

# Brilliant: Group Theory

Dave Fetterman

2/23/22

Note: Latex reference: <http://tug.ctan.org/info/undergradmath/undergradmath.pdf>

## 1 Chapter 1.2

### 1.1 Page 1

$R(R_1(x)) = A \rightarrow B, B \rightarrow A, C \rightarrow C$ . So reflection about CE.

### 1.2 Page 2

$R_2(R_1(x)) = A \rightarrow B, B \rightarrow C, C \rightarrow A$ . So rotation clockwise  $120^\circ$

### 1.3 Page 5

$R \star R = H \star H = V \star V = I$  on the letter "I".

### 1.4 Page 6 - 9

Cayley table for rotating letter "I":

	I	H	V	R
I	I	H	V	R
H	H	I	R	V
V	V	R	I	H
R	R	V	H	I

Note: check out <https://www.tablesgenerator.com/> here.

### 1.5 Page 10

- Klein four group:  $(+, [0, 1] \times [0, 1])$  is equivalent to the "I" rotation.
- First coord could be: Does it rotate?

- Second coord could be: Does it flip?

## 2 Chapter 1.3

Group Properties

- Some binary operation ( $\cdot$ )
- Identity (not e.g., even integers)
- Inverse (not e.g. multiplication modulo non-prime  $p$ )
- Associativity (not e.g. an average  $f(x, y) = (x + y)/2$ )?

## 3 Chapter 1.4

Cube symmetries

One way to think about it:

- Corner  $A$  maps to one of eight new corners
- Each mapping has three orientations of that corner spin (0 degrees, 120, 240)
- Therefore 24

Another way:

- One identity = 1
- Type I: Rotate around line joining two opposite face centers: 3 pairs \* 3 non-identity spins = 9
- Type II: Spin around line joining two opposite corners. 4 pairs \* 2 non-identity spins = 8
- Type III: Spin 180 degrees around line from front upper edge to back lower edge. Combo of a spin and a rotate. 6 pairs = 6.
- Sum to 24.

Another way:

- There are four diagonals to a cube.
- Their permutations are in 1:1 correspondence with the transformations possible. (24)
- Type I keeps none fixed. 90 degrees: Chain =  $4!/4 = 6$ . 180 degrees: two pairs. Select who  $A$  matches = 3.

- Type II rotates three, keeps one fixed = 8
- Type III does one swap, keeps two fixed =  $\binom{4}{2} = 6$

Note also: There are 24 reflection symmetries as well. (1:1 correspondence with rotations via "swap top center labels?")

## 4 Chapter 2.1

### 4.1 Page 2-3

The integers under multiplication are not a group, as they have no inverse. The set of rationals with multiplication as the group operation is not a group as 0 has no inverse

### 4.2 Page 5 - 7

- Dihedral group  $D_n$  has  $2n$  elements, is not commutative, not cyclical.
- If  $n$  is even, there is exactly one rotational symmetry  $R \neq I$  which commutes with all the other elements of  $D_n$  (the 180 degree rotation)

### 4.3 Page 8 - 9

- Symmetric group  $S_n$  is the set of permutations on  $n$  elements.
- "in-shuffle" of a deck of four cards is "split in half, interleave top half with bottom half, top card second", or  $\phi = (1, 2, 4, 3)$ .  $\phi^4 = I$

### 4.4 Page 10-11

- Cyclic group  $Z_n$  is the set of integers modulo  $n$  under addition.
- Note that though usually multiplication is the default group operation, this usually uses "+".

## 5 Chapter 2.2: More Group Examples

### 5.1 Page 1-2

- **Order of an element**  $g$  is smallest  $k$  such that  $g^k = e$ . Otherwise **infinite order**

### 5.2 Page 3

Quaternion group  $Q_8$  rules:

- $i^2 = j^2 = k^2 = ijk = -1$
- Implies  $ij = k, jk = i, ki = j$
- implies  $ji = -k, kj = -i, ik = -j$
- So this is not only *non-commutative* but *anti-commutative*
- $Q = \pm 1, \pm i, \pm j, \pm k$
- So one element of order 1, one of order 2 (element -1), remaining six of these elements have order 4

### 5.3 Page 4

Note that musical notes ( $Z_{12}$ ) has only generators 1, 5, 7, 11. These corresponding to chromatic, circle of fourths (anti-fifths), circle of fifths, downwards chromatic scales!

### 5.4 Page 55

- $GL_n(\mathbb{R})$  is invertible  $n \times n$  matrices in  $\mathbb{R}$ .
- $SL_n(\mathbb{R})$  is determinant 1  $n \times n$  matrices in  $\mathbb{R}$ .
- $A = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$  has order 2,  $B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$  has order 2, but  $AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$  has infinite order! Non-commutativity strikes.

### 5.5 Page 6-11

- **isomorphism** is a bijection preserving group operations.
- Can think of it as a relabeling of the Cayley table.
- Example given is Klein-four and symmetries of tall serif letter "I", or of a diamond/non-square rhombus.
- $Z_{12}$  is isomorphic to rotational symmetries of a 12-gon.
- $Q_8$  is isomorphic under matrix multiplication to  $\left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\} \subset GL_2(\mathbb{R})$
- $D_3$  is isomorphic to  $S_3$  since any permutation is possible in  $D_3$  and no more.

