in $\mathbb{F}_p$), then $d = bc/a$, then $\underbrace{p-1}_{a}\ \underbrace{p}_{b}\ \underbrace{p}_{c}$.

It follows that

$$\begin{aligned} \mathrm{GL}_2(\mathbb{F}_p)| &= p^4 - \left[\underbrace{(p^2 + p^2 - p)}_{a=0} + \underbrace{(p-1)pp}_{p\neq 0} \right] \\ &= p(p^3 - (2p-1) - p(p-1)) \\ &= p(p^3 - p^2 - p + 1) \\ &= p(p-1)(p^2 - 1) \\ &= p(p-1)^2(p+1) \end{aligned}$$

- Question: a p-Sylow of $\mathrm{GL}_2(\mathbb{F}_p)$ has order p.

  Example: $H = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \mid x \in \mathbb{F}_p \right\}$ is one. And

$$N_G(H) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, d \in \mathbb{F}_p^{\times},\ b \in \mathbb{F}_p \right\}$$

  Therefore

$$n_p(G) = \frac{|G|}{|N_G(H)|} = \frac{p(p-1)^2(p+1)}{\underbrace{(p-1)}_{a}\underbrace{p}_{b}\underbrace{(p-1)}_{d}} = p + 1 \equiv 1 \pmod p$$

November 14, 2023

Recall: Sylow Theorems

Let G be a finite group where $|G| = p^n m$, p prime, $m \in \mathbb{Z}$ and $p \nmid m$. Then

1. p-Sylows exist: $H \leq G$ with $|H| = p^n$.

2. All the p-sylows are conjugate in G.

3. $$n_p(G) = \#\{p\text{-Sylows of } G\} = \frac{|G|}{|N_G(\underbrace{P}_{\text{any } p\text{-Sylow}})|} \equiv 1 \pmod p$$

Note: $n_p(G)|m$ (from 3).

Theorem*: Feit-Thompson

All groups of odd order are solvable.
Proof too long to reproduce.

Proposition: Order pq Groups are Solvable

Let p, q be primes.
Any group G with order pq is solvable.

Proof

If $p = q$, then G is a p-group. So it is solvable.
So let us assume that $p \neq q$.
We may assume, without loss of generality, that $p < q$. Then $n_q(G) \equiv 1 \pmod q$ and $n_q(G) \mid p$.
Then $p \not\equiv 1 \pmod q$.
Therefore, $n_q(G) = 1$.
By Sylow 2, the unique q-Sylow, say Q, is normal in G.
Now $|G/Q| = |G|/|Q| = p$, hence G/Q is abelian. Similarly, since $|Q| = q$, Q is abelian.
So, with the filtration

$$G \underset{\neq}{\triangleright} Q \underset{\neq}{\triangleright} 1,$$

G is solvable.

Proposition: Order ppq Groups are Solvable

Let p, q be primes.
If $|G| = p^2 q$, then G is solvable.

Proof

If $n_p(G) = 1$, then the p-Sylow P will be normal and have order p^2, hence by the previous proposition (or since P is a p-group), P is solvable and G/P is cyclic of order q (hence abelian). So G will be solvable.
If $n_q(G) = 1$, then the q-Sylow Q wil be normal and have order q with $|G/Q| = p^2$, so G is solvable.
So we may assume, in the rest of the proof, that $n_p(G) = q$ and $n_q(G) \in \{p, p^2\}$.
Then $q \equiv 1 \pmod p$ by Sylow 3, and $p|(q-1)$, so $p \leq q-1$, so $p < q$.
But then $p \not\equiv 1 \pmod q$ (because $p \equiv 1 \pmod q \implies q|(p-1) \implies q < p$).
Therefore $n_q(g) = p^2$.
Let Q be a q-Sylow. Since $n_q(G) = p^2 = \frac{|G|}{|N_G(Q)|}$, we have $|N_G(Q)| = q$.
That is, $N_G(Q) = Q$.
Consider all the q-Sylows xQx^{-1} of G, p^2 in number.
For any $g \in xQx^{-1} \setminus \{1\}$, $\langle g \rangle = xQx^{-1}$, so g has order q.
Conversely, any $g \in G$ of order q a q-Sylow.
Consider

$$\Sigma = \bigcup_{xQ \in G/Q} x(Q \setminus \{1\})x^{-1}$$

a set consisting entirey of elements of order q.
The union is pairwise disjoint, since if

$$x(Q \setminus \{1\})x^{-1} \cap y(Q \setminus \{1\})y^{-1} \neq 0$$

then $\langle g \rangle = xQx^{-1} = yQy^{-1}$.

$$\implies (y^{-1}x)Q(y^{-1}x)^{-1} = Q \implies y^{-1}x \in N_G(Q) = Q$$

So $yQ = xQ$.
Now

$$|\Sigma| = |G/Q|(|Q| - 1) = p^2(q-1)$$

So

$$|G \setminus \Sigma| = |G| - |\Sigma| = p^2 q - p^2(q-1) = p^2$$

Now, let P be a p-Sylow of G. Then any element $g \in P$ will have order 1, p, or p^2 by Lagrange, so $g \notin \Sigma$.
Therefore

$$\underbrace{P}_{\text{order } p^2} \subseteq \underbrace{G \setminus \Sigma}_{\text{order } p^2} \implies P = G \setminus \Sigma$$

Hence $G \setminus \Sigma$ must be the unique p-Sylow of G, which contradicts $n_p(G) = q$.

Remark*: Burnside

Any group of order $p^a q^b$ is solvable

Definition: Word

Let X be a set (of "letters"), e.g. $X = \{x_1, \dots, x_n\}$.
A word in X is an infinite sequence $(a_1, a_2, a_3, \dots) = (a_n)_{n=1}^{\infty}$ such that for each $i = 1, 2, 3, \dots$,

$$\begin{cases} a_i = 1 \\ a_i = x, & x \in X \\ a_i = x^{-1} \end{cases}$$

and, for all $i >> 0$, $a_i = 1$.

Example

$X = \{x, y, z\}$.
$(x, x^{-1}, y, y, y, z, x, 1, 1, 1, \dots)$
$(y, 1, z, z, y^{-1}, 1, 1, 1, \dots)$

Definition: Reduced Word

A word (a_n) is reduced if $\forall i \geq 1$, $\forall x \in X$,

1. If $a_i = x$, then $a_{i+1} \neq x^{-1}$
2. If $a_i = x^{-1}$, then $a_{i+1} \neq x$.
3. If $a_i = 1$, then $a_{i+1} = 1$.

Note that neither of the previous examples are reduced.
The empty word $(1, 1, 1, \dots)$ is always reduced.

Fact/Construction: Word Reduction

Given any word (a_n), we construct the reduction, $\mathrm{red}(a_n)$, in the following way:

1. If $a_i = x$ and $a_{i+1} = x^{-1}$ or $a_i = x^{-1}$ and $a_{i+1} = x$, then skip both a_i and a_{i+1}.
2. If $a_i = 1$ but $a_{i+1} \neq 1$, skip a_i.

Example

$(x, x^{-1}, y, y, 1, z, x, 1, \dots)$
$\rightsquigarrow (y, y, 1, z, x, 1, \dots)$
$\rightsquigarrow (y, y, z, x, 1, \dots)$ is the reduction.

Definition: Free Group

The free group on X, $F(X)$, is the set of reduced words on X equipped with the binary operation for $\alpha = (a_n)$ and $\beta = (b_n)$:

$$\alpha * \beta = \text{red}(\text{concatenation of } \alpha \text{ and } \beta)$$

Example

$\alpha = (x, y, z, x^{-1}, 1, \ldots)$ and $\beta = (x, z^{-1}, y^{-1}, x^{-1}, y, 1, \ldots)$

$$\begin{aligned} &\rightsquigarrow (\underbrace{x, y, z, x^{-1}}_{\alpha}, \underbrace{x, z^{-1}, y^{-1}, x^{-1}, y}_{\beta}, 1, \ldots) \\ &\rightsquigarrow (y, 1, \ldots) \end{aligned}$$

Example

IMAGE HERE - TRIPLE TORUS
π_1 of the triple torus with piece removed is the free group on 2×3 letters.

Proposition (Universal Mapping Property)

Let X be a set and G be a group.
Then there is a natural bijection

$$\text{Fun}(X, G) \xrightarrow[\alpha]{\sim} \text{Hom}_{\text{group}}(F(X), G)$$

Where $\text{Fun}(X, G)$ is the collection of functions from X to G.

Proof

Given $f \in \text{Fun}(X, G)$ (i.e. a function $X \xrightarrow{f} G$) let $\alpha(f)$ be defined

$$\alpha(f)(a_1, a_2, a_3, \ldots, 1, 1, 1, \ldots) = \underbrace{f(a_1)}_{G} \underbrace{f(a_2)}_{G} \underbrace{f(a_3)}_{G} \cdots \underbrace{1 \cdot 1 \cdot 1 \cdots}_{\text{ignored}}$$

$\alpha(f)$ is a homomorphism (skipped; see Robert Boltje's lecture notes).
Conversely, given $\phi \in \text{Hom}_{\text{groups}}(F(X), G)$, let

$$\beta(\phi)(x) = \phi((x, 1, 1, \ldots))$$

Exercise: α and β are inverses.

Remark*:

In categorical terms, F is adjoint functor to the forgetful functor from Groups→Sets.

Definition: Normal Generated Subgroup

Let G be a group and $S \subseteq G$ a subset.
Recall $\langle S \rangle$ is the subgroup generated by S.
Define $\langle\langle S \rangle\rangle = \langle gsg^{-1} : s \in S, g \in G \rangle$.
This is the normal subgroup generated by S.

Definition: Presentation

Let x be a set (of letters) and $S \subseteq F(X)$ a "relation".
The quotient group $F(X)/\langle\langle S\rangle\rangle$, denoted by $\langle X : S\rangle$, is called a presentation of the group.

Example

Let $X = \{a, b, c\}$ and $S = \{abba, aa, ac^{-1}\}$.

$$\langle a, b, c : abba, aa, ac^{-1}, abac\rangle$$

refers to the qutioent group $F(x)/\langle\langle S\rangle\rangle$.

