# Summary of Group Theory

NyKi

November 26, 2024

## Contents

## 1 Preface

This file contains my notes for my study of group theory.

## 2 Elementary group theory

- **Definition of a group:** A group is a set G equipped with an operation $*: G \times G \to G$ such that:
  - $\forall a, b, c \in G \ a(bc) = (ab)c$ (Associativity)
  - $\forall a \in G \ \exists a^{-1} \in G \mid a * a^{-1} = a^{-1} * a = 1$ (Existence of inverses)
  - $\exists e \in G \mid \forall a \in G \ a * e = e * a = a$ (Such an e is called an dentity element)

  We usually denote the set and the operation $(G, *)$ with only the name of the set, in this case G. The symbol of the operation * is normally omitted and thus the operation is denoted by juxtaposition of elements. If $\forall a, b \in G$ we have $ab = ba$ then G is said to be commutative or **abelian**.
  Note that the identity in a group is unique (which we normally denote by either e or 1) and so is the inverse of an element. We can easily see that $\forall a_i \in G$ where $i$ ranges over some finite index set we have that $(a_1 a_2 \cdots a_k)^{-1} = a_k^{-1} \cdots a_1^{-1}$. We can check this by multiplying $a_1 a_2 \cdots a_k$ and $a_k^{-1} \cdots a_1^{-1}$ together. If the set underlying G is finite, then we can talk about its number of objects. We call this number the **order** of G and denote it by $|G|$.

- **Definition of a subgroup:** A subgroup H of a group G is a subset of G such that the operation of such group makes H into a subgroup. We write $H \leq G$.
  We also have multiple ways of checking if a subset is a subgroup, which we call **subgroup tests**:
  - **Finite subgroup test:** If H is a nonempty finite subset of a group G that is closed under the operation, then $H \leq G$.
  - **Full subgroup test:** A nonempty subset H of G is a subgroup of G iff $\forall a, b \in H$ we have that $ab^{-1} \in H$.

  If we consider the set $Sub(G)$ of all subgroups of a group G, then this set is closed under intersections. However, it is not closed under unions. We can make $Sub(G)$ into a complete lattice under set inclusion (this is an order theoretic structure, which means that the set inclusion gives the set some kind of order). In general it's also not closed under multiplication of sets (we define it like $HK = \{hk \ \forall h \in H, \ \forall k \in K\}$), however if one of the subgroups is normal (to be defined below) then the result is a subgroup. Moreover, multiplication of normal subgroups is again normal.
  We can talk about the **subgroup generated by a set X**, which is the intersection of all subgroups that contain X. It can also be described via all the finite products of elements in X + their inverses or as the smallest subgroup which contains X. We'll denote it by $\langle X \rangle$. The subgroup generated by just one element is of importance. The **order of an element** is the order of the subgroup generated by itself.
  An easy example is the trivial subgroup, which consists only of the identity.

- **Definition of normal subgroup:** A subgroup N of G is a normal subgroup if it's *invariant under conjugation*, that means that $\forall n \in N \ \forall g \in G \ \exists n' \in N$ such that $n' = gng^{-1}$. We write $\forall g \in G \ N = gNg^{-1}$. We denote normal subgroups by $N \lhd G$. To prove a subgroup is normal, we only need to prove that $N \subseteq gNg^{-1}$, because we can just right multiply by $g$ and left multiply by $g^{-1}$ and change $g$ with $g^{-1}$ (we can do this because invariation under conjugation happens by all members in the group) and get $gNg^{-1} \subseteq N$ which would imply $N = gNg^{-1}$. The intersection of normal subgroups is again normal, and the multiplication is also normal. So, the set of all normal subgroups of a group is closed under intersection and multiplication.
  An example of an important normal subgroup is the **center** of the group: $Z(G) = \{\forall g \in G \mid gx = xg \ \forall x \in G\}$, or in words all the elements of G that commute with every element in G. If we have a subset $X$ of the group, we can define the **normal**

**closure** to be the smallest normal subgroup that contains the subset, or the intersection of every normal subgroup that contains X. Both definitions are equivalent. We are gonna denote this by $\langle X\rangle_N$
These types of subgroups are important because their left cosets coincide with their right cosets (to be defined). We call a group G **simple** if its only normal subgroups are the trivial subgroup and G.