## 6 Chapter 2.3: Subgroups

### 6.1 Page 1 - 3

- Subgroups are closure-bound subsets of groups.
- Easy test:  $H \subset G$  if for every  $h_1, h_2 \in H, h_1 h_2 \in H$ , and for any  $h \in H, h^{-1} \in H$ .

### 6.2 Page 4

- Cartesian product of groups  $G, H$  is also a group:  $G \times H = (g, h) \cdot (g', h') = (gg', hh'), g \in G, h \in H$ . Is this also called the **direct product**?

### 6.3 Lagrange's theorem

Theorem: Order of every subgroup divides the containing group.

Lemma:  $H \subset G, r, s \in G. Hr = Hs \iff rs^{-1} \in H$ . Otherwise,  $Hr, Hs$  have no element in common.

One direction:  $rs^{-1} \in H \rightarrow Hr = Hs$

- $rs^{-1} = h \in H$  by supposition
- $Hh = Hrs^{-1} = H$
- $Hr = Hs$

Other direction:  $Hr = Hs \rightarrow rs^{-1} \in H$

- $Hr = Hs$  by supposition
- $Hrs^{-1} = H, \text{ so } h_1 rs^{-1} = h_2 \text{ for some } h_1, h_2.$
- $rs^{-1} = h_1^{-1} h_2 \in H$

Therefore, if  $Hr$  and  $Hs$  have some element in common, meaning  $h_1 r = h_2 s$ , then  $rs^{-1} = h_1^{-1} h_2 \in H$ . So, by the first direction above,  $Hr = Hs$ .

*Lagrange construction:*

- Take  $r_1 \in G$ , so  $Hr_1 = H$ .
- If  $H \neq G$ , take  $r_2 \in G - Hr_1$  to create  $Hr_2$ .
- Repeat. We will thus create disjoint  $Hr_1, Hr_2, \dots$  of the same size.

## 6.4 My take on Lagrange

- If  $t \in Hr$  since  $t = h_1 r$  and  $t \in Hs$  since  $t = h_2 s$ , then  $r = h_1^{-1} h_2 s \in Hs$  and likewise for  $s$ , so  $Hr = Hs$ . So every element is in both or neither.
- Therefore  $H(x) = Hx$  is a partition relation on the elements of  $G$ .
- Size of  $Hr$  equals size of  $H$  for obvious group reasons.
- Every element  $g$  of  $G$  is in some coset  $Hg$ .
- Therefore  $G$  is partitioned into cosets of equal size, which is size of  $H$ .
- Therefore size of subgroup  $H$  divides size of group  $G$

## 6.5 Page 7-12

- Note that if  $H$  and  $K$  are subgroups, so is  $H \cap K$ .
- $Z_6$  has subgroups  $Z_6, 0, 2, 4, 3, 0$ , all divisors of 6 in this case.
- $Z_p$ ,  $p$  prime, has only subgroups  $Z_p, 0$
- $Z_p \times Z_p$  has  $p + 3$  subgroups
  - $Z_p \times Z_p$
  - Generator  $(0,0)$
  - Generator  $(0,1)$
  - All generators  $(1, n), n \in [0, p - 1]$  .  $p$  of those.
- Another way to think about  $Z_p \times Z_p$ : Outside of  $(0,0)$ , the remaining  $p^2 - 1$  elements each have order  $p$ . They are generate a group of size  $p$ , minus the identity. So  $(p^2 - 1)/(p - 1) + 2 = p + 3$ .
- Subgroup count of  $Z_4 \times Z_2$ : a counting exercise, based on generators.
  - Look at all cyclic groups of each of the elements.
  - $(0,0)$  generates 1 group
  - Order 2: Three elements, which generate three distinct cyclic subgroups
  - Order 4: Four elements, which generate two distinct subgroups
  - Order 8:  $Z_4 \times Z_2$ , non-cyclic
  - And there's one distinct  $Z_2 \times Z_2$  group.
  - *Note: Is there a good (even recursive) formula for this?*

## 7 Chapter 2.4: Abelian Groups

### 7.1 Page 1-3

- Theorem:  $Z_a \times Z_b$  is isomorphic to  $Z_{ab}$  iff  $a$  and  $b$  are relatively prime.
- DF Proof: If  $a$  and  $b$  are relatively prime,  $(1,1)$  is of order  $ab$ . If  $a$  and  $b$  share factor  $c$ , then  $Z_{ab}$  has an element of order  $ab$ , but  $Z_a \times Z_b$  will have cycled by  $a * b/c$ .
- So decompose e.g.  $Z_{12}$  into  $Z_4 \times Z_3$ , for example.

### 7.2 Page 4-6

- Theorem: Every finite abelian group is isomorphic to a direct product of cyclic groups.
- Therefore, the number of these groups of order  $n$  is the product of the partitions of each of its prime factors' powers.
- Therefore, the number of abelian groups of size  $24 = 3 * 2^3 = p(3) * p(1) = 3 * 1 = 3$ ,  $Z_3 \times Z_8, Z_3 \times Z_4 \times Z_2, Z_3 \times Z_2 \times Z_2 \times Z_2$
- Therefore, the number of abelian groups of size  $2310 = 2 * 3 * 5 * 7 * 11$  is one.