Example*

IMAGE HERE - TRIPLE TORUS WITHOUT REMOVAL
π_1 of that is $\langle a_1, b_1, a_2, b_2, a_3, b_3 : [a_1, b_1][a_2, b_2][a_3, b_3]\rangle$.

Proposition (Universal Mapping Property)

Let $\langle X : S\rangle$ be a presentation of a group G (where $G = X$) and a group H,
Giving a group homomorphism $G \longrightarrow H$ is equivalent to giving a function $X \xrightarrow{f} H$ such that

$$S \subseteq \ker(\alpha(f) : F(X) \to H)$$

November 16, 2023

Definition: Monoid

A group is a set M equipped with a binary operation $*$ satisfying

1. $a * (b * c) = (a * b) * c, \quad \forall a, b, c \in M$
2. $\exists e \in G : \quad a * e = a = e * a, \quad \forall a \in M$
3. $\cancel{\forall a \in G : \quad \exists b \in G : \quad ab = e = ba}$

Say M is commutative if

1. $\forall a, b \in M : \quad : a * b = b * a$

Examples

$\mathbb{N}_0 = \{0, 1, 2, 3, 4, \ldots\}$ equipped with $+$ is a monoid.
$\mathbb{N} = \{1, 2, 3, 4, \ldots\}$ equipped with $\times$ is a monoid.
$\mathbb{Z}$ with $\times$ is a monoid.

Definition: Ring

A ring is a set R equipped with 2 binary operations $+$ and $\cdot$ such that

1. $(R, +)$ is a commutative group,
2. $(R, \cdot)$ is a monoid and,
3. $\forall a, b, c \in R$:
   - $a \cdot (b + c) = a \cdot b + a \cdot c$ and
   - $(a + b) \cdot c = a \cdot c + b \cdot c$

Notation

The additive neutral element is denoted by $0_R = 0$.
The multiplicative neutral element is denoted by $1_R = 1$.

Definition: Rng

If, instead, we drop the multiplicative identity requirement, we construct a rng or "ring without identity".

Sources of Rings

Three main sources of rings (at least historically)

1. Numbers
2. Functions
3. Linear Operators

- Numbers
  $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ are rings.

Definition: Subring

A subset $S \subseteq R$ is a subring if

1. $(S, +)$ is a subgroup of $(R, +)$ and,
2. $(S, \cdot)$ is a submonoid of $(R, \cdot)$.

i.e. $0_R \in S$, $1_R \in S$, and $x, y \in S \implies x + y, x - y, xy \in S$.

Example: Gaussian Integers

Let $R = \mathbb{C}$ (the operation notation is supressed when understood)
$S := \{a + bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$ (where $i^2 = -1$) is a subring of $\mathbb{C}$ since

1. $0 = 0 + 0i$
2. $1 = 1 + 0i$
3. $z = a + bi$ and $w = c + di$ are in S, then

$$z \pm w = (\underbrace{a \pm c}_{\in \mathbb{Z}}) + (\underbrace{c \pm d}_{\in \mathbb{Z}})i$$
$$zw = (\underbrace{ac - bd}_{\in \mathbb{Z}}) + (\underbrace{bc + ad}_{\in \mathbb{Z}})i$$

This subring is the Gaussian integers, denoted by $\mathbb{Z}[i]$.

- Remark
  To verify that $S \subset R$ is a subring, we need NOT verify that $x \in S \implies x^{-1} \in S$.
  e.g. $\frac{1}{3+5i} = \frac{3-5i}{(3-5i)(3+5i)} = \frac{3-5i}{34}$.

Rings of Numbers

Example: p-adics

Let $m \geq 1$ be an integer, $R := \mathbb{Z}/m\mathbb{Z}$ with $+$ and $\cdot$ is a ring.
$*$ (out of these, we can make "p-adic numbers")

Rings of Functions

Example: Functions

Let $X = \mathbb{R}$ and $A = \mathrm{Fun}(X, \mathbb{R}) = \{f : X \to \mathbb{R} \text{ functions}\}$.
Equip A with pointwise $+$ and $\cdot$: given $f, g \in A$, define

$$A \ni f + g : x \mapsto f(x) + g(x)$$
$$A \ni fg : x \mapsto f(x)g(x)$$

$0_A \in A$ is the constant function $0_A(x) = 0_{\mathbb{R}}$, $\forall x \in A$ and $1_A \in A$ is constant $1_{\mathbb{R}}$.
Then $\mathrm{Fun}(X, \mathbb{R})$ is a ring.

Example: Continuous Functions

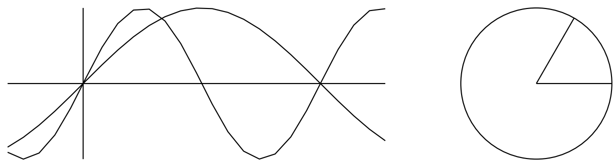
Let X be a topological space.
Define $C(X) = \{f \in \mathrm{Fun}(X, \mathbb{R}) \mid f \text{ is continuous at every } x \in X\}$, a subring of $\mathrm{Fun}(X, \mathbb{R})$.

Example: Infinitely Differentiable Functions

Let X be a manifold, e.g. $X = \mathbb{R}$.
Define $C^\infty(X) = f \in C(X) \mid f \text{ is indefinitely differentiable at every } x \in X\}$ is a subring.

Example: Periodic Functions

Let $X = \mathbb{R}$.
Define $C_{2\pi}(\mathbb{R}) = \{f \in C(\mathbb{R}) \mid f(\theta + 2\pi) = f(\theta) \text{ for all } \theta \in \mathbb{R}\}$.
e.g. $0, 1 \in C_{2\pi}(\mathbb{R})$.
For any $n \in Z$, $\cos(n\theta), \sin(n\theta) \in C_{2\pi}(\mathbb{R})$.
Note that this is the collection of all functions with period dividing 2π.



Example: Linear Combinations

Fix $N \geq 1$ and let

$$P_N = \left\{ b_0 + \sum_{n=1}^{N} b_n \cos(n\theta) + \sum_{n=1}^{N} c_n \sin(n\theta) \mid b_0, \ldots, b_n, c_0, \ldots, c_n \in \mathbb{R} \right\} \subseteq C_{2\pi}(\mathbb{R})$$

Constants 0 and 1 are in P_N and $f, g \in P_N \implies f \pm g \in P_N$.
However, for $f = g = \cos(N\theta) \in P_N$,

$$fg = \cos^2(N\theta) = \frac{1 + \cos(2N\theta)}{2}$$

Then $fg \in P_n \iff \cos(2N\theta) \in P_n$.
But, $\forall f \in P_n$, $\int_0^{2\pi} f \cdot \cos(2N\theta)\, d\theta = 0$ while $\int_0^{2\pi} \cos(2N\theta) \cdot \cos(2N\theta)\, d\theta \neq 0$.
So P_N is not a subring.
But,

$$P_\infty = \bigcup_{N \geq 1} P_N$$

is a subring.
Need to show that P_∞ is closed under $\cdot$.
By linearity, it is enough to show that $\forall m, n \geq 1$,

$$P_\infty \ni \begin{cases} \cos(m\theta)\cos(n\theta), \\ \cos(m\theta)\sin(n\theta), \\ \sin(m\theta)\sin(n\theta) \end{cases}$$

Since $e^{i\theta} = \cos(\theta) + i\sin(\theta)$,

$$\begin{aligned} \cos(m\theta)\cos(n\theta) &= \left(\frac{e^{im\theta} + e^{-im\theta}}{2}\right)\left(\frac{e^{in\theta} + e^{-in\theta}}{2}\right) \\ &= \frac{1}{4}\left(e^{i(m+n)\theta} + e^{i(m-n)\theta} + e^{i(n-m)\theta} + e^{-i(m+n)\theta}\right) \\ &= \frac{1}{4}\left(2\cos((m+n)\theta) + 2\cos((m-n)\theta)\right) \\ &= \frac{1}{2}\cos((m+n)\theta) + \frac{1}{2}\cos((m-n)\theta) \end{aligned}$$

The rest follow similarly.

Rings of Operators

Let V be a (real) vector space and $A := \mathrm{End}_{\mathbb{R}}(V) = \{T : V \to V \mid T \text{ is linear (MATH 21)}\}$.
Then A is a ring with 0_A = the zero transform and 1_A = the identity transformation.
When $V = \mathbb{R}^n$, we can choose a bsis (e.g. $(e_1, \ldots, e_n)$) and identify $A = M_{n\times n}(\mathbb{R})$.

Example

For $V = P_N$ or $V = P_\infty$,

$$\frac{d}{d\theta} : V \to V$$

is a linear opeartor., so $\frac{d}{d\theta} \in A$.
Note: unless $\dim(V) = 0, 1$, A is not a commutative ring.

Definition: Commutator (Ring)

Let A be a ring and $x, y \in A$.
The commutator $[x, y] = xy - yx$.
So x and y commute if and only if $[x, y] = 0$ in A.

Example

Let $V = C^\infty(\mathbb{R})$ with coordinates x and $A = \mathrm{End}_{\mathbb{R}}(V)$.
For

$$\begin{aligned} V \ni f(x) &\overset{T_1}{\rightsquigarrow} x \cdot f(x) \in A \\ V \ni f(x) &\overset{T_2}{\rightsquigarrow} f'(x) = \frac{d}{dx} f(x) \in A \end{aligned}$$

we have

$$\begin{aligned} [T_1, T_2]f(x) &= T_1(T_2(f(x))) - T_2(T_1(f(x))) \\ &= xf'(x) - (xf(x))' \\ &= -f(x) \end{aligned}$$

So $[T_1, T_2] = -\mathrm{Id} \in A$.

Definition: Zero Divisor

Let R be a ring.
An element $r \in R$ is called a zero divisor if $\exists s \neq 0 \in R$ such that $rs = 0_R$ or $sr = 0_R$.

Definition: Integral Domain

Say R is an integral domain if $0_R \neq 1_R$ and $\{\text{zero divisors of } R\} = \{0_R\}$.

