Group Theory

Amit Rajaraman

March 31, 2020

Contents

§1 Introduction to Groups

1.1 Definitions and Basics

Definition 1.1. A group G is an ordered pair $(G, *)$ where G is a set and $*$ is a binary operation such that

1. $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$, that is, G is associative.
2. There exists an element e in G, which we call an *identity* of G, such that for all $g \in G$, $a * e = e * a = a$.
3. For each $g \in G$, there exists an element $g^{-1} \in G$ called an *inverse* of g such that $g * g^{-1} = g^{-1} g = e$.

We say that G is a group under $*$ if $(G, *)$ is a group. If $*$ is clear from context, we sometimes just say that G is a group.
We further say that G is a *finite group* if G is a finite set. Note that any group is nonempty.

Definition 1.2. We say that a group $(G, *)$ is *abelian* if $a * b = b * a$ for all $a, b \in G$.

Exercise 1.1. Show that $\mathbb{Z}, \mathbb{R}, \mathbb{C}$ and $\mathbb{Q}$ are abelian groups under the addition operation.

Exercise 1.2. Show that $\mathbb{Z} \setminus \{0\}, \mathbb{R} \setminus \{0\}, \mathbb{C} \setminus \{0\}$ and $\mathbb{Q} \setminus \{0\}$ are abelian groups under the multiplication operation.

We define the set $\mathbb{Z}/n\mathbb{Z}$ for some integer n as follows. Let $\sim$ be an equivalence class given by

$$a \sim b \text{ if and only if } n \mid (b - a).$$

Each equivalence class is given by $\overline{a} = \{a + kn \mid k \in \mathbb{Z}\}$. There are precisely n equivalence classes, namely $\overline{0}, \overline{1}, \ldots, \overline{n-1}$. These n equivalence classes are the elements of the set $\mathbb{Z}/n\mathbb{Z}$.
For $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$, we further define addition and multiplication as

$$\overline{a} + \overline{b} = \overline{a + b} \text{ and } \overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

We see that $\mathbb{Z}/n\mathbb{Z}$ is an abelian group under the addition operation with $e = \overline{0}$ and the inverse of $\overline{a}$ as $\overline{-a}$. We denote this group as $\mathbb{Z}/n\mathbb{Z}$.
Further, recall from number theory that a number a has a multiplicative inverse modulo n if and only if $(a, n) = 1$. We also see that the set of equivalence classes $\overline{a}$ which have multiplicative inverses modulo n is also an abelian group under multiplication. We denote this group as $(\mathbb{Z}/n\mathbb{Z})^\times$.

Definition 1.3. Let $(A, \star)$ and $(B, \diamond)$ be two groups. We can form a new group $A \times B$, called the *direct product* of A and B, whose elements are those in the cartesian product, and whose operation $\cdot$ is as follows.

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 \star a_2, b_1 \diamond b_2) \text{ for all } a_1, a_2 \in A, b_1, b_2 \in B$$

Theorem 1.1. Let G be a group under an operation $\star$. Then

1. The identity of G is unique.
2. For each $g \in G$, g^{-1} is unique.
3. For each $g \in G$, $(g^{-1})^{-1} = g$.
4. For any $a_1, a_2, \ldots, a_n \in G$, the value of $a_1 \star a_2 \star \cdots \star a_n$ is independent of how we bracket it. This is called the *generalized associative law.*
5. For $a, b \in G$, $(a \star b)^{-1} = b^{-1} \star a^{-1}$.

Proof. We prove each of the parts of the theorem.

1. Let f and g be two identities of G. We have $f \star g = f$ and $f \star g = g$, which implies that $f = g$. Thus the identity of a group is unique.