### 7.3 Page 7-11: $Z_n^*$ or $U(n)$

- Group  $Z_n^*$ : elements of  $Z_n$  relatively prime to  $n$ , under multiplication.
- $|Z_n^*| = \phi(n)$ , the totient function.
- This is a group even if  $n$  not prime because there is  $ax + bn = 1$  if  $x, n$  are relatively prime.
- $Z_8^* = \{1, 3, 5, 7\}$  is isomorphic to  $Z_2 \times Z_2$  since every element squared is 1.
- $Z_{10}^* = \{1, 3, 7, 9\}$  is isomorphic to  $Z_4$  since it is generated by 3.
- $Z_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$  is isomorphic to  $Z_4 \times Z_2$  by counting element orders.
- Note: Primitive roots of  $n$  are those that generate  $Z_n^*$ . There are primitive roots mod  $n$  if and only if  $n = 1, 2, 4, p^k, 2p^k$ .
- TODO: read <https://brilliant.org/wiki/primitive-roots/> and why these are the only solutions. Also, look up *Legendre symbol*

## 8 Chapter 2.5: Homomorphisms

### 8.1 Page 1 - 6

- Homomorphism  $\phi : \phi(a) *' \phi(b) = \phi(a * b)$ . Note that  $*$  and  $*'$  are different operations.
- This means, "translate each via the function, then combine" yields the same result as "combine first, then translate". So structure is preserved.
- Note this is like isomorphism, except homomorphism can squash some items to zero.
- Also, this can change to an entirely separate domain, e.g.  $\det(AB) = \det(A)\det(B)$
- Easy to prove homomorphism preserves identities and inverses.
- Order of transformed element  $\phi(g)$  divides order of  $g$ , since  $g^k = e$  and  $\phi(g)^k = \phi(e)$ , but consider that  $\phi(g)$  could hit  $e$  at some divisor of  $k$  - we could map everything to the identity and make that 1!

### 8.2 Page 7- 10: Counting homomorphisms

- Main idea: Knowing where we send identity determines entire homomorphism for a cyclic group.
- Homomorphism count for  $Z_4 \rightarrow Z_{10}$ : There are 10 places to send identity, but recall that  $\phi(1)$  has to have order 4 since  $\phi(1 + 1 + 1 + 1) = \phi(0) = 0$ . Therefore,  $\phi(1)$  has to be 0 or 5. So 2 possibilities.
- Homomorphism count for  $Z_{99} \rightarrow Z_{100}$ : Since  $\phi(99) = 0$  and  $\phi(1) \times 100 = 0$ , and order of  $\phi(1)$  must divide both, only one possibility:  $\phi(1) = 1$ .
- Homomorphism count for  $Z_{99} \rightarrow Z_{99}$ : 99, since  $99 \cdot \phi(1) = 0$ , so  $\phi(1)$  can go anywhere.
- Homomorphism count for  $D_3 \rightarrow Z_3$ : 1, since  $D_3$  has 3 elements of order 2, 2 of order 3, 1 of order 1. Only mapping everything to 0 works.

### 8.3 Page 11: Counting automorphisms

- Automorphism is isomorphism from group to itself.
- Count of automorphisms of  $Z_8$ : If 1 maps to an order-8 element, we're isomorphic. There are four: 1, 3, 5, 7
- $\text{Aut}(Z_8)$  is isomorphic to  $Z_2 \times Z_2$ , since  $\phi_3(1)^2 = \phi_5(1)^2 = \phi_7(1)^2 = 1$ , where  $\phi_a$  maps  $a$  to 1. Three elements of order 2 means it's the Klein 4 group.



- Count of *automorphisms* (meaning, we need all the elements in the codomain) of  $Z_2 \times Z_2 \times Z_2$ : Think of  $\phi((1, 0, 0)), \phi((0, 1, 0)), \phi((0, 0, 1))$  as the basis for the group. There are seven choices for the first, six for the next, and *four* for the third.
- The above group is  $(\phi(e_1)|\phi(e_2)|\phi(e_3)) = GL(\mathbb{F}_2)$ , invertible matrices of 3x3.

## 9 Chapter 2.6: Quotient Groups

### 9.1 Aside: Complex multiplication

- Complex modulus (size) of  $a + bi$  is defined as  $root(a^2 + b^2)$
- Complex multiplication: Angles add, moduli multiply
- One proof of moduli:  $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$  and  $\sqrt{a^2 + b^2}\sqrt{c^2 + d^2} = \sqrt{a^2c^2 + b^2d^2 - 2abcd + ad^2 + bc^2 + 2adb c}$
- One proof of angles: Convert to  $r_1(\cos(a) + \sin(a))r_2(\cos(b) + \sin(b))$  and multiply
- More visual proof: Think of  $c_1(a + bi) = c_1a + i(c_1b)$ .  $a$  scales original vector, and  $bi$  rotates by 90 degrees and scales.