Example

$R = \mathbb{Z}$ is an integral domain, since if $n \neq 0 \in \mathbb{Z}$, then $\forall m \in \mathbb{Z} : mn = 0 \implies n = 0$.

Counterexample

$R = \mathbb{Z}/6\mathbb{Z}$ is not an integral domain, since $\overline{2} \pmod 6$ is a nonzero zero divisors.
e.g. $\overline{2} \cdot \overline{3} = \overline{0}$ and $\overline{3} \neq \overline{0}$.

Counterexample

$R = M_{2\times 2}(\mathbb{R})$. Consider

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad B_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Then $A_1B_1 = 0 = B_1A_1$ since A_1 and B_1 project onto the x and y axes respectively.
IMAGE HERE - PROJECTION OF V ONTO AXES
Similarly, A_2 is a zero divisor since $A_2A_2 = 0$.

Definition: Nilpotency

Let R be a ring and $r \in R$.
Say r is nilpotent if $\exists N \geq 1$ such that $r^N = 0_R$ in R.
$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ is nilpotent (with $N = 2$), but
$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ is not nilpotent.

Proposition:

Let R be a ring and $r \in R$ be a non zero divisor.
Then $\forall a, b \in R$, $ra = rb \implies a = b$ and $ar = br \implies a = b$.

Proof

By distributive law, $ra = rb \implies r(a - b) = 0_R$.
Let $s := a - b$. Since, by assumption, r is not a zero divisor, $s = 0$ and $a = b$.
The proof is similar in the other case.

Corollary

In an integral domain R, cancellation law $ra = rb$ and $r \neq 0_R$ implies $a = b$.

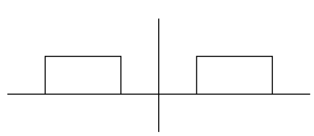
Remarks

If S is a subring of R and R is an integral domain, then S is also an integral domain.

- Example
  Since $\mathbb{C}$ is an integral domain, so are $\mathbb{Z}$ and $\mathbb{Z}[i]$.

Examples of Zero Divisors

Let $A = C(\mathbb{R})$
If f and g are zero at all overlap, they are zero divisors.



November 21, 2023

Definition: Ring

A ring is a set R equipped with two binary operations $+$ and $\cdot$ such that

1. $(R, +)$ is an abelian group.
   - Additive neutral element: $0_R = 0$.
   - Additive Inverse: $-x$.
2. $(R, \cdot)$ is a monoid.
   - Multiplicative neutral element: $1_R = 1$.
3. Distributive laws:
   - $a \cdot (b + c) = a \cdot b + a \cdot c$
   - $(b + c) \cdot a = b \cdot a + c \cdot a$

Examples

1. Numbers
2. Functions
3. Operators

Definition: Left/Right Inverse

Let R be a ring and $x \in R$
A left inverse of x is an element $l \in R$ such that $lx = 1_R$.
A right inverse of x is an element $r \in R$ such that $xr = 1_R$

Proposition: Bilateral Inverse

Suppose $x \in R$ has both a left inverse l and a right inverse r.
Then $l = r$ is a 2-sided inverse.

Proof

$$l = l1_R = l(xr) = (lx)r = 1_R r = r \quad \blacksquare$$

Definition: Unit

1. An element $x \in R$ is called invertible or a unit in R if x has a (2-sided) inverse.
2. The inverse (multiplicative) of x is denoted x^{-1}.
3. $R^{\times} = \{\text{units in } R\}$ forms a group with $\cdot$ as the binary operation called the unit group of R.

Example 1: Numbers

Let $R = \mathbb{Z}$.
An integer $n \in \mathbb{Z}$ if and only if $\exists m \in \mathbb{Z} : mn = 1$ if andonly if $n = 1$ or $n = -1$.
Therefore $\mathbb{Z}^{\times} = \{1, -1\}$ is a cyclic group of order 2.

Example 2: Numbers

$R = \mathbb{Q}, \mathbb{R},$ or $\mathbb{C} \implies R^{\times} = R \setminus \{0_R\}$.
Recall $\mathbb{R}^{\times} = \mathbb{R} \setminus \{0\}$.

Example 3: Numbers

$R = \mathbb{Z}/p\mathbb{Z}$ where p is a prime.
Have shown that $(Z/p\mathbb{Z})^{\times} = (\mathbb{Z}/p\mathbb{Z}) \setminus \{\overline{0}\}$.

Definition: Division Ring

Let R be a nonzero ring (i.e. $1_R \neq 0_R$).
Say R is a division ring if $R^{\times} = R \setminus \{0_R\}$.

Definition: Field

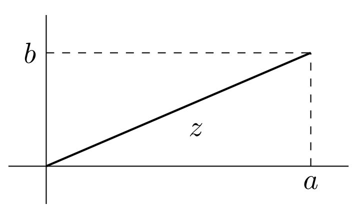
A field is a commutative division ring.

Examples

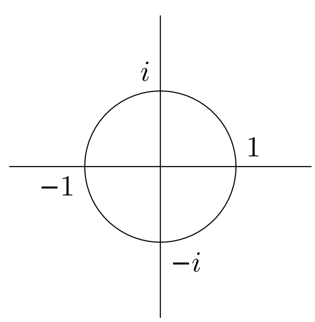
$R = \mathbb{Q}, \mathbb{R}, \mathbb{C},$ and $\mathbb{Z}/p\mathbb{Z}$ are fields.
But $\mathbb{Z}$ is not a field.

Example 5

Let $R = Z[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$.
Q: $R^{\times} = ?$
Define (a norm) $N : R \to \mathbb{N}_0$ (natural numbers with 0) by $N(a + bi) = (a + bi)(a - bi) = a^2 + b^2 (= |z^2|)$.



- Proposition
  For $R = \mathbb{Z}[i]$, $R^{\times} = \{1, -1, i, -i\} = \langle i \rangle$ is a cyclic subgroup of order 4.



- Proof
  Suppose $\alpha = a + bi \in R$ is a unit in $R = \mathbb{Z}[i]$.
  Say $\alpha\alpha' = 1$ where $\alpha' = a' + b'i \in R$.
  Since $N(\alpha\alpha') = N(\alpha)N(\alpha') = N(1) = 1$ and $N(\alpha), N(\alpha') \in \mathbb{N}_0$.
  By Example 1 (Integers) above, $N(\alpha) = 1$.

Example 6

Let $A = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\} \subset \mathbb{R}$.
Then A is a subring of $\mathbb{R}$, because $0, 1 \in A$,
$(a + b\sqrt{2}) \pm (a' + b'\sqrt{2}) = (a \pm a') + (b \pm b')\sqrt{2}$, and

$$(a + b\sqrt{2})(a' + b'\sqrt{2}) = (aa' + 2bb') + (ab' + a'b)\sqrt{2} \in \mathbb{Z}$$

if $a, a', b, b' \in \mathbb{Z}$.
Q: $\mathbb{Z}[\sqrt{2}]^\times = ?$
Define (a norm) $N'(a + b\sqrt{2}) = (a + b\sqrt{2})(a - b\sqrt{2}) = (a + b\sqrt{2})(a + b\sqrt{2})^* = a^2 - 2b^2$.
So $N' : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}$.
Note: for $\alpha = (a + b\sqrt{2}), \beta = (a' + b'\sqrt{2}) \in A$,

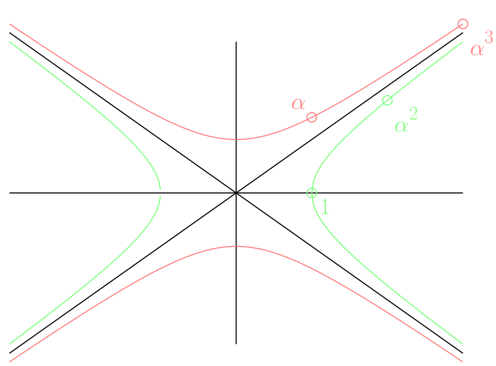
$$\begin{aligned} N'(\alpha)N'(\beta) &= \underbrace{(a + b\sqrt{2})}_{\alpha}\underbrace{(a - b\sqrt{2})}_{\alpha^*}\underbrace{(a' + b'\sqrt{2})}_{\beta}\underbrace{(a' - b'\sqrt{2})}_{\beta^*} \\ &= \alpha\beta\alpha^*\beta^* \end{aligned}$$

- Proposition
  $\mathbb{Z}[\sqrt{2}]^\times = \{a + b\sqrt{2} \mid a^2 - 2b^2 = \pm 1\}$

  - Proof
    ($\subseteq$) Suppose $\alpha = a + b\sqrt{2} \in A^\times$, say $\exists \beta \in A$: $\alpha\beta = 1$.
    Take N' of both sides, and get

$$\underbrace{N'(\alpha)N'(\beta)}_{\in \mathbb{Z}} = N'(1) = 1$$

    Therefore $N'(\alpha) \in \mathbb{Z}^\times = \{\pm 1\}$ and $a^2 - 2b^2 = \pm 1$.
    ($\supseteq$) If $a^2 - 2b^2 = \pm 1$, then for $\alpha = a + b\sqrt{2}$ and $\beta = a - 2b\sqrt{2}$, we have $\alpha\beta = \pm 1$.
    So either $\alpha\beta = 1$ or $\alpha(-\beta) = 1$.
    And either β or $-\beta$ is the sought inverse of α.
    So $\mathbb{Z}[\sqrt{2}]^\times \overset{1-1}{\longleftrightarrow} (x, y) \in \mathbb{Z}^2$ such that $x^2 - 2y^2 = \pm 1$.
    History: India in the 12th Century; later Pell's Equations



$\alpha^2 = (1+\sqrt{2})(1+\sqrt{2}) = 3+2\sqrt{2}$
$\alpha^3 = (3+2\sqrt{2})(1+\sqrt{2}) = 7+5\sqrt{2}.$

- Fact (MATH 223A; Aglebraic Number Theory)
  Dirichlet's Unit Theorem
  $\mathbb{Z}[\sqrt{2}]^\times = \{\pm(1+\sqrt{2})^n \mid n \in \mathbb{Z}\}$