2. Let $a, b \in G$ be two inverses of some $g \in G$. We have

$$\begin{aligned} a \star g &= b \star g \text{ where } e \text{ is the identity of } G \\ a \star g \star a &= b \star g \star a \\ a \star e &= b \star e \\ a &= b \end{aligned}$$

3. We have $g^{-1}g = gg^{-1} = e$ which implies that $(g^{-1})^{-1} = g$.

4. We leave this as an exercise to the reader. The idea is induction on n. First show the basis, then that any bracketing of k elements $g_1, \ldots, g_k$ can be reduced to $g_1 \star (g_2 \star (\cdots g_k)) \cdots)$. Next, argue that $a_1 \star a_2 \star \cdots \star a_n$ can be reduced to $(a_1 \star \cdots \star a_k) \star (a_{k+1} \star \cdots \star a_n)$ for some k. Apply the induction condition on each subproduct to complete the result.

5. Using the fourth result in this theorem on $(a \star b) \star (b^{-1} \star a^{-1})$ and $(b^{-1} \star a^{-1}) \star (a \star b)$ gives the required result.

■

Notation. Henceforth, for any group G under operation $\star$, we shall write $a \star b$ as ab unless it is needed that we mention it explicitly.
For some group G, $g \in G$ and $n \in \mathbb{Z}^+$, we write $xxx \cdots x$ (n times) as x^n.
We usually write the identity element of any group as 1.

Theorem 1.2. Let G be a group and let $a, b \in G$. The equations $ax = b$ and $ya = b$ have unique solutions for $x, y \in G$. In particular, $ax = bx$ if and only if $a = b$ and $ya = yb$ if and only if $a = b$.

Proof. Premultiplying and postmultiplying the two equations respectively and using the fact that inverses are unique gives the unique solution for x and y. ■

Definition 1.4. Let G be a group and $x \in G$. Let n be the smallest positive integer such that $x^n = 1$. This number is called the *order* of x and is denoted by $|x|$. If no positive power of x is the identity, x has order defined to be infinity and is said to be of infinite order.

Theorem 1.3. Any element of a finite group is of finite order.

Proof. Let $x \in G$. There are only finitely many distinct elements among $x, x^2, x^3, \ldots$. If $x^a = x^b$ for some integers a, b such that $b > a$, we have $x^{b-a} = 1$, that is, x is of finite order. ■

Example. In any group, the only element of order 1 is the identity. In the (additive) groups $\mathbb{R}, \mathbb{Z}, \mathbb{Q}$ and $\mathbb{C}$, any non-identity element is of order infinity. In $(\mathbb{Z}/7\mathbb{Z})^\times$, $\overline{2}$ is of order 3.

Definition 1.5. Let $G = \{g_1, g_2, \ldots, g_n\}$ be a finite group with $g_1 = 1$. The *multiplication table* of G is an $n \times n$ matrix whose i, j element is $g_i g_j$.

This is a helpful way to understand the structure of any group.

Definition 1.6. Let G be a group under an operation $\star$. A subset H of G is called a *subgroup* of G if H also forms a group under the operation $\star$.

Example. $\mathbb{Q}$ is a subgroup of $\mathbb{R}$ under addition.

Exercise 1.3. If $x, g \in G$. Prove that $|x| = |gxg^{-1}|$. Deduce that $|ab| = |ba|$ for any $a, b \in G$.

Exercise 1.4. Let G be a group. Prove that if $x^2 = 1$ for all $x \in G$, G is abelian.

Exercise 1.5. If x is an element of a group G, prove that $\{x^n \mid n \in \mathbb{N}\}$ is a subgroup of G. This subgroup is called the *cyclic subgroup* generated by x.

Exercise 1.6. If x is an element of infinite order in G, prove that $x^n, n \in \mathbb{Z}$ are all distinct. Deduce that if $x^i = x^j$ for some $i, j \in \mathbb{Z}, i \neq j$, x is of finite order.

Exercise 1.7. Let A, B be two groups and let $a \in A, b \in B$. Show that $(a, 1)$ and $(1, b)$ commute in $A \times B$. Further show that the order of (a, b) in $A \times B$ is the least common multiple of $|a|$ and $|b|$/

Exercise 1.8. Let $G = \{1, a, b, c\}$ be a group of order 4. If G has no elements of order 4, prove that there is a unique group table for G. Deduce that G is abelian. This group is called the *Klein four-group*.