### 9.2 Page 1-6

- $S^1$ , is defined as the group of complex numbers with modulus 1.
- The coset  $zS^1$  is any complex number multiplied by  $S^1$ , which is a circle about the origin.  $z = 2$  and  $z = 2i$  would be in the same coset. These cosets are members of  $C^*$  with the same modulus (length).
- These are disjoint cosets that fill out  $\mathbb{C}^*$  (don't include the zero, since no inverse).
- If you consider  $H = x + iy$ ,  $x > 0, y = 0$  (positive reals) then the cosets are rays from the origin. Any  $zH$  is just the different sizes of that (say, unit) vector. These cosets are members of  $C^*$  with the same angle.
- **quotient group** of  $\mathbb{C}^*$  by  $S^1$ :
  - Members are cosets
  - Multiplying is defined as  $aH \times bH = abH, H \in S^1, a, b \in \mathbb{C}^*$
  - $S^1$  is therefore the identity.
  - This group is isomorphic to  $R^+$  under multiplication (or really, like  $\mathbb{H}$ ).
  - "A ray of angle A and a ray of angle B multiply to a ray of angle AB, forget about the size".

- This is like collapsing out the divisor, in this case,  $S^1$ .
- size  $|G/H| = |G|/|H|$  since cosets are equally sized.
- **Gotcha:** Only works (meaning,  $g_1, g'_1 \in C_1, g_2, g'_2 \in C_2$  implies  $g_1g_2$  in same coset as  $g'_1g'_2$ ) if  $H$  is **normal** in  $G$ .
- Note: Normal means  $xH = Hx$ , so that makes sense that  $g_1Cg_2C = g_1g_2C * C = g_1g_2C$
- So  $\mathbb{C}^*/H$  is all the rays with the same modulus, or  $S^1$ .
- "A ray of size  $X$  and a ray of size  $Y$  multiply to a ray of size  $XY$ , and forget about the angles".
- So  $\mathbb{C}^*/S^1 = H$  and  $\mathbb{C}^*/H = S^1$ !

### 9.3 Page 7-12

- Another example:  $\mathbb{Z}/10\mathbb{Z} = \mathbb{Z}_{10}$  under addition. Forget about the non-unit digits!
- Another example:  $\mathbb{Q}/\mathbb{Z}$  is  $\bar{q} = q + \mathbb{Z}$ , so  $\overline{1/2} + \overline{2/3} = \overline{1/6}$
- Another example: if  $N$  is the **center** (omni-commuter subgroup) of  $D_4$ , then  $N$  is two elements  $I, R_{180}$ . Forgetting about those we have cosets  $(I, R_{180})N, (R_{90}, R_{270})N, (D_1, D_2)N, (V, H)N$ . All non-identity are degree 2, so isomorphic to  $Z_2 \times Z_2$
- Another example:  $Z_{13}^*$  with multiplication mod 13.  $N = 1, 12$  is a normal subgroup.  $Z_{13}^*/N$  is "forget about the +/- 1 of it and think of these as 1 through 6.
- Another example: **commutator subgroup**  $[a, b]$  is generated by all  $aba^{-1}b^{-1}$  for all  $a, b \in G$ . Note: group members are products of these guys, not necessarily all of that form. This is just  $e$  for an Abelian group. Its size measures "how far" the group is from being Abelian.
- **Main idea** of quotients: "what do we force to the identity?" If we say every  $\overline{aba^{-1}b^{-1}} = \bar{1}$ , then you can multiply by  $ba$  to get  $\overline{ab} = \overline{ba}$ . So  $G/[G, G]$  is necessarily Abelian.

## 10 Chapter 3.1: Number Theory

### 10.1 Page 1- 7

- A Fermat's little theorem proof
  - Take prime  $p$ , and  $a$  not divisible by  $p$ .

- $a, 2a, 3a, \dots, (p-1)a \equiv 1, 2, 3, \dots, (p-1) \pmod p$  since they're the same elements mod  $p$ .
- Take the product of each:  $a^{p-1}(p-1)! \equiv (p-1)! \pmod p$
- Divide  $(p-1)!$  out (there's an inverse mod  $p$ ) and you get  $a^{p-1} \equiv 1 \pmod p$
- Another: Since the order of  $a$  in  $\mathbb{Z}_p^*$  is  $p-1$ ,  $a^{p-1} \equiv 1 \pmod p$ .
- Note: Generalization of Fermat's little theorem using same group argument:  $a^{\phi(n)} \equiv 1$  if  $a$  and  $n$  relatively prime.

## 10.2 Page 8-11

- Wilson's theorem:  $1 * 2 * \dots * (p-1) \equiv -1 \pmod p$ .
- One proof: These all have inverses, except 1 and  $-1 \pmod p$ , which are self-inverting ( $x^2 = 1$  solutions).
- This also proves that the product of all elements of a finite Abelian group *which has a single element  $g$  of order 2* is that element,  $g$ .
- A hard proof TODO. The powers of a **primitive root of  $p$**  yield all elements  $a \pmod p$ . So  $\mathbb{Z}_p^*$  is cyclical for any prime  $p$ .
- One more proof: if  $k$  relatively prime to  $p-1$ , where  $p$  a prime  $> 2$ , then  $1^k + 2^k + \dots + (p-1)^k \equiv 0 \pmod p$ , since each of these summands is a different member of the group, summing to  $\frac{p(p-1)}{2}$

## 11 Chapter 3.2: Games

### 11.1 15 puzzle

I think this will go: - The board is a permutation of  $(1, 2, \dots, 15)$ , read like a book, with a blank somewhere in there, immaterial. - Sliding the blank left or right doesn't change the order. - Sliding it up or down skips three backward or forward.