Example 7: Operator

Let A be a commutative ring (e.g. $A = \mathbb{Z}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$) and $n \geq 1$ integer.
Let

$$R = M_{n\times n}(A) = \left\{ \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} \mid a_{ij} \in A \right\}$$

With "usual" matrix + and $\cdot$. R is a ring with

$$0 = \begin{bmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{bmatrix} \quad 1_R = \begin{bmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{bmatrix}$$

Q: $R^\times = ?$
$B \in R$ is a unit if and only if $\exists C \in R : BC = I_n = CB$.
"Recall" (MATH 21 or 117) $\det(B)$ can be defined as over $\mathbb{R}$, and
Define $D \in R : d_{ij} = (-1)^{i+j}\det((j,i) - \text{minor of } B)$.
And we have $BD = \det(B)\cdot \det I_n = DB$ e.g.

$$B = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \implies D = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

So $B \in R^\times$ if and only if $\det(B) \in A^\times$ (take $C = \overbrace{\frac{1}{\det(B)}}^{\in A^\times} \cdot D$)
Define:

$$\mathrm{GL}_n(A) = M_{n\times n}(A)^\times = \{B \in M_{n\times n}(A) \mid \det(B) \in A^\times\}$$

For example,

$$\mathrm{GL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in \mathbb{Z}, ad-bc = \pm 1 \right\}$$

$$\mathrm{GL}_2(\mathbb{F}_p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in \mathbb{F}_p, ad-bc \neq 0 \text{ in } \mathbb{F}_p \right\}$$

IMPORTANT FACT: $|\mathrm{GL}_2(\mathbb{F}_p)| = p(p-1)^2(p+1)$ and

$$\left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{F}_p \right\}$$

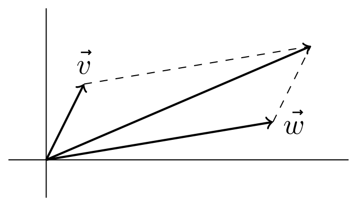
is a p-Sylow.

Definition: Quaternions

(Numbers of Operators)
$\mathbb{H} = \mathbb{R}^4 = \{(a, b, c, d) \in \mathbb{R}^4\}$ but write $a + b\hat{\imath} + c\hat{\jmath} + d\hat{k}$.

Complex Arithmetic

Addition and Subtraction as vectors.



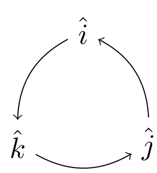
Multiplication:

1. "Force" distribution law.
2. $r \in \mathbb{R}$ commutes $i : ri = ir$.
3. $i^2 = -1$

Quaternion Arithmetic

Addition and Subtraction as vectors.
Multiplication:

1. "Force" distribution law.
2. $r \in \mathbb{R}$ commutes $\hat{\imath}, \hat{\jmath}, \hat{k} : r\hat{\imath} = \hat{\imath}r$
3. $\hat{\imath}^2 = \hat{\jmath}^2 = \hat{k}^2 = -1$



$\hat{\imath}\hat{\jmath} = \hat{k} = -\hat{\jmath}\hat{\imath}$
$\hat{\jmath}\hat{k} = \hat{\imath} = -\hat{k}\hat{\jmath}$
$\hat{k}\hat{\imath} = \hat{\jmath} = -\hat{\imath}\hat{k}$

Example

$$\begin{aligned}(2 + 3\hat{\imath})(5\hat{\imath} - 7\hat{\jmath}) &\overset{1}{=} 2(5\hat{\imath}) + 2(-t\hat{\jmath}) + (3\hat{\imath})(5\hat{\imath}) + (3\hat{\imath})(-7\hat{\jmath}) \\ &= 10\hat{\imath} - 14\hat{\jmath} + 15\hat{\imath}^2 - 21\hat{\imath}\hat{\jmath} \\ &= -15 + 10\hat{\imath} - 14\hat{\jmath} - 21\hat{k}\end{aligned}$$

Definition: Quaternion Conjugate

Let $q = a + b\hat{i} + c\hat{j} + d\hat{j} \in \mathbb{H}$.
The quaternion conjugate $q^* = a - b\hat{i} - c\hat{j} - d\hat{j} \in \mathbb{H}$
Note $(q^*)^* = q$
Define $N''(q) = qq^* a^2 + b^2 + c^2 + d^2 = q^* q \in \mathbb{R}_{\geq 0}$.

Proposition: Quaternions Form a Division Ring

$\mathbb{H}$ is a division ring (not a field, since $\hat{i}\hat{j} \neq \hat{j}\hat{i}$)

Proof

Let $q \in \mathbb{H}$ be nonzero, then $N''(q) = r > 0$ is a real number.
Then $qq^* = r = q^* q$. Multiplying through by $1/r$, which commutes with both q and q^*,

$$q\left(q^* \frac{1}{r}\right) = 1 \quad \text{and} \quad \left(\frac{1}{r} q^*\right) q = 1$$

So $\frac{q^*}{N''(q)}$ is the 2-sided inverse.

Example

$(1 + 2\hat{i} + 3\hat{j} + 4\hat{k} = \frac{1}{1^2+2^2+3^2+4^2}(1 - 2\hat{i} - 3\hat{j} - 4\hat{k})$.

November 28, 2023

Definition: Center of a Ring

Let R be a ring.
The center (or centre or zentrum) $Z(R) = \{r \in R \mid rx = xr, \forall x \in R\}$.
Fact: $Z(R)$ is a subring of R.
Sketch of Proof: $0_R, 1_R \in Z(R)$, $x, y \in Z(R) \implies x \pm y, xy \in Z(R)$.

Example 0:

If R is commutative if and only if $Z(R) = R$.

Example 1:

$R = \mathbb{H} = \{a + b\hat{i} + c\hat{j} + d\hat{k} \mid a, b, c, d \in \mathbb{R}\}$
What is $Z(\mathbb{H})$?
By construction, $Z(\mathbb{H}) \supseteq \mathbb{R} = \{a + 0\hat{i} + 0\hat{j} + 0\hat{k} \mid a \in \mathbb{R}\}$.
Claim: $Z(\mathbb{H}) = \mathbb{R}$.

- Proof
  ($\subseteq$) Let $a + b\hat{i} + c\hat{j} + d\hat{k} \in Z(\mathbb{H})$.
  Then

$$\begin{aligned}
&1. \quad (a + b\hat{i} + c\hat{j} + d\hat{k})\hat{i} = \hat{i}(a + b\hat{i} + c\hat{j} + d\hat{k}) \\
&2. \quad (a + b\hat{i} + c\hat{j} + d\hat{k})\hat{j} = \hat{j}(a + b\hat{i} + c\hat{j} + d\hat{k}) \\
&3. \quad (a + b\hat{i} + c\hat{j} + d\hat{k})\hat{k} = \hat{k}(a + b\hat{i} + c\hat{j} + d\hat{k})
\end{aligned}$$

Expand 1.

$$-b + a\hat{\imath} + d\hat{\jmath} - c\hat{k} = -b + a\hat{\imath} - d\hat{\jmath} + c\hat{k}$$

Therefore $c = 0$ and $d = 0$.
Left as an exercise: expand 2. and 3. to demonstrate $b = 0$. ■

Definition: Ring Homomorphism

Let R and S be rings.
A function $f : R \to S$ is called a ring homomorphism if

1. $f(r_1 + r_2) = f(r_1) + f(r_2), \forall r_1, r_2 \in R$.
   (implies that $f(0_R) = 0_S$ and $f(-r) = -f(r)$, $\forall r \in R$)

2. $f(r_1 r_2) = f(r_1)(f(r_2), \forall r_1, r_2 \in R$ and $f(1_R) = 1_S$.
   (implies $f(r^{-1}) = (f(r))^{-1}, \forall r \in R^{\times}$)

Example 0:

$R \xrightarrow{\text{Id}} R$ is a ring homomorphism.
Fun exercise: If $\mathbb{R} \xrightarrow{f} \mathbb{R}$ is a ring homomorphism, then $f = \text{Id}$.

Example 1:

If R' is a subring of R, then the inclusion $i : R' \hookrightarrow R$ is a ring homomorphism.
e.g. $\mathbb{Z}[\sqrt{2}] \xrightarrow{\text{incl.}} \mathbb{R}$

Example 2:

In general, a ring homomorphism does not need to be injective or surjective.
Let $R = \mathbb{Z}[\sqrt{2}]$.
Define $f : R \to R$ by $f(a + b\sqrt{2}) = a - b\sqrt{2}$.
Then f is a ring homomorphism (automorphism).
Need to check that $\forall a_1, a_2, b_1, b_2 \in \mathbb{Z}$:

1. $f((a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2})) = f(a_1 + b_1\sqrt{2}) + f(a_2 + b_2\sqrt{2})$.

2. $f((a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2})) = f(a_1 + b_1\sqrt{2})f(a_2 + b_2\sqrt{2})$

3. $f(1 + 0\sqrt{2}) = 1 + 0\sqrt{2}$

- Proof of 1

$$\begin{aligned}
f((a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2})) &= f((a_1 + a_2) + (b_1 + b_2)\sqrt{2} \\
&= (a_1 + a_2) - (b_1 + b_2)\sqrt{2} \\
&= (a_1 - b_1\sqrt{2}) + (a_2 - b_2\sqrt{2}) \\
&= f(a_1 + b_1\sqrt{2}) + f(a_2 + b_2\sqrt{2})
\end{aligned}$$

- Proof of 2

$$\begin{aligned}
f((a_1+b_1\sqrt{2})(a_2+b_2\sqrt{2})) &= (a_1a_2+2b_1b_2)-(a_1b_2+a_2b_1)\sqrt{2} \\
&= (a_1-b_1\sqrt{2})(a_2-b_2\sqrt{2}) \\
&= f(a_1+b_1\sqrt{2})f(a_2+b_2\sqrt{2})
\end{aligned}$$

- Proof of 3
  $1+0\sqrt{2} = 1-0\sqrt{2}$

- Remark
  Id and f are the only ring homomorphisms $\mathbb{Z}[\sqrt{2}] \xrightarrow{g} \mathbb{Z}[\sqrt{2}]$.
  Prove: $g(\sqrt{2}) = \sqrt{2}$ or $-\sqrt{2}$.

