BASIC FACTS ABOUT GROUPS

(To be filled in later.)

- Uniqueness of identity: $e' = e'e = e$.
- Uniqueness of inverse: $b = be = b(ac) = (ba)c = ec = c$.
- Granting a right-identity and right-inverses, they are two-sided: Given a, let b a right-inverse of a and then let c be a right-inverse of b. Then also b is a left-inverse of a,
$$ba = (ba)e = (ba)(bc) = ((ba)b)c = (b(ab))c = (be)c = bc = e.$$
Now compute that e is a left-identity since given a,
$$ea = (ab)a = a(ba) = ae = a.$$
- Generalized associativity: For $n \geq 2$ let $P(n)$ be the proposition that for all group elements $g_1, \cdots, g_n$, all groupings of the product $g_1 \cdots g_n$ are equal. Certainly $P(2)$ holds. And if $n > 2$ and $P(k)$ holds for $2 \leq k < n$ then $P(n)$ follows by generalized induction,
$$\begin{aligned}(g_1 \cdots g_i)(g_{i+1} \cdots g_n) &= (g_1 \cdots g_i)((g_{i+1} \cdots g_j)(g_{j+1} \cdots g_n))\\ &= ((g_1 \cdots g_i)(g_{i+1} \cdots g_j))(g_{j+1} \cdots g_n)\\ &= (g_1 \cdots g_j)(g_{j+1} \cdots g_n).\end{aligned}$$
- Generalized commutativity in abelian groups.
- $g^2 = g \implies g = e$.
- Left and right cancellation laws.
- $(g^{-1})^{-1} = g$ because $g^{-1}g = e$.
- $(ab)^{-1} = b^{-1}a^{-1}$.
- $ax = b \iff x = a^{-1}b$ and $xa = b \iff x = ba^{-1}$.
- For any $a \in G$ and $n \in \mathbb{Z}$, define
$$a^n = \begin{cases} e & \text{if } n = 0,\\ a^{n-1} \cdot a & \text{if } n > 0,\\ (a^{-n})^{-1} & \text{if } n < 0.\end{cases}$$
Then
$$a^{n+m} = a^n a^m \quad \text{and} \quad (a^n)^m = a^{nm} \quad \text{for all } n, m \in \mathbb{Z}.$$
- Definition of subgroup, various subgroups tests, arbitrary intersection of subgroups is a subgroup. Definition of $\langle S \rangle$.