**Their proof:** Think of this as a series of swaps with  $(j, 16)$ , 16 being the blank tile. To return to the bottom right corner, 16 must make an even number of moves. So only even permutations allowed. So  $(14, 15)$  is not a viable swap, nor any of the odd permutations.

## 12 Chapter 3.3: Peg solitaire

- Consider Klein four group:  $xy = yx = z, yz = zy = x, xz = zx = y$ .

- Label all pegs such that three consecutive are always, in some order: x, y, z
- Invariant: product of all occupied spaces. If x jumps over y to get to z, eliminating jumped peg,  $xy = z$ .
- 11 x's, 11 z's, 10 y's yield  $xz = y$  as the product.

## 13 Chapter 3.4: Rubix's Cube

- Each element is the state  $(S_{12}, S_8, (Z_2)^{12}, (Z_3)^8)$ , representing around a fixed set of centers: (middle selections, corner selections, middle orientation, corner orientation).
- Invariant: First and second perms for all F,B,D,U,L,R are odd, so first two args need same permutation parity
- Invariant: (Not proven here): Sum of edge orientations (0,1) is zero, sum of corner orientations (0, 1, 2) is zero.
- **Commutator:**  $ghg^{-1}h^{-1}$  measure how entangled  $g$  and  $h$  are. If they're commutative, it is  $e$ .
- For Rubix's cube, commutators  $ghg^{-1}h^{-1}$  are great for only moving pieces where effects of  $g$  and  $h$  overlap.
- $g$  and  $h$  are **conjugates** if some  $x$  such that  $h = x^{-1}gx$ . "h is same as g, just in a different location".
- Conjugate interpretation: "h is move via x, operate with g, move back via x."
- For Rubix's cube - you can use conjugates to make whatever change to a different part of the cube (move it to the operating table, operate, move it back).

## 14 Chapter 4.1: Normal Subgroups

### 14.1 Normal definition

- **Normal subgroup intuition:** Every conjugacy  $g^{-1}Hg$  moves a group to another subgroup. Normal subgroups  $g^{-1}Ng = N$  are the ones *that don't move* when you conjugate them.
- Example of non-normal: Any one of the  $n$  sets of  $S_{n-1}$  among conjugates of  $S_n$ . Move it, mess with it, move it back - it's broken free by then.
- Normal definition: Group  $N$  is normal if and only if (all equivalent):
  - $gN = Ng$  for all  $g \in G$

- $gNg^{-1} = N$  for all  $g \in G$  (equiv to above)
- $gng^{-1} \in N$  for all  $g \in G$
- *Theorem: Any subgroup of index 2 is normal.* Proof:  $G$  has two distinct cosets  $N$ ,  $gN$ , but also  $N$  and  $Ng$  so  $gN = Ng$ .
- Normal doesn't recursively nest.
  - If  $G$  has normal subgroup  $H$  and  $H$  has normal subgroup  $K$ ,  $K$  is normal in  $H$  too (those elements also "pass through  $K$ ")
  - However,  $H$  can be normal in  $G$  (e.g.  $(I, R_{180}, F_v, F_h)$  in  $D_4$ ,  $K$  can be normal in  $H$  (e.g.  $I, V$ , but  $K$  is not normal in  $G : VR_{90} = D_{ul}, R_{90}V = D_{ur}$ )
- Normal examples in  $GL_2(\mathbb{C})$ :  $SL_2(\mathbb{C})$  (determinant 1) and non-zero diags  $zI_2$ .
- Non-normal examples in  $GL_2(\mathbb{C})$ :  $GL_2(\mathbb{R})$  and non-zero diags with different entries. Easy to throw some arbitrary ones in Wolfram Alpha and see everything messed up after conjugation.
- $G$ 's **Center**:  $Z(G)$  are the omni-commuters. Always normal.
- $G$ 's **Commutator group**  $[G, G]$ : Product of any  $aba^{-1}b^{-1}$  for  $a, b \in G$ . is normal, since  $g[a, b]g^{-1} = [gag^{-1}, gbg^{-1}]$ .

## 14.2 Normal properties and examples

- $S_3$  has three normal subgroups: two trivial ones, and  $([], [123], [321])$  since it's of index 2.
- $Q_8$  has four non-trivial subgroups, all normal: those generated by  $I, j$ , or  $k$ , all of order 4, index 2.  $-1$  also generates an order 2 group, but it's the center.
- Definition: Product  $HK = hk : h \in H, k \in K$ .
- Property: If  $H \cap K = \{1\}$ , and  $H, K$  are finite,  $|HK| = |H| \cdot |K|$ . Why?  $h_1k_1 = h_2k_2 \implies h_2^{-1}h_1 = k_1^{-1}k_2$ , proving they're both  $e$  since left is in  $H$ , right in  $K$ .
- Property : If  $H, K$  subgroups of  $G$ , then  $HK$  is a subgroup too if  $H$  or  $K$  is normal, otherwise not always. Why?
  - Assume  $H$  is normal.
  - Identity:  $e_h e_k = e$  is in there.
  - Inverse: If  $hk \in HK$ , then  $k^{-1}h^{-1} = k^{-1}h^{-1}k^1 * k^{-1}$  is in  $H, K$  due to  $H$ 's normality.