Example 3

Let X and Y be topological spaces (e.g. $X \subseteq R^m$, $Y \subseteq R^n$)
Let $\phi : X \to Y$ be a continuous map.
We have the map $C(X) \xleftarrow{\phi^*} C(Y) = \{f : Y \to \mathbb{R} \mid \text{continuous everywhere}\}$.
If $f : Y \to \mathbb{R}$, then $f \circ \phi = \phi^*(f) : X \xrightarrow{\phi} Y \xrightarrow{f} \mathbb{R}$.
Then ϕ^* is a ring homomorphism.

- Proof of Addition
  Left as an exercise.

- Proof of Multiplication
  Let $f_1, f_2 \in C(Y)$ and want to verify that $\phi^*(f_1f_2) = \phi^*(f_1)\phi^*(f_2)$.
  Both sides are elements in $C(X)$, so need to verify

$$[\phi^*(f_1f_2)](x) = [\phi^*(f_1)\phi^*(f_2)](x), \forall x \in X$$

$$\begin{aligned}
((f_1f_2)\circ\phi)(x) &= (f_1f_2)(\underbrace{\phi(x)}_{\in Y}) \\
&= f_1(\phi(x))f_2(\phi(x)) \\
&= (\underbrace{\phi^*f_1}_{\in C(X)})(x)(\underbrace{\phi^*f_2}_{\in C(X)})(x) \\
&= [(\phi^*f_1)(\phi^*f_2)](x)
\end{aligned}$$

Example 4

IMAGE HERE - DOUBLE TORUS SYMMETRIC ABOUT AN AXIS
Then $C(X) \xleftarrow{\phi^*} C(X)$.

Non-example 4'

Let $R = \mathbb{H}$ and let $f : R \to R$ be defined by $f(q) = q^*$.
That is, if $q = a + b\hat{i} + c\hat{j} + d\hat{k}$ then $q^* = a - b\hat{i} - c\hat{j} - d\hat{k}$.

- Proof of Addition
  $f(q_1+q_2) = f(q_1)+f(q_2), \forall q_1, q_2 \in \mathbb{H}$ (cf. $\mathbb{Z}[\sqrt{2}]$)

- Failure of Multiplication
  $f(q_1 q_2) \neq f(q_1) f(q_2)$ in general.
  If $q_1 = \hat{i}$ and $q_2 = \hat{j}$, then

$$(\hat{i}\hat{j})^* = (\hat{k})^* = -\hat{k} \neq \hat{k} = (-\hat{i})(-\hat{j})$$

  So $f = *$ is not a ring homomorphism.

Definition: Ring Anti-Homomorphism

Addition is unchanged, but $f(r_1 r_2) = f(r_2) f(r_1)$.

Example

Claim $* = f$ above is an antihomomorphism.
First, $1^* = 1$.
If $q_1 = q_1^{\prime} + q_1^{\prime\prime}$ and if we know $(q_1^{\prime} q_2)^* = q_2^* (q_1^{\prime})^*$ and $(q_1^{\prime\prime} q_2)^* = q_2^* (q_1^{\prime\prime})^*$, then we conclude

$$(q_1 q_2)^* = q_2^* q_1^*, \forall q_1, q_2 \in \mathbb{H}$$

by adding the two and using the distributive law.
Similarly for $q_2 = q_2^{\prime} + q_2^{\prime\prime}$.
Therefore, it is enough to show that $q_1 \in \{a, b\hat{i}, c\hat{j}, d\hat{k}\}$ and $q_2 \in \{t, x\hat{i}, y\hat{j}, z\hat{k}\}$.
Many cases are trivial (e.g. a commutes with everything).
Consider $q_1 = c\hat{j}$ and $q_2 = z\hat{k}$, then

$$((c\hat{j})(z\hat{k}))^* = (cz\hat{i})^* = (-cz)\hat{i} = cz\hat{k}\hat{j} = (-z\hat{k})(-c\hat{j} = (z\hat{k})^* (c\hat{j})^*$$

Proposition:

Let $u \in R^{\times}$.
Then the map

$$\begin{aligned} \operatorname{Int}(u) : R &\to R \\ x &\mapsto u x u^{-1} \end{aligned}$$

is a ring homomorphism.

Proof:

1. Addition

$$\operatorname{Int}(u)(r_1 + r_2) = u(r_1 + r_2)u^{-1} = (ur_1 + ur_2)u^{-1} = ur_1 u^{-1} + ur_2 u^{-1} = \operatorname{Int}(u)(r_1) + \operatorname{Int}(u)(r_2)$$

2. Product

$$u r_1 r_2 u^{-1} = (u r_1 u^{-1})(u r_2 u^{-1})$$

$$u 1 u^{-1} = 1$$

Note $\operatorname{Int}(u^{-1})$ is the 2-sided inverse of $\operatorname{Int}(u)$.

Example 5

Let $R = \mathbb{H}$.
Recall

$$
\begin{aligned}
N : \mathbb{H}^{\times} &\to \mathbb{R}_{>0} \\
q &\mapsto N(q) = qq^* = q^* q
\end{aligned}
$$

$N : H^{\times} \to \mathbb{R}_{>0}$ is a group homomorphism.
i.e. $N(q_1 q_2) = N(q_1)N(q_2), \forall q_1, q_2 \in \mathbb{H}^{\times}$.

Proof

$$
\begin{aligned}
N(q_1 q_2) &= (q_1 q_2)(q_1 q_2)^* \\
&= (q_1 q_2)(q_2^* q_1^*) \\
&= q_1 (q_2 q_2^*) q_1^* \\
&= q_1 \underbrace{N(q_2)}_{\in \mathbb{R} = Z(\mathbb{H})} q_1^* \\
&= q_1 q_1^* N(q_2) \\
&= N(q_1) N(q_2)
\end{aligned}
$$

Definition:

$\mathbb{H}^{\times 1} = \ker(\mathbb{H}^{\times} \xrightarrow{N} \mathbb{R}_{>0}) = \{a + b\hat{i} + c\hat{j} + d\hat{k} \mid a^2 + b^2 + c^2 + d^2 = 1\} = S^3$ is a (mult) group.
Note, for $u \in H^{\times 1}$, $u^{-1} = u^*$.

Definition:

$V = \{q \in \mathbb{H} \mid q + q^* = 0\} = \{x\hat{i} + y\hat{j} + z\hat{k} \mid x, y, z \in \mathbb{R}\} = \mathbb{R}^3$.

Proposition:

For $u \in \mathbb{H}^{\times 1}$, write $R(u) = \mathrm{Int}(u)$.
Then $R(u) : \mathbb{H} \to \mathbb{H}$ is a linear map (MATH 21) and $R(u)V \subseteq V$.

Proof

Since Int is a ring automorphism, for $a_1, a_2 \in \mathbb{R}$ and $v_1, v_2 \in \mathbb{H}$,

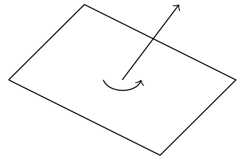
$$
R(u)(a_1 v_1 + a_2 v_2) = [R(u)(a_1)][R(u)(v_1)][R(u)(a_2)][R(u)(v_2)] = a_1 R(u)(v_1) + a_2 R(u)(v_2)
$$

So $R(u)$ is linear.
Let $q \in V$ (i.e. $q + q^* = 0$). Then

$$
(R(u)q) + (R(u)q)^* = uqu^* + (uqu^*)^* = uqu^* + uq^*u^* = u(q + q^*)u^* = 0
$$

Proposition:

Let $u \in \mathbb{H}^{\times 1}$, write $u = (\cos(\theta)) + (\sin(\theta))\hat{v}$ where $\theta \in \mathbb{R}$ and $\hat{v} \in V \cap \mathbb{H}^{\times 1} = S^2$.
Then $R(u) : \mathbb{R}^3 = V \to V = \mathbb{R}^3$ is the rotation of $\mathbb{R}^3$ with the axis $\hat{v}$ by the angle 2θ.



November 30, 2023

Definition: Ideal

Let I be an additive subgroup of a ring R. Say that I is

1. a left ideal of R if $\forall x \in I$, $\forall r \in R$, $rx \in I$ (i.e. closed under left multiplication by R)
2. a right ideal of R if $\forall x \in I$, $\forall r \in R$, $xr \in I$ (i.e. closed under right multiplication by R)
3. a (bilateral) ideal of R if I is both a left ideal and a right ideal.

Remarks

1. When R is commutative, the three notions coincide.
2. The only subring that is a left or a right ideal is R.

Example 0

Let $X \subseteq R$ be a subset.
The left ideal generated by X

$$RX = {}_R(X) = \left\{ \sum_{i=1}^{n} r_i x_i \mid n \in \mathbb{N}_0, r_i \in R, x_i \in X \right\}$$

By convention, when $n = 0$ nothing is summed.
The right ideal generated by X

$$XR = (X)_R = \left\{ \sum_{i=1}^{n} x_i s_i \mid n \in \mathbb{N}_0, x_i \in X, s_i \in R \right\}$$

The (bilateral) ideal generated by X

$$(X) = \left\{ \sum_{i=1}^{n} r_i x_i s_i \mid n \in \mathbb{N}_0, x_i \in X, r_i, s_i \in R \right\}$$

Definition: Principle Ideal

If $X = \{x\}$, then write $(X) = (\{x\}) = (x)$ and call it the principle ideal generated by X.

Proposition:

Let D be a division ring (e.g. $\mathbb{R}, \mathbb{F}_p, \mathbb{H}$).
Then the only left (respectively right) ideals of D are $\{0\}$ and D.

Proof

Let I be a nonzero left ideal, so $\exists x \in D$ such that $x \in 0$ and $x \in I$.
Then since D is a division ring, x has an inverse y such that $xy = 1_D = yx$.
Since I is a left ideal, take $r = y$ and $x = x \in I$.
In the definition, we get $1_D \in I$, but then for any $r \in D$, $r = r1_D \in I$.
The argument for right ideals follows similarly. ■

Proposition:

Let $R = \mathbb{Z}$.
Then the ideals of $\mathbb{Z}$ are exactly $a\mathbb{Z}$ where $a \in \mathbb{N}_0$.