1.2 Dihedral Groups

For each $n \in \mathbb{Z}^+$, $n \geq 3$, let D_{2n} be the set of symmetries of a regular n-gon. A symmetry is any rigid motion of the n-gon which can be done by taking a copy of the polygon, moving it around in 3-dimensional space and superimposing it on the original polygon.
We can think of this as first labeling the n vertices as $1, 2, \dots, n$ and describing each symmetry of the permutation σ of $\{1, 2, \dots, n\}$ corresponding to this symmetry.
We make D_{2n} into a group by defining st for $s, t \in D_{2n}$ to be the symmetry obtained by first applying t then s. That is, if s, t have corresponding permutations σ and τ, the permutation corresponding to st is $\sigma \circ \tau$.

To find the order of D_{2n}, we first observe, vertex 1 can go to any vertex $i, 1 \leq i \leq n$. Next, as 2 must remain adjacent to 1 even after applying the symmetry, it can go to either $i + 1$ or $i - 1$. As we have fixed the position of two of the vertices and the polygon is rigid, we have fixed the entire permutation. We have $n \times 2 = 2n$ possible permutations and so, the order of D_{2n} is $2n$.

This group is called the *dihedral group of order* $2n$.
These $2n$ symmetries are the n rotations by $2\pi i/n$ radians about the center for $i = 1, 2, \dots, n$ and the n reflections about the n lines of symmetry.

Let r be the rotation symmetry that rotates the n-gon by $2\pi i/n$ radians and let s be the reflection symmetry that reflects the n-gon about the axis passing through vertex 1 and the origin.

Exercise 1.9. Prove the following.

1. $1, r, r^2, \dots, r^{n-1}$ are all distinct and $r^n = 1$, so $|r| = n$.
2. $|s| = 2$.
3. $s \neq r^i$ for any i.
4. $sr^i \neq sr^j$ for all $0 \leq i, j \leq n-1, i \neq j$ so
$$D_{2n} = \{1, r, r^2, \dots, r^{n-1}, s, sr, \dots, sr^{n-1}\}.$$
5. $rs = sr^{-1}$.
6. $r^i s = sr^{-i}$.

After doing the above exercise, we observe that all the elements of D_{2n} have a unique representation of the form $s^k r^i$ where $k = 0$ or 1 and $0 \leq i \leq n - 1$.

With the above expression of D_{2n} purely in terms of r and s as motivation, we introduce a new concept which can help in the expression of groups in a compact way.

Definition 1.7. We say that a subset S of a group G is a *set of generators* of G if every element in G can be written as a product of elements in S and their inverses. We indicate this by $G = \langle S \rangle$.

For example, $\mathbb{Z} = \langle \{1\} \rangle$.
Any equations in G that the generators satisfy are called *relations* in G. So in D_{2n}, we have the relations $r^n = 1, s^2 = 1$ and $rs = sr^{-1}$. It turns out that any relation in G can be deduced from these three relations. In general, if some group G is generated by a set S and there exist relations $R_1, R_2, \dots, R_m$ such that any relation in G can be deduced from these relations, we shall call the generators and the relations together a *presentation* of G. We write
$$G = \langle S \mid R_1, R_2, \dots, R_m \rangle.$$

For example,

$$D_{2n} = \langle \{r, s\} \mid r^n = 1, s^2 = 1, rs = sr^{-1} \rangle.$$

Very often, given a presentation there is some non-obvious relation that can be deduced from the given relations.
There is in fact an (as of the time of writing, unsolved) problem called the *word problem* in groups, which asks for a way to determine whether two "words" (products of elements of the group and their inverses) are equal given a set of relations.

