Lecture 5. relations *September 27, 2025*

1 Relations

1.1 Symmetry Groups

An alternative to number systems as the basis of groups is symmetries of systems/ objects. To construct these consider the set S and a group acting on the set S called the permutation group $Perm(S)$ which is the set of bijective maps $f : S \leftrightarrow S$ has a law of composition defined as function composition. The order of the group $Perm(S)$ is $|Perm(S)| = n!$ when S is finite (usually this is the case with a permutation group). If $S = \{1, 2, \ldots, n\}$ then $Perm(S)$ is denoted S_n is is known as the symmetry group.

Definition 1 (Symmetric Groups)**.** The symmetric group is a set $Perm(S)$ acting on a set S of order n, denoted S_n such that $Perm(S)$ is the set of bijective maps $f : S \leftrightarrow S$ with the law of composition of $Perm(S)$ being function composition. We denote the permutations via σ^n and τ^n, where σ is a permutation via shifts and τ is a permutation via swaping two given elements.

Problem (1.1.1)**.** We know that the group S_n is non-abelian $\forall n \geq 3$. Why is this? First we demonstrate by example. Consider the group with the set $S = \{1, 2, 3, 4\}$, notice that $|S_4| = 4! = 24$. The group is made of up a sequence of perumtations $e, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3$, where σ^n is a shift of order n such that $(1, 2, \ldots, m) \mapsto (\ldots, m, 1, 2, \ldots)$, so, for example, $(1, 2, 3)$ under σ^2 results in $\sigma^2(1, 2, 3) = (2, 3, 1)$ since $(1, 2, 3) \overset{\sigma}{\mapsto} (3, 1, 2) \overset{\sigma}{\mapsto} (2, 3, 1)$. The τ is a switch between any two elements: $(1, 2, 3) \overset{\tau}{\mapsto} (1, 3, 2)$, but τ^2 simply reverses whatever mapping we made by acting on the same elements we applied τ to, i.e., $(1, 2, 3) \overset{\tau}{\mapsto} (1, 3, 2) \overset{\tau}{\mapsto} (1, 2, 3)$. Given these facts, (note that we are going to drop the commas for the sequence of numbers) notice that $\tau\sigma(1234) \Rightarrow (1234) \overset{\sigma}{\mapsto} (4123) \overset{\tau}{\mapsto} (1423)$, but $\sigma\tau(1234) \Rightarrow (1234) \overset{\tau}{\mapsto} (2134) \overset{\sigma}{\mapsto} (4213)$. Notice, then, that $(1423) \neq (4213)$, thus it mustn't be the case that S_4 is abelian. This, in general, is true for all $S_n \mid n \geq 3$.

A similar notion that arises from symmetric groups is the dihedral group: the set of symmetries of S under rotation and reflection where S is the set of verticies of a regular n-gon in the plane (a plane). We call this D_n.

Definition 2 (Dihedral Groups)**.** A dihedral group, denoted D_n is the set of symmetries of S under rotation and reflection (function composition) as the law of composition, where S is the set of all verticies of a regular n-gon. This is a special type of symmetric group.

As a quick side-note we use μ and ρ is function notation for our relfections and rotations, respectively, in relation to dihedral groups. There is a good amount of similarity with τ and σ from symmetric groups.

Problem (1.1.2)**.** Consider the dihedral group D_3, notice that it is isomorphic to S_3. Notice, however, that this is not the case for D_4 and S_4. We use ρ and μ for rotations and reflections (LoC) under D_n (similar to σ and τ). For D_3 we have a 3-gon, which is simply a triangle. We may assign to each of its three verticies a number such that under the transformations of ρ and μ we achieve rotations and reflections. Below is an example of this:

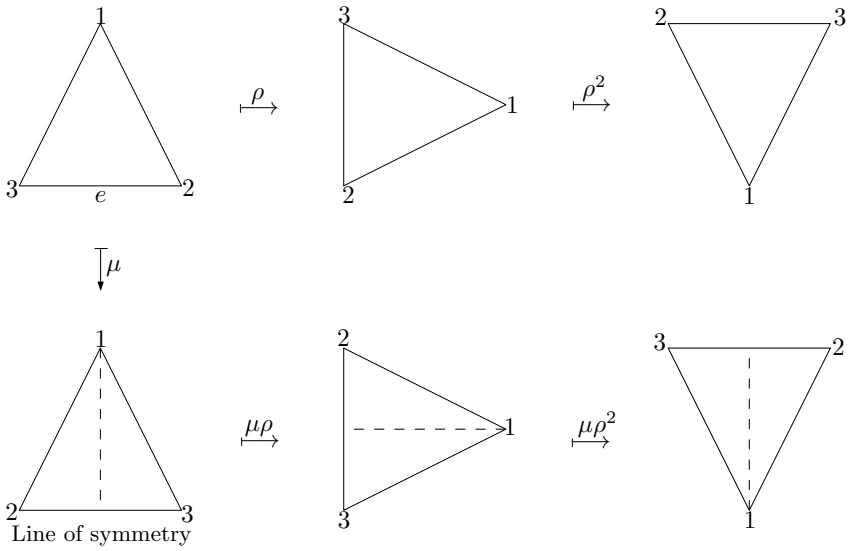

Figure 1

The observed triangle is a geometric representation of D_3. We can see that the order is given by $|D_3| = |\{e, \rho, \rho^2, \mu, \mu\rho, \mu\rho^2\}| = 6$, the same as S_3; however when observing D_4 and S_4, we notice that these are incapible of being isomorphic since they have different orders: $|D_4| = |\{e, \rho, \rho^2, \rho^3, \mu, \mu\rho, \mu\rho^2, \mu\rho^3\}| = 8$ and $|S_4| = |\{e, \sigma, \sigma^2, \sigma^3, \tau\sigma, \tau\sigma^2, \tau\sigma^3, \tau^2\sigma, \ldots\}| = 24$. Interesting! It seems, from observation that while S_n follows the rule of order $n!$, D_n follows the rule of order $2n$. Notice that the mappings that involve μ in D_3 are all reflections on a different axis of symmetry, the axis of symmetry under e, ρ and ρ^2. We can thus imagine D_3 as $2n$ due to the fact that it has n rotations, and therefore n axies of symmetry $\Rightarrow n + n = 2n$. □

Something to note is that, as we increase in dimensionality (recall that D_n is restricted to n-gons in $\mathbb{R}^2$), i.e., as n increases for $\mathbb{R}^n$, then the order of the group has more and more complex reflections (μs), which meet S_n's order and even exceeds it. A general rule is: for $\mathbb{R}^n$, $|G| = 2^n(n!)$. The number of rotations and reflections, however, can be infinite (for example consider the set of all symmetries of a circle).

Definition 3 (Linearity)**.** Linearity of a bijective function is determined by the rule that $\phi(v + w) = \phi(v) + \phi(w), \forall v, w \in \mathbb{R}^n$ and $\phi(\lambda v), \forall v \in \mathbb{R}^n, \lambda \in \mathbb{R}$. Notice our v, w quantities are vectors and our λ quantity is a scalar.

Definition 4 (General and Special Linear Groups)**.** Consider the symmetries of $S = \mathbb{R}^n$ but restrict the set of bijections to be only those which are linear (as defined in the previous definition). This forms the group $GL_n(\mathbb{R})$, i.e., the group of $n \times n$ matrices with nonzero determinant. Similarly, a special case is $SL_n(\mathbb{R})$, which is the special linear group which is the same as the general linear group except the determinant is specified to be 1.

Definition 5 (Orthogonal Groups). An orthogonal group is a type of symmetric group that is the linear maps $\Gamma : \mathbb{R}^n \to \mathbb{R}^n$ that respect (preserve) distance.

1.2 Group Relations

Definition 6 (Subgroups). A subgroup of G is a subset $H \subset G$ such that H is closed under the law of composition of G (i.e., $\forall a, b \in H ab \in H$) and $\forall a \in H \exists a^{-1} \in H$ s.t. $aa^{-1} = e$.

Definition 7 (Generators and Generation). Group generation happens as a concequence of our definition of subgroups. Notice, that given $H \leq G$ (we use $\leq$ and $\geq$ notation to indicate subgroup-ness) we can construct the smallest subgrop of G by taking the intersection of all subgroups of G; notice that this intersection is indeed a subgroup as well. For generation of a group we want to take the samllest subset denoted $S \subset G$ such that there exist a samllest subgroup that contains S:

$$G_{smallest} = \bigcap_{H \leq G; H \geq S} H$$

we use the terminology that $S = \langle S \rangle$ is the generator of G if $\langle S \rangle = G$.

We can now use this bit of information to come up with a more formal definition of cyclic groups:

Definition 8 (Cyclic Groups). A group is a cyclic group $\Leftrightarrow$ all elements in the group are generated by a single element.

1.3 Homomorphisms

Definition 9 (Homomorphisms). If H and G are two groups, a homomorphism is given by $\varphi : H \to G$ as a map that respects the laws of composition in G and H, i.e., $\forall a, b \in H$,

$$\varphi(ab) = \varphi(a)\varphi(b).$$

We can denote this using a commutative diagram,

$$\begin{array}{ccc} G \times G & \xrightarrow{\varphi \times \varphi} & H \times H \\ {\scriptstyle m_G}\downarrow & & \downarrow{\scriptstyle m_H} \\ G & \xrightarrow{\varphi} & H, \end{array}$$

where m_G, m_H are the laws of compsoition for G, H, respectively. What makes this diagram a homomorphism is thereby the very fact that it commutes.

Let's take two interesting cases: the inverse and the identity of a group under homomorphism: consider e_H and e_G. By homomorphism, it must be the case that $\varphi(e_H e_G) = \varphi(e_H)\varphi(e_G)$, however, notice that since this is the identity, in order to preserve group structure, we result in the identity (e_H or simply e). if this is the case we can say $\varphi(e_G) = e$ and $\varphi(e_H) = e$, thus, $\varphi(e_H) = e = \varphi(e_G)$. Similarly, take the inverse of some given $a \in G$, $a^{-1} \in G$, notice that $\varphi(a^{-1}) = \varphi(a)^{-1}$.