- Closure:  $h_1k_1 * h_2k_2 = h_1k_1h_2(k_1^{-1}k_1)k_2 = h_1(k_1h_2k_1^{-1})k_1k_2 = h_1h_3 * k_1k_2$  for some  $h_3$
- Property: If  $H, K$  are normal subgroups of  $G$ ,  $HK$  is normal. Maybe not otherwise (e.g. take  $H = \{1\}, G$  a non-normal subgroup). Why? More tricks.  $ghkg^{-1} = gh(g^{-1}g)kg^{-1} = (ghg^{-1})(gkg^{-1}) = h'k'$  for some other  $h' \in H, k' \in K$ .
- **Centralizer** of  $G$ 's subgroup  $H$  is a subgroup of  $G$  which commutes with all  $H$ :  $C_G(H) = \{g \in G : gh = hg \text{ for all } h \in H\}$ . This is  $G$  if and only if  $G$  is Abelian (almost definitional). May not contain  $H$ .
- **Normalizer** of  $G$ 's subgroup  $H$  is a subgroup of  $G$  which makes  $H$  normal:  $N_G(H) = \{g \in G : gH = Hg\}$ . This is  $G$  if and only if  $H$  is normal in  $G$  (almost definitional). Largest subgroup of  $G$  where  $H$  is normal.
- Centralizer is a normal subgroup of normalizer with two different proofs:
  - With  $n \in N_G(H), c \in C_G(s)$ , show that  $ncn^{-1}$  commutes with members of  $H$ , so it's in  $C_G$ , therefore normal.  $hn$  is some  $nh'$ , and same for  $n^{-1}$ , so  $ncn^{-1}h = nch'n^{-1} = nh'cn^{-1} = h'ncn^{-1}$  so  $ncn^{-1}$  passed through  $h$ , is therefore in the centralizer, and so  $C_G(H)$  is normal.
  - Using First isomorphism theorem (later):
    - \*  $N_G(H)$  is the big "dividend" group,  $C_G(H)$  is the "divisor", and  $Aut(H)$  the "quotient" (codomain of the homomorphism)
    - \* The homomorphism  $\phi : N_G(H) \rightarrow Aut(H)$  is  $g \rightarrow \phi_g(x) = gxg^{-1}$ .
    - \* The kernel of this homomorphism is that which maps to  $I \in Aut(H)$ .
    - \* The kernel is the centralizer, since  $\phi_c(x) = cxc^{-1} = cc^{-1}x = x$ , identity.
    - \* Therefore,  $N_G(H)/Ker(\phi) = N_G(H)/C_G(H) \rightarrow Aut(H)$ . so  $C_G(H)$  must be normal!
    - \* (Kernels of homomorphisms always normal (DSF Proof): If  $\phi : G \rightarrow H$  is a homomorphism, and  $g \in G, k \in Ker(\phi)$ , then  $gkg^{-1} \in K$  since  $\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1}) = \phi(g)\phi(g^{-1}) = e$ . So  $K$  is normal in  $G$ .

## 15 Chapter 4.2: Isomorphism theorems

- Example of intuitive isomorphism:  $M_2(\mathbb{Z})/N \cong (\mathbb{Z}_2)^4$ , where  $N$  is the subgroup with even entries. How? Can either list all cosets or construct a homomorphism  $\phi \begin{pmatrix} a & b \\ c & d \end{pmatrix} = (a(\text{mod}2), b(\text{mod}2), c(\text{mod}2), d(\text{mod}2))$ .

### 15.1 First Isomorphism Theorem and example

- $G = GL_2(\mathbb{R})$ , invertible 2x2 real matrices
- $N = SL_2(\mathbb{R})$  is subgroup of  $G$  with determinant 1.
- $\varphi$  is  $\det$ , since  $\det(AB) = \det(A)\det(B)$ .
- $G/N \cong \mathbb{R}^*$  intuitively, since for any matrix, you can divide by the determinant scalar, and find the representative in the group  $N$ . Can think of  $N$  as the kernel of the homomorphism - it doesn't matter, it's mapped to identity.
- **First isomorphism theorem:** given surjective homomorphism  $\varphi : G \mapsto H$  with kernel  $\text{Ker}(\varphi) = \{g \in G | \varphi(g) = e_H\}$ , then  $G/\text{Ker}(\varphi) \cong H$ .
- Another example in the above, if  $a = \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix}$ ,  $b = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ , then  $(aN)(bN)$  is some  $cN$ , where  $\det(c) = 4$ , like  $2I$

### 15.2 Third Isomorphism theorem

- Theorem: If  $G/N$  is abelian, then every subgroup  $H$  of  $G$  containing  $N$  is normal in  $G$ .
  - $H/N \subset G/N$ , and so  $H/N$  is abelian too.
  - Abelian means  $ghN = hgN$
  - This also shows there is some  $n$  such that  $gh = hgn$ .
  - But since  $N$  is normal in  $G$ ,  $gn = n'g \rightarrow hgn = (hn')g$ , and  $hn' \in H$ , therefore  $gh = (hn')g$ , and  $H$  is normal in  $G$ .
- Actual theorem says subgroups of  $G$  containing  $N$  correspond to subgroups of  $G/N$ .
- Also,  $\frac{G/N}{H/N} \cong \frac{G}{H}$

### 15.3 Second Isomorphism theorem

- Actual theorem says: if  $H$  is a subgroup of  $G$ , and  $N$  is a normal subgroup of  $G$ , then  $\frac{H}{H \cap N} \cong \frac{HN}{N}$
- In particular, if  $H \cap N = \{1\}$ , then  $\frac{HN}{N} \cong H$ .
- Why?
- $HN$  contains both  $H$  and  $N$  since  $N$  is normal.
- Therefore  $(HN)/N$  is a group.