- **Definition of a homomorphism:** A map of sets $f : G \to H$ is a group homomorphism if we have $f(ab) = f(a)f(b)\ \forall a, b \in G$.
  This definition basically says that the map f "conserves" the group structure. More precisely, it commutes with the proper group operations (it doesn't matter if you do f first then multiply or you multiply first and then do f). We can make the category *Grp* where objects are groups and the morphisms are the homomorphisms between them. For simplicity, we'll sometimes call homomorphisms just morphisms to ease writing and reading. We can assign to a morphism $f : G \to H$ different types of structures:
  - **Im(f):** Defined to be the set of all x in H that can be "reached" with f. More precisely, $Im(f) = \{f(a)\ \forall a \in G\}$. This is a subgroup of H.
  - **Ker(f):** Defined to be the set of all x in G that are sent to the group identity in H. More precisely, $Ker(f) = \{x \in G \mid f(x) = e\}$ where e denotes the identity in H. This is a normal subgroup of G. Moreover, every normal subgroup can be identified with the kernel of some morphism.
  - **Coker(f):** This structure is defined using a quotient (to be defined later). It is $Coker(f) = H/Im(f)$. This object correspondes to the dual of the kernel in category theory.

  A morphism $f : G \to H$ can be:
  - **Injective (monomorphism):** If $\forall a, b \in G\ f(a) = f(b)$ implies $a = b$. Equivalent to $Ker(f) = \{0\}$.
  - **Surjective (epimorphism):** If $\forall a \in H\ \exists b \in G$ such that $f(b) = a$. Equivalent to $Im(f) = H$.
  - **Isomorphism:** Both injective and surjective.
  - **Endomorphism:** $G = H$.
  - **Automorphism:** Both endo and iso.

  The definition of group may seem mysterious at first, but we can make sense of it thanks to Cayley's Theorem now that we have defined isomorphisms.

- **Theorem 2.1 (Cayley's Theorem)** *Every group G is isomorphic to a subgroup of Sym(G), where Sym(G) denotes the symmetric group of G (elements are permutations of the set of G and operation is composition of permutations.)*

  We can interpret this theorem by saying that groups represent symmetries of the set they are built upon, so if we have a set we can "add" an operation which gives the set symmetries. Of course, we can always interpret a group abstractly by saying it's an abstraction of some operations present in mathematics, but having some intuition is always nice.

- **Definition of cosets:** A left coset $gH$ of a subgroup $H \leq G$ is defined to be the set $\{gh\ \forall h \in H\}$ where $g \in G$. We can define the right coset $Hg$ by commuting the operation inside the set from $gh$ to $hg$. In reality, we can define the set $gS$ for any subset S of G, but if S is a subgroup then it attains some nice properties that are really important (in the following list, a and b denote arbitrary members of the group and H,K are arbitrary subgroups):

  1. $a \in bH$ iff $aH = bH$.
  2. Either $aH = bH$ or $bH \cap aH = \emptyset$
  3. $aH = bH$ iff $a^{-1}b \in H$
  4. $|aH| = |aK|$ if they are finite (note that here we are talking about cardinalities of finite sets, not the order of groups. In general, a coset of a subgroup is not a group under the same operation as in the overlying group).
  5. The left cosets of H cover G. More precisely $\forall g \in G\ \exists g' \in G$ such that $g \in g'H$.

  We can also prove all of these with right cosets instead of left cosets. Particularly, of interest there are the normal subgroups, where these cosets coincide ($gN = Ng$).
  It's possible to define an equivalence relation $a \sim b$ iff $aH = bH$, which is indeed one. Its equivalence classes are the cosets themselves.
  Thanks to all of these properties we can define the **index** of a subgroup into its supergroup: $[G : H]$ is equal to the number of possible different cosets for the subgroup H. Using the above, we can define it to be $[G : H] = |G|/|H|$. This leads us to the next theorem:

- **Theorem 2.2 (Lagrange's Theorem)** *Suppose G is a group and H is a subgroup of G. Then, the order of H divides the order of G. More precisely,* $|G| = [G : H]|H|$.

  This one provides an strong requirement for a subset to be a subgroup: its order needs to divide the order of the group, which becomes pretty useful when trying to find subgroups. For example, if G has prime order, then the only possible subgroups are the trivial subgroup and G. So that means that any element needs to have either order 1 (which means it's the identity) or order p (generate the group), so we can generate the group with only one element and thus it's cyclic.
  We can also "generalize" Lagrange's Theorem:

- **Theorem 2.3 (Generalized Lagrange's Theorem)** *Suppose $G$ is a group and $H$,$K$ are subgroups of $G$ with $K \subset H$. Then we have the equality $[G:K]=[G:H][H:K]$.*

  We can see this is a generalization of Lagrange's Theorem if we note that $[G:1]=|G|$, where 1 denotes the subgroup of G that consists only of the identity (it is a subgroup because it's finite and closed under the operation), so we could rewrite it as $[G:1]=[G:H][H:1]$.

