Napkin notes

rctcwyvrn

August 2020

1 Groups

1.1 Basics

A group is the pair $(G, *)$ such that

- G contains an identity element 1_G such that $1_G * g = g = g * 1_G \forall g \in G$
- $*$ is associative, $(a * b) * c = a * (b * c)$, so the parenthesis can be fully omitted.
- Each element $g \in G$ has an inverse $h \in G$ st. $g * h = 1_G$

Remark: It is not required that $*$ is commutative, ie $a * b = b * a$

Examples:

- $(Z, +)$
- (Q without $0, \cdot$)
- The complex unit circle, $(S^1, \times)$. 1 is the identity and all inverses $1/z$ must be on the unit circle since $|1/z| = 1 \ \forall z \in S^1$
- **Cyclical group** of order n $\mathbb{Z}/n\mathbb{Z}$
- **Nonzero residues mod prime p** $(\mathbb{Z}/p\mathbb{Z})^\times$
  •Note: We need p to be a prime because ?? I have no fucking clue
- The **trivial group**, the group with just the identity element

Non-abellian examples (Group operators are not commutative):

- **General linear matricies** of size n: $GL_n(\mathbb{R})$. $n \times n$ real matricies which have nonzero determinant. It turns out that each inverse will also have nonzero determinant so the group is valid. Follows from $det(AB) = detAdetB$, so if they're inverses $1 = detAdetB$ so they're both non-zero

- $SL_n(\mathbb{R})$, **Special Linear**, a subset of General Linear where the determinant is 1. Similarly valid because $det(AB) = detAdetB$ implies $det(I) = 1 = 1 * detB$ so $detB = 1$ and must be in SL_n
- S_n a set of permutations of $1..n$ imagined as functions from $1..n$ to itself. The group operator is then composition.
  - The identity permutation is the one that doesn't move any elements
  - The inverse of a permutation is the one that moves the elements in the exact opposite way as the original. So the net result of applying both the original and the inverse is no change, the identity permutation
- The **dihedral group of order 2n**, D_{2n}. The set is the set of orientations of a n-gon with $[1..n-1]$ rotations or a reflection and $[1..n-1]$ rotations. Each orientation is coded as the operations required to get there, so the group operator is like composition.
  - The identity orientation is with 0 rotations and 0 reflections
  - Note that $r^n = 1$ and $s^2 = 1$, so the inverse of $s^c r^d$ is $s^c r^b$ where $b = n - d$
- The **product group** of groups $(G, *_g)$ and $(H, *_h)$, $(G \times H, *)$ defined as
  - The set $G \times H$
  - The operator * where $(g_1, h_1) * (g_2, h_2) = (g_1 *_g g_2, h_1 *_h h_2)$

Non-examples:

- $(\mathbb{Z}, *)$ because the identity is 1 and there are no inverses
- $(\mathbb{Z}^+, +)$ because no inverses

Notation: A group $(G, *)$ will just be referred to as G and $a * b$ as just ab. Notation: $g^n = g * g * ... * g$ and g^{-1} is the inverse of g

1.2 Properties of groups

Time to deduce as much as possible about groups from just the definitions Claim:

- The identity of a group is unique
- The inverse is also unique
- The inverse of g^{-1} is g

Proof:

- Assume there are two identities 1 and 1‘. Then $1 * 1‘ = 1$ and $= 1‘$, so $1 = 1‘$

- Assume there are two inverses h and j for g. Then $h = h*1_g = h*(g*j) = (h*g)*j = 1_g*j = j$
- $(g^{-1})^{-1} * g^{-1} = 1_g = g * g^{-1}$

A more useful proposition

Proposition: Inverse of products

Let G be a group and $a, b \in G$, then $(ab)^{-1} = b^{-1}a^{-1}$

Proof Just compute it

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a1_G a^{-1} = aa^{-1} = 1_G$$

Lemma: Left multiplication is a bijection

Let G be a group, pick a $g \in G$. Then the map $G \to G$ given by $x \mapsto gx$ is a bijection

Proof

- Injectivity: Consider arbitrary x, y such that $gx = gy$. $x = 1_g * x = g^{-1}(gx) = g^{-1}(gy) = 1_G * y = y$, so $x = y$.
- Surjectivity: Consider arbitrary $y \in G$. Let $x = g^{-1}y$. $f(x) = gg^{-1}y = 1_G y = y$.

1.3 Isomorphisms

What does it mean for groups to be isomorphic?