- $\varphi(h) = hN$  is a surjective homomorphism to  $(HN)/N$
- The kernel is anything in  $N$ , which would be  $H \cap N$ .
- Result follows from first isomorphism theorem.

## 15.4 Examples using the first isomorphism theorem

- : Typically, in order to identify  $G/N \cong K$ , find the surjective homomorphism  $G \rightarrow K$  where  $\text{Ker}(\varphi) = N$ .
- Example:  $G = \mathbb{Z} \times \mathbb{Z}$  with addition,  $N =$  group generated by  $(1, 0)$ .  $G/N \cong \mathbb{Z}$  intuitively, since you're forgetting the first coordinate. To make it formal :  $\varphi((x, y) = y)$ .
- Harder example:  $G = \mathbb{Z} \times \mathbb{Z}$  with addition,  $H =$  group generated by  $(2, 3)$ , or  $(2a, 3a)$ .  $G/H \cong \mathbb{Z}$ , actually, since  $\phi((x, y) = 3x - 2y)$  is surjective (think of  $\phi((a, a)) = a$  and its kernel is  $H$ ).
- Harder example:  $G = \mathbb{Z} \times \mathbb{Z}$  with addition,  $H =$  group generated by  $(2, 4)$ , or  $(2a, 4a)$ .  $G/H \cong \mathbb{Z} \times \mathbb{Z}_2$ , actually, since  $\phi((x, y) = 2x - y, x \pmod{2})$  is surjective and its kernel is  $H$ .
- TODO: Get a better intuition here. Is this group like, how far away from this null space line am I?

## 16 4.3a: Interlude; Group actions

### 16.1 Group Actions

Reference: <https://brilliant.org/wiki/group-actions>

- **group action** on group  $G$ , set  $X$ , is function  $f : G \times X \rightarrow X$ . It's often written  $f(g, x) = g \cdot x$ . which has some groupy properties.
  - $f(e_G, x) = x$  for all  $x \in X$ , or  $e_G \cdot x = x$
  - $f(g, f(h, x)) = f(gh, x)$  for all  $x \in X$ , or  $g \cdot (h \cdot x) = (gh) \cdot x$ .
  - Canonical Example: if  $G$  is  $S_n$ , and  $X = \{1, 2, \dots, n\}$ .
- **fixed point of a group element**  $g \in G$  is  $x \in X$  such that  $g \cdot x = x$ . So,  $f = g(x)$  is the (very straightforward) mapping,  $g$  is the function, and  $x$  would be a point that doesn't change.



- For point  $x$ , **stabilizer of the point** is called  $G_x$ , and is the set of  $g \in G$  that map  $x$  as a fixed point:  $g(x) = x$ . of a of element  $g \in G$  is  $x \in X$  such that  $g \cdot x = x$ . So, it's the *subgroup* that makes  $x$  totally stable.
- **fixed point** of element  $g \in G$  is  $x \in X$  such that  $g \cdot x = x$ . So,  $f = g(x)$  is the (very straightforward) mapping,  $g$  is the function, and  $x$  would be a point that doesn't change.
- **orbit of element**  $x \in X$  is how far  $x$  reaches, the set of  $y \in X$  such that there's a  $g \cdot x = y$ .
- Example: So if  $G = \mathbb{Z}_2 = e, g, X = \mathbb{Z}$ , and the action is  $e \cdot x = x, g \cdot x = -x$ , then
  - Fixed points of  $e$  are all of them, of  $g$  is 0.
  - Stabilizers of  $x$  are  $e$  for all,  $e, g$  for 0.
  - Orbit of 0 is  $\{0\}$ , orbit of every other  $n$  is  $\{n, -n\}$
  - *orbits* are an equivalency relation! So they partition  $X$ .
- Action is **transitive** if there is only one orbit in the relation (sounds like a regular group): for any  $x, y \in X$ , there is a  $g$  such that  $g \cdot x = y$ .
- Action is **faithful** if only  $e_G$  if the only omni-stabilizer element is  $e_G$ . Intersection of all  $G_x$  is  $e_G$ .
- Another way to think about faithful: Think of  $G$  as a homomorphism to  $Sym(X)$ , permutations of the group. Faithful actions are injective / have a trivial kernel.
- Examples of actions
  - Every group acts on itself by left multiplication. It is transitive and faithful (since the Cayley table is a latin square). One orbit.
  - Every group acts on itself by conjugation  $g \cdot x = gxg^{-1}$ . Orbits are the conjugacy classes. The **centralizer**  $C_G(x)$  is the stabilizer of  $x$ .
  - If  $H$  is a subgroup of  $G$ , then cosets  $G/H$  and left multiplication are a group action. They are a transitive action since there is one orbit: you can always get from  $gH$  to  $kH$  by  $(kg^{-1})H$ .
  - **Core Group**: The group  $\bigcap_{g \in G} gHg^{-1}$  of  $G$ 's subgroup  $H$  is the largest normal subgroup of  $H$ . Proof:
    - \* It's contained in  $H$  since  $hHh^{-1} \in H$ , and it's an intersection.
    - \* It's normal because  $kCore_G(H)k^{-1} = k(\bigcap_{g \in G} gHg^{-1})k^{-1} = \bigcap_{g \in G} kgHg^{-1}k^{-1} = Core_G(H)$  since every  $kg$  is just a  $g$  but permuted.