Proof

For any $a \in \mathbb{Z}$, the additive subgroup $a\mathbb{Z} = \{na \mid n \in \mathbb{Z}\}$ is indeed an ideal since $\forall r \in \mathbb{Z}$, $\forall na \in a\mathbb{Z}$, $r(na) = (rn)a \in a\mathbb{Z}$.
Conversely, if I is any ideal of $\mathbb{Z}$, it is an additiive subgroup of $\mathbb{Z}$; in Group Theory we have shown that $I = a\mathbb{Z}$ for some $a \geq 0$. ■

Definition: Principle Ideal Domain (PID)

Let R be an integral domain ($0_R \neq 1_R$ and the only zero divisors of R is 0_R).
Say that R is a principle ideal domain (PID) if any ideal in R is a principle ideal.

Example 1

Following from the previous proposition, $\mathbb{Z}$ is a PID.

Example 2

Let F be a field (e.g. $\mathbb{C}$ or $\mathbb{F}_p$) and $R = M_{2\times2}(F) = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in F\right\}$ is a noncommutative ring.

$$I_1 = \left\{\begin{bmatrix} x & 0 \\ y & 0 \end{bmatrix} \mid x, y \in F\right\} \quad I_2 = \left\{\begin{bmatrix} 0 & 0 \\ x & y \end{bmatrix} \mid x, y \in F\right\}$$

are additive subgroups of R.
Then I_1 is a left ideal but NOT a right ideal of R while I_2 is only a right ideal.
Let $r = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ and $z = \begin{bmatrix} x & 0 \\ y & 0 \end{bmatrix} \in I_1$ be arbitrary. Then $rz = \begin{bmatrix} ax + by & 0 \\ cx + dy & 0 \end{bmatrix} \in I_1$.
However, for $z = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and $r = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $zr = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \notin I_1$ if $b \neq 0_F$.
Exercise: Prove I_2 is a right ideal but not a left ideal.

Proposition:

The only (bilateral) ideals of $M_{2\times2}(F)$ are $\{0\}$ and R.

Sketch of Proof

Let I be a nonzero, bilateral ideal, say $\exists \begin{bmatrix} a & b \\ c & d \end{bmatrix} \neq 0$ in I.
Note $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} c & d \\ a & b \end{bmatrix}$ while $\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} b & a \\ d & c \end{bmatrix}$ and $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} d & c \\ b & a \end{bmatrix}$.
So, without loss of generality, we may show that $a \neq 0$ gives

$$\begin{bmatrix}1&0\\0&0\end{bmatrix}\begin{bmatrix}a&b\\c&d\end{bmatrix}\begin{bmatrix}1&0\\0&0\end{bmatrix}=\begin{bmatrix}a&0\\0&0\end{bmatrix}\implies\begin{bmatrix}\frac{1}{a}&0\\0&0\end{bmatrix}\begin{bmatrix}a&0\\0&0\end{bmatrix}=\begin{bmatrix}1&0\\0&0\end{bmatrix}\in I$$

Repeating this trick gives

$$\begin{bmatrix}1&0\\0&0\end{bmatrix},\begin{bmatrix}0&1\\0&0\end{bmatrix},\begin{bmatrix}0&0\\1&0\end{bmatrix},\begin{bmatrix}0&0\\0&1\end{bmatrix}\in I$$

Therefore, $I = R$.

Definition: Quasisimple Ring

Say a ring R is quasisimple if the only ideals in R are $\{0\}$ and R (e.g. division rings, $M_{2\times 2}(F)$).

Construction:

Let I be an ideal of R. Then R/I (the quotient group for $+$) has a natural ring structure:

$$(r_1 + I)(r_2 + I) := r_1 r_2 + I$$

Well-defined: If $r_1', r_2' \in R$ satisfy (1) $r_1' + I = r_1 + I$ and (2) $r_2' + I = r_2 + I$, then we want $r_1' + r_2' + I = r_1 r_2 + I$.
(1) says $r_1' - r_1 = x \in I$ and (2) says $r_2' - r_2 = y \in I$. So $r_1' = r_1 + x$ and $r_2' = r_2 + y$. Then

$$r_1' r_2' = (r_1 + x)(r_2 + y) = r_1 r_2 + r_1 y + x r_2 + xy$$

$r_1 y \in I$, since I is a left ideal; $x r_2 \in I$ since I is a right ideal; $xy \in I$ since it is an ideal.
Since I is an additive subgroup, $r_1' r_2' + I = r_1 r_2 + I$.
Need to verify the axioms for a ring:

$$((r_1 + I)(r_2 + I))(r_3 + I) = (r_1 + I)((r_2 + I)(r_3 + I))$$

This follows from $(r_1 r_2) r_3 = r_1 (r_2 r_3)$.
$1_R + I$ is the multiplicative neutral element.
Distribution laws: similarly follow from the distribution laws of R itself.

Definition: Canonical Quotient Homomorphism

The canonical quotient homomorphism

$$\begin{aligned} R &\xrightarrow{\pi} R/I \\ r &\longmapsto r + I \end{aligned}$$

Definition / Proposition: Kernel of a Ring Homomorphism

Let $\phi : R \to S$ be a ring homomorphism.
The kernel of ϕ is $\ker(\phi) = \{r \in R \mid \phi(r) = 0_S\}$ is a bilateral ideal.
cf. $G \xrightarrow{\phi} H$ group homomorphisms, $\ker(\phi) \trianglelefteq G$.

Proof

$\ker(\phi)$ is an additive subgroup and if $x \in \ker(\phi)$ and $\forall r \in R$, then $\phi(rx) = \phi(r)\phi(x) = \phi(r)0 = 0$ and similarly $\phi(xr) = 0$. ■

Theorem: Universal Mapping Property (Rings)

Let R be a ring and I a bilateral ideal.
Then for any ring S, there is a natural correspondence

$$\left\{f \in \mathrm{Hom}_{\text{ring}}(R,S) \mid \ker(f) \geq I\right\} \leftrightarrow \mathrm{Hom}_{\text{ring}}(R/I,S)$$

Sketch of Proof

$(\longrightarrow)$ Given such f, define the function $\overline{f} : R/I \to S$ by $r + I \mapsto f(r)$. Show well-defined and is a ring homomorphism.
$(\longleftarrow)$ given $R/I \xrightarrow{\phi} S$, $f = \phi \circ \pi$.

- Recall: Universal Mapping Property (Groups)
  $G \trianglerighteq N$, then for any group H

$$\left\{f \in \mathrm{Hom}_{\text{group}}(G,H) \mid \ker(f) \geq N\right\} \leftrightarrow \mathrm{Hom}_{\text{group}}(G/N,H)$$

Theorem: Correspondence & 2nd Isomorphism for Ideals

Let I be an ideal of R.

Part 1

$$\{\text{bilateral ideals } J \text{ of } R \text{ that contain } I\} \leftrightarrow \{\text{bilateral ideals of } \overline{J} \text{ of } R/I\}$$

$J \mapsto J/I$ and $\overline{J} \mapsto \pi^{-1}(\overline{J})$.

Part 2

$R/J \xrightarrow{\sim} (R/I)/(J/I)$ as rings.
Proof omitted.

Operations on Ideals

Let I and J be ideals of R.

1. $I \cap J$ is an ideal of R.

2. $I + J = \{x + y \mid x \in I, y \in J\}$ is an ideal of R.

3. $IJ = \left\{\sum_{k=1}^{n} x_k y_k \mid n \in \mathbb{N}_0, x_k \in I, y_k \in J\right\}$ is an ideal of R.

Example 3

Let $R = \mathbb{Z}$, $I = a\mathbb{Z}$ and $J = b\mathbb{Z}$ where $a, b \geq 0$.
Then $I \cap J = \{n \in \mathbb{Z} \mid a|n \text{ and } b|n\} = \mathrm{lcm}(a,b)\mathbb{Z}$.
$IJ = \left\{\sum_{k=1}^{n}(ax_k)(by_k) \mid n \in \mathbb{N}_0, x_k, y_k \in \mathbb{Z}\right\} = (ab)\mathbb{Z}$.
$I + J = \{ax + by \mid x, y \in \mathbb{Z}\} = \gcd(a,b)\mathbb{Z}$ (MATH 110).

- Example 4: Euclidean Algorithm
  If $a = 8$ and $b = 22$, then $22 = 2(8) + 6$ and $8 = 1(6) + 2$.
  Then $2 = 8 - 6 = 8 - (22 - 2(8)) = 3(8) + (-1)22$.

December 5, 2023

Recall

For $R = \mathbb{Z}$,

1. Let $a, b \in \mathbb{Z}$. Say a divides b (and write $a|b$) if $\exists c \in \mathbb{Z}$ such that $b = ac$.

   Note that in noncommutative rings, one must specify left or right divisibility.

2. Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}$ ("modulus"). Write $a \equiv b \pmod{m}$ if $m|(a-b)$.

   $\equiv$ is an equivalence relation and, for any $c \in \mathbb{Z}$, $a \pm c \equiv b \pm c \pmod{m}$ and $ac \equiv bc \pmod{m}$.
   $\mathbb{Z}/m\mathbb{Z}$ is a ring.

3. $p > 0$ in $\mathbb{Z}$ is a prime number if $p \neq 1$ and satisfies the two equivalent conditions:

   (a) if $p = ab$ for some $a, b \in \mathbb{Z}$, then either $a = \pm 1$ or $b = \pm 1$.

   (b) if $p|ab$ for any $a, b \in \mathbb{Z}$, then $p|a$ or $p|b$.