Consider

- $\mathbb{Z} = [\ldots -2, -1, 0, 1, 2 \ldots]$
- $10\mathbb{Z} = [\ldots -20, -10, 0, 10, 20]$

These groups are "different" but not really. You can think of it as the "names" of the values are different, but the values in the groups are actually basically the same.
Specifically this means there exists a bijection map between the two groups $x \mapsto 10x$, which respects the group action, $f(x+y) = f(x) + f(y)$

So f can re-assign the names without changing the structure of the group or how elements interact with each other, so now we can say that the two groups $\mathbb{Z}$ and $10\mathbb{Z}$ are really the same thing

Definition Isomorphism

Let $(G, *)$ and $(H, \star)$ be groups. A bijection $\phi : G \mapsto H$ is an **isomorphism** if

$\phi(g_1 * g_2) = \phi(g_1) \star \phi(g_2), \forall g_1, g_2 \in G$

Write isomorphic as $G \cong H$
Example

The cyclical group mod 6 and the non-zero residues mod 7. The group operator for the first is + and the second is $\times$.

Claim: The bijection is $\phi(a \mod 6) = 3^a \mod 7$.

- Does it make sense? If $a \equiv b \mod 6$, does that imply that $3^a = 3^b \mod 7$? Yes, because Fermat's little theorem.
- Is it a bijection? Check manually and it turns out that it is
- Does it respect the group action? Yes because $\phi(a + b) = 3^{a+b} = 3^a \times 3^b$

1.4 Order of groups + Langrange's theorem

Two definitions of order for groups:

1. **Order of a group** G**,** $|G|$ is the number of elements in G
   - Example: The order of the cyclic group $\mathbb{Z}/n\mathbb{Z}$ is n
2. **Order of an element** g**,** $ord(g)$ is the smallest positive integer n such that $g^n = 1_G$, or ∞.
   - The order of -1 in $(\mathbb{Q}, \times)$ is 2
   - The order of each element of $\mathbb{Z}/6\mathbb{Z}$
     - $ord(1) = 6$
     - $ord(2) = 3$
     - $ord(3) = 2$
     - $ord(4) = 3$
     - $ord(5) = 6$

Fun facts

1. If $g^n = 1_G$ then $ord(g)$ divides n
2. Let G be a finite group, $ord(g)$ is finite $\forall g \in G$

Theorem: Langrange's theorem for orders

Let G be a finite group. Then $x^{|G|} = 1_G$, $\forall x \in G$

This theorem is basically a generic Fermat's little theorem, ie that in the residues mod prime p, $a^{p-1} = 1$

1.5 Subgroups

Definition: Subgroup

A subgroup is a group $(iH, \star)$ where H is a subset of G and $(G, \star)$ is a group

- If $H \neq G$, then H is a proper subgroup

Remark: To specify the subgroup you only need to know the set H, the operator $\star$ is inherited

Example: Subgroups

- $2\mathbb{Z}$ is a subgroup of $\mathbb{Z}$, and is also isomorphic to $\mathbb{Z}$
- A subset of the permutations from $[1..n] \mapsto [1..n]$, except the last element always stays the same at the nth position
- The subset of $G \times H$, $(g, 1_H)$ $\forall g \in G$. The group operation still works because $1_H \star 1_H = 1_H$. It's also isomorphic to G by the map $(g, 1_H) \mapsto g$
- Stupid examples
  - The trivial group $\{1_G\}$
  - The entire group G

Example: Subgroup generated by x

This boi $\langle x \rangle = \{\ldots, x^{-2}, x^{-1}, 1, x, x^2, x^3, \ldots\}$

- So if $ord(x) = 5$, the subgroup is $\langle x \rangle = 1, x, x^2, x^3, x^4$. Isomorphic to the cyclic group $\mathbb{Z}/5\mathbb{Z}$ by the map $x^n \mapsto n$
- If $ord(x) = \infty$ then the subgroup generated by x is just G

Example: Non examples of subgroups (of $(Z, +)$

- The set $\{0 \ldots\}$ because it is not a group, does not contain inverses.
- The set of all integer cubes is not a subgroup because it's not closed under addition
- The empty set is not a subgroup because it does not have an identity element

Remark: Why these axioms? Why associative and not commutative?

- In general you want to balance making an definition nice to work with, and making it apply to enough objects
- Associativity is nice and is also true for almost all operations. It allows us to prove the inverse is unique, which in turn gives us a nice bit of symmetry