- \* It's the largest normal one since if there were another normal subgroup  $N' \in H$ , then  $gn'g^{-1} \in N'$  and  $gn'g^{-1} = h$  for some  $h \in H$ , so  $n' = g^{-1}hg$ , and therefore  $n'$  is somewhere in the core group.
- \* Therefore, the core group is the kernel of the map  $G \rightarrow \text{Sym}(G/H)$ , since those map to  $H$ . So if  $H$  doesn't contain any trivial subgroups, it's faithful, and is called **simple**
- Another group action:  $PGL_2(\mathbb{C}) =$  projective linear group of 2x2 matrices on the complex plane (plus infinity), sending  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}$ .
- **Orbit stabilizer theorem:** If  $G$  is finite, and  $x \in G$  has a stabilizer  $G_x$  and orbit  $\text{orb}(x)$ , then  $|G| = |G_x| |\text{orb}(x)|$ . Proof:
  - Since stabilizer is a subgroup, the count of distinct cosets (index) times the subgroup is the size by Lagrange.
  - Consider homomorphism  $\phi$  from  $G/G_x \rightarrow \text{orb}(x) = gG_x \rightarrow g \cdot x$
  - And the set  $aG_x$  and  $bG_x$  are equal under  $\phi$  iff  $a(x) = b(x)$ , since  $b^{-1}aG_x = G_x$ , implying  $b^{-1}a \in G_x \rightarrow b^{-1}a(x) = x \rightarrow a(x) = b(x)$ .
  - Also, this map is onto since every element  $y \in \text{orb}(x)$ , meaning some  $g \cdot x = y$  is in that  $gG_x$ .
  - Example: *symmetric group*:  $S_n : G_x \cong S_{n-1}! \rightarrow |G_x| = (n-1)! \cdot |\text{orb}(x)| = n$ . So  $|G| = n!$ .
  - Example: *cube symmetries*: Vertex is  $x$ , rotation of adjacent vertices is  $G_x$ .  $|G_x| |\text{orb}(x)| = 3 \cdot 8 = 24$ . Can also do with edges and faces. Turns out cube symmetries  $\cong S_4$

## 17 Aside: Conjugacy classes

### 17.1 Conjugacy classes defined

- Note: It's easy to take a group to another group by conjugation group action  $\phi(g, H) : ghg^{-1}$ . Though the whole group gets mapped to another group, the elements inside get mapped to **conjugacy classes**.
- Within group  $G$ , elements  $h, h'$  in conjugacy class  $H$  have some  $g \in G$  such that  $h' = ghg^{-1}$  (and therefore,  $g^{-1}h'g = h$ ). So, it's an equivalence relation, thus a partition.

- Note: if the group  $G$  is abelian,  $h' = ghg^{-1} \rightarrow gg^{-1}h = h$ , so all conjugacy classes there are of size one ( $ghg^{-1} = gg^{-1}h = h$ )
- Each one of these classes corresponds to the orbit of that element  $h$  under conjugation.
- Why useful? They can be used to show structure (and thus classify, look at isomorphisms, etc.) of groups.
- Example: In  $GL_n(\mathbb{R})$ ,  $A = PBP^{-1}$  is matrix similarity.  $B$  represents  $A$  under a change of bases.
- Example: In  $S_3$ , there are three conjugacy classes:  $\{()\}$ ,  $\{(abc), (bac)\}$ ,  $\{(ab), (bc), (ac)\}$ . Easy to think about with permutations - this is just relabeling the members going in, doing the permutation, then reversing the labels.
- Example:  $\mathbb{Z}/5\mathbb{Z} = \mathbb{Z}_5$  which is Abelian, so 5 classes (one for each element).

## 17.2 $A_5$ example and the class equation

- Examples: In  $A_5$ , types are repped by  $()$ ,  $(12)(34)$ ,  $(12)(23) = (123)$ , and  $(12)(23)(34)(45) = (12345)$ .
- **Gotcha:** Note that There are  $5!/5 = 24$  5-cycles, and that subgroup order has to divide 60, so there must be two conjugacy classes of 5-cycles. Makes sense that  $(12345)$  and  $(21345)$  can't be same class, since there's nowhere to "stash" during the relabeling.
- Theorem: Sum of conjugacy class orbits is size of group, or, for arbitrary class reps  $g_1 \dots g_k$ ,  $|G| = \sum_{i=1}^k [G : C_G(g_i)]$ . Note that  $|Z(G)|$  is all of the reps and classes of size one. Why does this work? Orbit-stabilizer says that  $C_G(g_i)$  is the stabilizer, and the conjugacy classes form a partition.
- **Class Equation:** Just writing down the size of the equivalence classes. In  $A_5$ , this would be  $60 = 1 + 15 + 20 + 12 + 12$  (second set of 5-cycles).
- Note that any *normal* subgroup in  $A_5$  has to be union of those since conjugation by  $A_5$  elements maps to the whole conjugacy class. BUT - there are no sums that divide 60. So  $A_5$  has no normal subgroups, so it is simple!