      The equivalence between (3a) and (3b) relies on

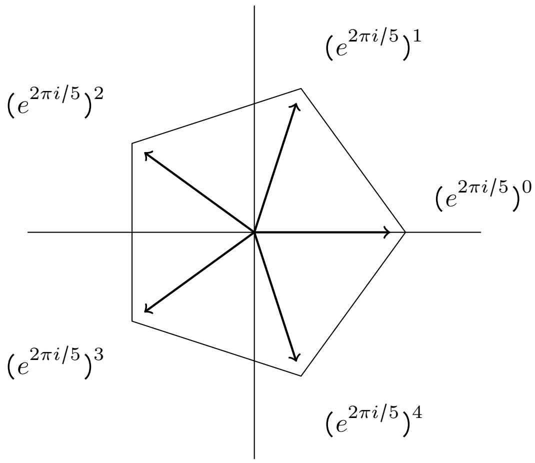
Theorem:

Any nonzero integer n can be uniquely written:

$$n = \pm 2^{e_2} \cdot 3^{e_3} \cdot 5^{e_5} \cdot \cdots \cdot p^{e_p} \cdot \cdots$$

where $e_p \in \mathbb{N}_0$ are exponents, and all but finitely many equal zero.
This can be generalized to general rings, such as
:

$$\mathbb{Z}\left[e^{2\pi \text{ i/p}}\right]$$



If an analogue of the theorem holds for R_p, then we get Fermat's Last Theorem.

On Commutative Rings

Let R be a commutative ring

1. Let $a, b \in \mathbb{R}$. Say a divides b (and write $a|b$) if $\exists c \in R$ such that $b = a \cdot c$.

   Note that in noncommutative rings, one must specify left or right divisibility.

2. Let $a, b \in R$ and $I \subseteq R$ an ideal ("modulus"). Write $a \equiv b \pmod{I}$ if $I \ni (a - b)$.

   $\equiv$ is an equivalence relation and, for any $c \in R$, $a \pm c \equiv b \pm c \pmod{I}$ and $ac \equiv bc \pmod{I}$.

3. Let $\pi \in R\{0\}$ and suppose $\pi \notin R^\times$.

   (a) Say π is an irreducible element if $\pi = ab$ for some $a, b \in R$, then $a \in R^\times$ or $b \in R^\times$.

   (b) Say π is a prime element if $\pi | ab$ for any $a, b \in R$, then $\pi | a$ or $\pi | b$.

Proposition:

Let R be an integral domain and let $x \in R$ be a nonzero unit element.
If x is a prime element, then x is irreducible.

Proof

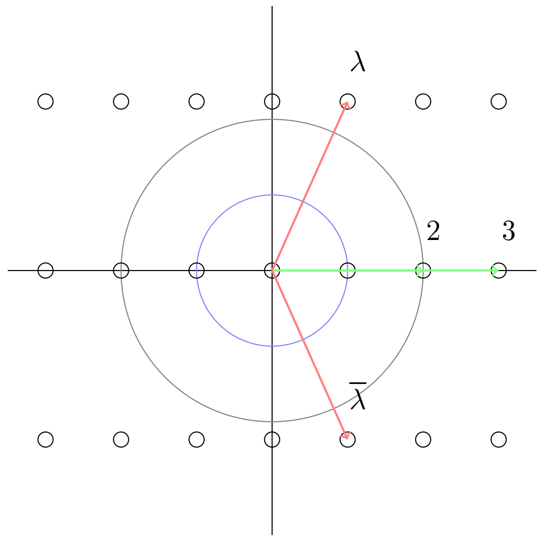
Suppose x is a prime element and that (1) $x = ab$ for some two $a, b \in R$.
Then $x|ab$, since $ab = x \cdot 1$. By assumption of primarlity, $x|a$ or $x|b$.
Without loss of generality, we may assume that $x|a$. Say (2) $a = x \cdot c$ for some $c \in R$.
Combine (1) and (2), and get $x = (xc)b = x(cb)$.
Since $x \neq 0$ and R is an integral domain, we can cancel x and get $1 = cb = bc$.
Therefore $b \in R^\times$. ■

Converse

The converse (irreducible implies prime) is generally false.

- Example

$R = \mathbb{Z}[\sqrt{5}i] = \{a + b\sqrt{5}i \mid a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C} = \mathbb{Z}[i]$.



Define $N : R \to \mathbb{N}_0$ by $N(a + b\sqrt{5}i) = |a + b\sqrt{5}i|^2 = a^2 + 5b^2$.
Note that $N(\alpha\beta) = N(\alpha)N(\beta)$, $\forall \alpha, \beta \in R$.
$\{\alpha \in R \mid N(\alpha) = 1\} = \{\pm 1\} = R^\times$
There are no elements of R with norm 2 or 3.
Then $2, 3, \lambda, \overline{\lambda}$ are irreducible elements of $R = \mathbb{Z}[\sqrt{5}i]$, but not prime elements.

Proof (Irreducibility)

Start with λ. Suppose $\lambda = \alpha\beta$ for some $\alpha, \beta \in R$. Take N.

$$\begin{aligned} N(\lambda &= N(\alpha)N(\beta) \\ 6 &= \underbrace{N(\alpha)}_{\in \mathbb{N}_0}\underbrace{N(\beta)}_{\in \mathbb{N}_0} \end{aligned}$$

Therefore, $(N(\alpha), N(\beta)) \in \{(1,6), (2,3), (3,2), (6,1)$, but no elements of R are of norm 2 or 3.
So $N(\alpha) = 1$ or $N(\beta) = 1$, which implies $\alpha \in R^\times$ or $\beta \in R^\times$.
As an exercise, show that $\overline{\lambda}, 2, 3$ are irreducible.

Proof (Primacy)

2 is not a prime element of $R = \mathbb{Z}[\sqrt{5}i]$.
$\lambda\overline{\lambda} = 6 = 2 \cdot 3$, so $2 | \lambda\overline{\lambda}$, but if $2|\lambda$ or $2|\overline{\lambda}$ then, by the multiplicativity of N we would have

$$4 = N(2) | N(\lambda) = N(\overline{\lambda}) = 6$$

in $\mathbb{Z}$, which is absurd.
Therefore 2 is not a prime element.

Definition: Associates

Let R be an integral domain.
Two elements x and y are associates in R and we write $x \sim y$ if $x|y$ and $y|x$.
Equivalently, $x = y \cdot u$ for some $u \in R^\times$.
Equivalently, $x, y \in R$ lie in the same orbit in the action of $R^\times$ on R by multiplication.
In dealing with divisibility, an element is as good as any of its associates.

Proposition:

Let R be an integral domain, $r, s \in \mathbb{N}_0$, and $p_1, \ldots, p_r$, $q_1, \ldots, q_s$ prime elements of R. Suppose

$$(*) \quad p_1 \cdots p_r = q_1 \cdots q_s$$

Then $r = s$ and, after renumbering, we have $p_i \sim q_i$, $i = 1, \ldots, r$.

Remark

The proposition becomes false when "prime" is replaced with "irreducible".

Proof

Induction on r.
If $r = 0$, $1 = q_1(q_2 \cdots q_s)$, which implies (if $s > 0$), that q_1 is a unit which is absurd.
Suppose we know the proposition for all the values smaller than r.
Note $p_1 | q_1 \cdots q_s \implies p_1 | q_i$ for some $i = 1, \ldots, s$.
Then $q_1 = p_r x$, $\exists x \in R$. But q_1, being prime, is irreducible. Hence $x \in R^\times$.
Therefore, $p_r \sim q_i$ for some i. So reorder the q's, and we may assume that $p_r \sim q_s$ so $p_r = q_s \cdot u$. Substituting and canceling gives

$$\begin{aligned} p_1 \cdots p_{r-1} p_r &= q_1 \cdots q_{s-1} q_s \\ p_1 \cdots p_{r-1} q_s u &= q_1 \cdots q_{s-1} q_s \\ p_1 \cdots (p_{r-1} u) &= q_1 \cdots q_{s-1} \end{aligned}$$

Using the inductive hypothesis, we get $r - 1 = s - 1$. Therefore $r = s$ and after renumbering, $p_i \sim q_i$ for all i.

Definition: Unique Factorization Domain (UFD)

Let R be an integral domain.
Say R is a unique factorization domain if every nonzer, nonunit$x \in R$ can be written as some product PRIME elements.

Definition: Maximal Ideal

Let R be a commutative ring, and $I \subsetneq R$ an ideal.
Say I is a maximal ideal if for any ideal $J \supseteq I$, we necessarily have $J = I$ or $J = R$.
Equivalenetly, R/I is a field.

Definition: Prime Ideal

Let R be a commutative ring, and $I \subsetneq R$ an ideal.
Say I is a prime ideal if R/I is an integral domain.
Equivalently, $\forall a, b \in R$, $ab \in I \implies a \in I$ or $b \in I$.

Definition: Ascending Chain of Ideals

Let R be a ring.
An ascending chain of ideals is

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq I_n \subseteq \cdots$$

where each I_k is an ideal of R.

Definition: Noetherian Ring

Say R is a Noetherian ring if every ascending chain of ideals is stationary.

$$\exists N >> 0 : \quad I_{N+k} = I_n, \quad \forall k \geq 0$$

Theorem: A Principle Ideal Domain is a Unique Factorization Domain

Lemma

Let R be a PID, $x \in R \setminus \{0\}$, $x \notin R^{\times}$. Then the following are equivalent

1. (x) is maximal.

2. (x) is a prime ideal.

3. x is a prime element.

4. x is an irreducible element.

- Proofs
  (1) $\implies$ (2) since a field is an integral domain.
  (2) $\implies$ (3) since $ab \in (x) \iff x|ab$, $a \in (x) \iff x|a$, and $b \in (x) \iff x|b$.
  (3) $\implies$ (4) has been proven above.
  (4) $\implies$ (1)
  Let x be an irreducible element and $I := (x)$.
  Suppose J is an ideal containing I. Since R is a PID, $J = (y)$ for some $y \in R$.
  So $x \in (x) \subseteq (y) = \{yr \mid r \in R\}$.
  Write $x = yr$ for some $r \in R$.
  Since x is irreducible, either $y \in R^{\times}$ or $r \in R^{\times}$.
  If $y \in R^{\times}$, then $J = (y) = R$; if $r \in R^{\times}$, then $x \sim y \implies I = (x) = (y) = J$.
  Therefore I is maximal.

Proposition: A PID is Noetherian

Say $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$ is an ascending chain.
Write it as $(\alpha_1) \subseteq (\alpha_2) \subseteq \cdots \subseteq (\alpha_n) \subseteq \cdots$.
Claim: $\bigcup_{n=1}^{\infty} I_n$ is an ideal of R.

