Definitions

Group: a set G endowed with an operation $* : G \times G \to G$ that has the following properties.

- well-defined: $a * b \in G$ for all $a, b \in G$;
- associativity: $a * (b * c) = (a * b) * c$
- unit: there exists an element $e \in G$ such that $a * e = e * a = a$ for all $a \in G$;
- inverses: for every $a \in G$ there exists an element $b \in G$ such that $a * b = b * a = e$ (denoted $b = a^{-1}$).

Abelian (commutative) group: a group $(G, *)$ with the property that $a * b = b * a$ for all $a, b \in G$.

Subgroup of a group $(G, *)$: a subset $H \subset G$ such that $(H, *)$ is a group (same operation as G).

Cyclic subgroup generated by an element a : $\langle a \rangle = \{a^n; n \in \mathbb{Z}\}$. This is the smallest subgroup that contains a.

Cyclic group: A group that is generated by just one of its elements.

Order of a group: the number of elements in that group. Notation: $|G|$.

Order of an element: the number of elements in the subgroup generated by that element;

$$|a| = |\langle a \rangle| = \begin{cases} \min\{n \geq 1; a^n = e\} & \text{if such a power exists;} \\ \infty & \text{otherwise (i.e. } a^n \neq e \text{ for all } n \geq 1) \end{cases}$$

Centralizer of an element a**:** $C(a) = \{b \in G; a * b = b * a\}$ (it is subgroup of G).

Center of a group G**:** $Z(G) = \{b \in G; b * x = x * b \text{ for all } x \in G\}$ (it is subgroup of G).

Theorems

1. Subgroup tests for a nonempty subset H of a group $(G, *)$

   One-step test: $a, b \in H \implies a * b^{-1} \in H$
   Two-step test: $a, b \in H \implies a * b \in H$ and $a \in H \implies a^{-1} \in H$

2. If $|a| < \infty$, then $|a^k| = \dfrac{|a|}{\gcd(k, |a|)}$.

3. If $|a| = \infty$ and $k \neq 0$, then $|a^k| = \infty$.

4. Every cyclic group is abelian. Therefore if a group is not abelian, it cannot possibly be cyclic.

5. However, even a nonabelian group has cyclic subgroups, and it can have other abelian subgroups. For instance, the center of G is an abelian subgroup of G.

6. An element a generates a *finite* group $G \Leftrightarrow |a| = |G|$.

7. The structure of a cyclic group $G = \langle a \rangle$ of order n

   - every subgroup of G is cyclic
   - the order of every subgroup divides $|G|$
   - the order of every element of G divides the order of the group
   - for every divisor d of n there exists a *unique* subgroup H of G with $|H| = d$; namely H is the cyclic subgroup generated by $a^{n/d}$
   - for every divisor d of n (including n), there are exactly $\varphi(d)$ elements of order d
   - if $k \nmid n$, there are no elements in G of order k

Examples of groups

1. $\mathbb{Q}, \mathbb{R}$ are groups under addition. $\mathbb{R}^*, \mathbb{Q}^*, \mathbb{R}^*_+, \mathbb{Q}^*_+$ are groups under multiplication.
2. $\mathbb{Z}$ is a group with $+$. It is the quintessential example of an infinite cyclic group.
   - generated by 1 and -1; that is, $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$
   - all its subgroups are cyclic, generated by nonnegative integers; they are of the form $\langle n \rangle = n\mathbb{Z}$
   - $m \in \langle n \rangle \Leftrightarrow m$ is a multiple of n
3. Z_n is group under addition modulo n. It is the quintessential example of a cyclic group of order n.
   - generated by 1
   - it is in fact generated by all k with $\gcd(k, n) = 1$; these are all its generators
   - its subgroups are of the form $\langle d \rangle$ where $d|n$; and $|\langle d \rangle| = |d| = n/d$.
   - it has $\varphi(d)$ elements of order $d|n$ and no elements of any order that does not divide n
   - the one and only subgroup of order $d|n$ of G has exactly $\varphi(d)$ generators, namely the elements of G of order d
4. $U(n) = \{1 \leq k \leq n; \gcd(k, n) = 1\}$ is a group under multiplication modulo n.
   - It has order $\varphi(n) = \varphi(p_1^{c_1})\varphi(p_2^{c_2}) \ldots \varphi(p_r^{c_r})$, if $n = p_1^{c_1} \ldots p_r^{c_r}$.
   - Recall that φ is called Euler's phi function and that $\varphi(p^c) = p^{c-1}(p-1)$.
   - The group $U(n)$ is abelian, but not necessarily cyclic. (E.g. $U(8)$ is not cyclic.)
   - It is NOT a subgroup of Z_n since they don't have the same operation.
5. D_n is the group of symmetries of the regular n-sided polygon.
   - Its elements are transformations of the 2-dimensional real plane into itself that leave the polygon in the same position in the plane. So they are function $\mathbb{R}^2 \to \mathbb{R}^2$ that preserve a regular n-sided polygon centered at the origin.
   - It has $2n$ elements: n rotations $(R_0, R_{2\pi/n}, \ldots, R_{2(n-1)\pi/n})$ and n flips across the symmetry axes of the polygon.
   - It is not abelian.
   - Rotation $\circ$ flip = (another) flip, flip $\circ$ rotation = (yet another) flip, flip $\circ$ flip = rotation
   - The elements of D_n can be expressed as 2×2 real matrices.
6. $\mathrm{GL}(2, F)$ the group of 2×2 *invertible* matrices with entries from $F = \mathbb{Q}, \mathbb{R}, \mathbb{Z}$ or Z_p (p is a prime). This is a group under matrix multiplication (all arithmetic is done in F, so modulo p in case of Z_p).
   - Saying that a matrix is invertible is the same as saying that its determinant has an inverse in F. That means the determinant is $\neq 0$ if $F = \mathbb{Q}, \mathbb{R}, Z_p$. But when $F = \mathbb{Z}$ this amounts to the determinant being ± 1.
   - It is not abelian.
   - Its center is $\{\lambda I; \lambda \in F\}$, where $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.
7. $\mathrm{SL}(2, F)$ is the group of 2×2 matrices with entries from $F = \mathbb{Q}, \mathbb{R}, \mathbb{Z}$ or Z_p (p is a prime) and determinant 1. This is a group under matrix multiplication (all arithmetic is done in F, so modulo p in case of Z_p).
   - It is not abelian.
   - It is a subgroup of $\mathrm{GL}(2, F)$.