- **The quotient group.** We start by defining, for a group G and a normal subgroup N the set of cosets of N in G: $G/N$. Due to N being a normal subgroup, we don't need to differentiate between right and left cosets. This can also be defined as the equivalence classes of the equivalence relation $a \sim b$ iff $aH = bH$.
  Now to give it a group structure, we simply define $[a][b]=[ab]$. This is well defined and satisfies the axioms of a group.
  We can define the **projection homomorphism** $\pi_N : G \to G/N$ via $\pi_N(x)=xN$. When the subgroup is clear, we just denote it by $\pi$.

- **Theorem 2.4 (Canonical decomposition of homomorphisms)** *Let G be a group, $f:G \to H$ a group morphism, i the inclusion morphism of $Im(f)$ to H, $\alpha : G/Ker(f) \to Im(f)$ defined by $\alpha(gN)=f(g)$, then the following diagram commutes:*

$$\begin{tikzcd}
G \arrow[r, "f"] \arrow[d, "\pi"] & H \\
G/Ker(f) \arrow[r, "\alpha"] & Im(f) \arrow[u, "i"]
\end{tikzcd} \tag{1}$$

  *In other words $f = i \circ \alpha \circ \pi$.*
  *Moreover, $\alpha$ is an isomorphism, so $G/Ker(f) \cong Im(f)$.*

  This theorem is also known as the first isomorphism theorem. In reality, this theorem comes from a deeper and simpler theorem of sets, the canonical decomposition of functions between sets, which is in essence the same but considering general morphisms of sets instead of morphisms of groups.

- **Theorem 2.5 (Second isomorphism theorem)** *Let G be a group, H a subgroup and N a normal subgroup. Then, N is a normal subgroup of HN, and $H \cap N$ a normal subgroup of H. Moreover,*

$$HN/N \cong H/(H \cap N) \tag{2}$$

- **Direct product:** We define the direct product of a group $(G,*)$ and $(H,\star)$ to be the group $(G\times H,\cdot)$ where $\cdot$ is defined as $(g_1,h_1)\cdot(g_2,h_2)=(g_1 * g_2, h_1 \star h_2)$. This is basically the group with the underlying set the cartesian product of $G$ and $H$ and the operation is component wise with respect to each group. We can extend this definition to the direct product of more than 2 groups, using the same cartesian product construction. We also normally denote the direct product via $\otimes$ instead of the usual cartesian product symbol. If we have a group and some subgroups, we can see if our supergroup is the direct product of them via the next theorem:

- **Theorem 2.6 (Conditions for direct product)** *Let G be a group and $H_1, H_2, \cdots, H_n$ be subgroups of G. Then, $G = \bigotimes_{k=1}^n H_k$ iff*

  1. $G = \Pi_{k=1}^n H_k$
  2. $(\forall\ 1 \le k \le n)\ H_k \lhd G$
  3. $(\forall\ 1 \le k \le n)\ H_k \cap (\Pi_{j=1\ j\neq k}^n H_j) = \{e\}$

- **Presentation of groups:** We first define the **free group** over a set, in a not really rigorous way, but that will let us do practically everything we want with them. If we have a set $X$, the free group over $X$, which it's sometimes denoted by $FX$ or $Free(X)$ or as we'll see $\langle X\rangle$, is defined to be the set of **words** where the letters are the members of the set $X$ and their inverses, in which we add an identity and the operation is concatenation. For example, with $X=\{a,b,c\}$, some members of the free group over X would be *abc*, *bbbaac*, $a^{-1}c$, $b^{-1}b=e$. Note that this group right now is infinite. We can now "subject" these words onto some conditions. For example, if we have *ab* in a word we can make it so we can change it with *c*. So, for example we have $bbcabaaaab = bbccaaac$. We'll call these conditions that are of the type some member of the group $= e$ a **relation**. A **presentation of a group** $G$ is simply a set $X$ of symbols and a set of members of the free group of $X$ which we'll call $R$ where $Free(x)$ subject to the relations $\alpha = e\ \forall \alpha \in R$ is isomorphic to $G$. We will denote these by $\langle X, R\rangle$. We now have the following theorem:

- **Theorem 2.7 (Quotients of free groups)** *Let $X$ denote a set and $R$ a set of relations for the free group $FX$. Then, the group generated subject to the relations $R$ is $(FX)/\langle R\rangle_N$. We also have that every group is a quotient of a free group, and thus has a presentation. Moreover, finite groups have finite presentations (both $X$ and $R$ finite).*

  Probably the most important part of this theorem is that we can have a group presentation for any group.

- **Theorem 2.8 (Subgroups of free groups)** *If we have $H \le FX$, then $H$ itself is free.*

-