- Proof of Claim
  Let $x, y \in J$ and $r \in R$ be arbitrary.
  By definition, $x \in I_n$ and $y \in I_m$ for some $m, n \in \mathbb{N}$
  Take $k := \max\{m, n\}$ and $x, y \in I_k$.
  Since I_k is an ideal, $x \pm y$, $rx \in I_k \subseteq J$.

- Proof of Proposition So

$$J = \bigcup_{n=1}^{\infty} (\alpha_n) \underset{R=\text{PID}}{=} (\beta) \ni \beta$$

  for some $\beta \in R$. But then $\beta \in (\alpha_m)$ for some $m \in \mathbb{N}_0$.
  Therefore $J = (\beta) \subseteq (\alpha_m) = I_m$, and $I_{M+k} = I_m$, $\forall k \geq 0$.

December 7, 2023

Theorem: PID is UFD.

A Principle Ideal Domain is a Unique Factorization Domain.

Lemma 1:

In a Principle Ideal Domain, an element $x \in R$ is prime if and only if x is irreducible.

Lemma 2:

Any Principle Ideal Domain is Noetherian.

Proof

Let R be a Principle Ideal Domain. We need to prove every $x \in \mathbb{R} \setminus (\{0\} \cup R^{\times})$ admits a prime decomposition.
Thanks to Lemma 2, we only need to show that x is a product of irreducibles.
Towards a contradiction, assume that x is not the product of any irreducibles.
In particular, x is not irreduicble. So $\exists x_2, y_2 \in R \setminus (\{0\} \cup R^{\times})$ such that $x = x_2 y_2$.
Then $(x) \subseteq (x_2)$ and $(x) \subseteq (y_2)$. If both x_2 and y_2 were products of irreducibles, then so would be x.
We may assume, without loss of generality, that x_2 is not a product of irreducibles.
Repeat the same argument, and we have $x_2 = x_3 y_3$ with x_3 not being any product of irreducibles, and $(x_2) \underset{\neq}{\subset} (x_3)$.
Repeat again and again, and we get an ascending chain of ideals

$$(x) \underset{\neq}{\subset} (x_2) \underset{\neq}{\subset} (x_3) \underset{\neq}{\subset} \cdots \underset{\neq}{\subset} (x_n) \underset{\neq}{\subset} \cdots$$

which contradicts Lemma 2. ■

Definition: Euclidean Norm

Let R be an integral domain.
A Euclidean norm on R is a function $N : R \to N_0$ with properties

1. $N(0_R) = 0$.

2. For any $a, b \in R$, $b \neq 0$, $\exists q, r \in R$, $a = qb + r$ such that either $r = 0$ or $N(r) < N(b)$.

Definition: Euclidean Domain

A Euclidean domain is an integral domain that admits a Euclidean norm.

Example A

$R = \mathbb{Z}$ and $N(m) = |m|$.
Condition (1) is clearly satisfied, and, for (2), use the division algorithm.

$$a = qb + r, \quad 0 \leq r \leq |b|$$

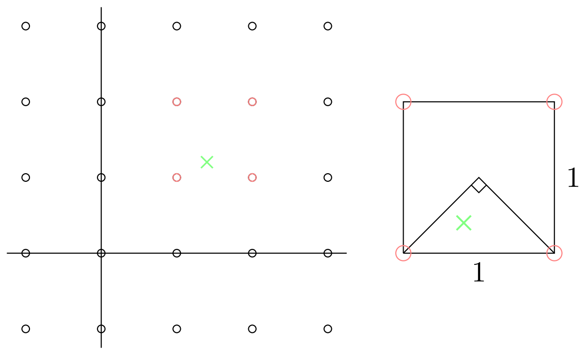
In practice, a slightly more efficient way for $b > 0$ is

$$a = q'b + r', \quad -\frac{|b|}{2} \leq |r| < \frac{|b|}{2}$$

Where $q' = q$ if $r \in \left[0, \frac{|b|}{2}\right)$ and $q' = q + 1$ if $r \in \left[\frac{|b|}{2}, |b|\right)$ with $r' = r - |b|$.

Example B

$R = \mathbb{Z}[i]$ and $N(a + bi) = a^2 + b^2$.
To verify (2), let $\alpha, \beta \in \mathbb{Z}[i]$ and $\beta \neq 0$.
Then consider $\frac{\alpha}{\beta} \in \mathbb{C}$



Choose $q \in R$ be the closest corner of the square to $\frac{\alpha}{\beta}$.
Note

$$\left|\frac{\alpha}{\beta} - q\right| \leq \frac{1}{\sqrt{2}}$$
$$|\alpha - q\beta| \leq \frac{1}{\sqrt{2}}|\beta|$$

Then $\alpha - q\beta = r \in R$, $\alpha = q\beta + r$ and $N(r) = |r|^2 \leq \frac{1}{2}|\beta|^2 = \frac{1}{2}N(\beta)$.

Example C

Let F be a field and $R = F[x] = \{\text{polynomials in } X \text{ with coefficients in } F\} = \{a_0 + a_1X + \cdots + a_dX^d \mid d \in \mathbb{N}_0, a_i \in F\}$.
Define $N(f(x)) = \begin{cases} \deg f(x) & \text{if } f(x) \text{ is not the zero polynomial} \\ 0 & \text{if } f(x) \text{ is the zero polynomial} \end{cases}$.

Note: On Hierarchy

Euclidean $\Longrightarrow$ PID $\Longrightarrow$ UFD

Theorem: Euclidean is PID

A Euclidean domain is a Principle Ideal Domain.

Proof

Let R be a domain and $N : R \to \mathbb{N}_0$ a Euclidean norm.
Let I be an ideal of R. If $I = \{0_R\}$, $I = (0_R)$.
So assume $I \neq \{0_R\}$. Then consider the nonempty subset

$$S_I = \{N(b) \mid b \in I \setminus \{0_R\}\} \subseteq \mathbb{N}_0$$

Let $a \in I \setminus \{0_R\}$ be such that $N(a)$ is the smallest element in S_i.
Claim: $I = (a)$.

- Proof of Claim

  Clearly, $I \supseteq (a)$.
  For $\subseteq$, let $b \in I$ be arbitrary and apply axiom 2 to get $q, r \in R$ such that $b = qa + r$ with either $r = 0$ or $N(r) < N(a)$.
  If $r = 0$, $b \in (a)$. Note $r = b - qa \in I$, so unless $r = 0$ we get a contradiction.

Definition: Cartesian Product of Rings

If R and S are rings, then the cartesian product $R \times S = \{(r, s) \mid r \in R, s \in S\}$ is a ring with compontentwise binary operations.

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$$
$$(r_1, s_1) \cdot (r_2, s_2) = (r_1 \cdot r_2, s_1 \cdot s_2)$$

Example

If X and Y are topological spaces, then $C(X \coprod Y) = C(X) \times C(Y)$.

Chinese Remainder Theorem

Recall: two ideals I and J are said to be coprime if $I + J = (1) = R$.
If I and J are coprime ideals in R, then the natural map

$$\begin{aligned} R/I \cap J &\xrightarrow{\overline{f}} R/I \times R/J \\ (r + I \cap J) &\longmapsto (r + I, r + J) \end{aligned}$$

is an isomorphism of rings.

Proof

Start with

$$\begin{aligned} R &\xrightarrow{f} R/I \times R/J \\ (r + I \cap J) &\longmapsto (r + I, r + J) \end{aligned}$$

which is a ring homomorphism where

$$\ker(f) = \{r \in R \mid r \in I \text{ and } r \in J\} = I \cap J$$

. Therefore, it is enough to show that f is surjective. Since I and J are coprime, $I + J = (1)$, so there exist $x \in I$ and $y \in J$ such that $x + y = 1_R$. Now let $(a + I, b + J) \in (R/I) \times (R/J)$ be arbitrary. We want to find $r \in R$ such that $r \equiv a \pmod I$ and $r \equiv b \pmod J$.

$$a \pmod I \equiv bx + a(1 - x) = bx + ay = b(1 - y) + ay \equiv b \pmod J$$

Useful in Number Theory

Theorem (Lagrange):

Every natural number is the sum of four squares of integers.

Example

$15 = 3^2 + 2^2 + 1^2 + 1^2$.

Idea of Proof

1. For every prime p, solve $p = a_1^2 + a_2^2 + a_3^2 + a_4^2$.

2. If $A = a_1^2+a_2^2+a_3^2+a_4^2 = N(a_1+a_2\hat{\imath}+a_3\hat{\jmath}+a_4\hat{\jmath}) = N(q_1)$ and $B = b_1^2+b_2^2+b_3^2+b_4^2 = N(b_1+b_2\hat{\imath}+b_3\hat{\jmath}+b_4\hat{\jmath}) = N(q_2)$, then $ab = N(q_1 q_2)$.
   For $3 = N(1+\hat{\imath}+\hat{\jmath})$ and $5 = N(2+\hat{\imath})$, $(1+\hat{\imath}+\hat{\jmath})(2+\hat{\imath}) = 1 + 3\hat{\imath} + 2\hat{\jmath} - \hat{k}$ and $15 = 1^2 + 3^2 + 2^2 + 1^2$.

Hurwitz's Quaternions

$\left\{t + x\hat{\imath} + y\hat{\jmath} + z\hat{k} \mid \text{either } t,x,y,z \in \mathbb{Z} \text{ or } t,x,y,z \in \mathbb{Z} + \frac{1}{2}\right\}$

Theorem: Classification of Finitely Generated Abelian Groups

Any finititely generated abelian group G is isomorphic to

$$G \cong \underbrace{\mathbb{Z} \times \cdot \times \mathbb{Z}}_{r \text{ copies}} \times \mathbb{Z}/(a_1) \times \cdot \times \mathbb{Z}/(a_k)$$

where $0 < a_1 | a_2 | \cdots | a_k$ and (a_i) are invariant facotrs uniquely determined by G. e.g.

$$(\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}) \times \mathbb{Z}/(2) \times \mathbb{Z}/(12) \times \mathbb{Z}/(84) \times \mathbb{Z}/(420)$$

This will be proven in MATH 201 using module theory over principle ideal domains.