Exercise 1.10. Let

$$X_{2n} = \langle \{x, y\} \mid x^n = y^2 = 1, xy = yx^2 \rangle.$$

Show that if $n = 3k$, X_{2n} has order 6. (Note the similarity between X_{2n} and D_6 in this case.
Also show that if $(3, n) = 1$, then $x = 1$.

1.3 Symmetric groups

Let Ω be any nonempty set and S_Ω the set of all bijections from Ω to Ω (that is, all permutations). Make S_Ω a group under function composition. (Function composition is associative, the identity is the identity mapping on Ω and any bijection has an inverse)
In the case where $\Omega = \{1, 2, \ldots, n\}$, we denote S_Ω by S_n and call it the *symmetric group of order n*.
It is a simple combinatorial exercise to show that S_n has exactly $n!$ elements. We now describe a notation to write the elements of S_n, called the *cycle decomposition* of any permutation. A *cycle* is a string of integers that cyclically permutes the elements of this string (leaving all other integers fixed). So the cycle $(a_1\, a_2\, a_3\, \cdots\, a_k)$ sends a_1 to a_2, a_2 to a_3, …, a_{k-1} to a_k and a_k to a_1. In general, for any element of S_n can be rearranged and written as k (disjoint) cycles as

$$\sigma = (a_1\ a_2\ \cdots\ a_{m_1})(a_{m_1+1}\ a_{m_1+2}\ \cdots\ a_{m_2})\cdots(a_{m_{k-1}+1}\ a_{m_{k-1}+2}\ \cdots\ a_{m_k})$$

This notation is very easy to read as to determine what an element i is sent to, we just need to find the element written after i in the cycle decomposition.
Any permutation σ can also be easily written as its cycle decomposition using the following algorithm.

1. To start a new cycle, pick the smallest number in $\{1, 2, \ldots, n\}$ that has not appeared in a previous cycle. Call it a. Begin the new cycle $(a$.

2. Let $\sigma(a) = b$. If $b = a$, close with a parenthesis and return to step 1. If $b \neq a$, write b next to a so the cycle becomes $(ab$.

3. Let $\sigma(b) = c$. If $c = a$, close with a parenthesis and return to step 1. If $c \neq a$, write c next to b and repeat this step using c as b until the cycle closes.

Naturally this process gives the correct cycle decomposition. The *length* of a cycle is the number of integers which appear in it. A cycle of length l is called an l-cycle. We further adopt the convention that 1-cycles are not written. (So if some i does not appear in the cycle decomposition, it is understood that the permutation fixes i) The identity permutation is written as 1.
So the final step in the algorithm is to remove all 1-cycles.

Note that

$$(1\,3) \circ (1\,2) = (1\,2\,3) \text{ and } (1\,2) \circ (1\,3) = (1\,3\,2).$$

This shows that S_n is a non-abelian group for all $n \geq 3$.
Further, since disjoint cycles permute elements in disjoint sets, disjoint cycles commute.

Exercise 1.11. Let $\sigma = (1\,2\,\cdots\,m)$. Show that σ^i is also an m-cycle if and only if $(m, i) = 1$.

Exercise 1.12. Show that the order of an l-cycle in S_n is l. Deduce that the order of any element in S_n is the least common multiple of the lengths of the cycles in its cycle decomposition.

Exercise 1.13. Let p be a prime. Show that an element of S_n is of order p if and only if its cycle decomposition is a product of commuting p-cycles.

1.4 Matrix Groups

For the sake of understanding matrix groups, we define a field as follows.
A field is a set F together with two binary operations $+$ and $\cdot$ such that $(F, +)$ is an abelian group (call its identity 0) and $(F - \{0\}, \cdot)$ is an abelian group. Further,

$$a \cdot (b + c) = a \cdot b + a \cdot c \text{ for all } a, b, c \in F.$$

For each $n \in \mathbb{Z}^+$, we define $GL_n(F)$ to be the set of all $n \times n$ matrices whose elements are elements of F and whose determinant is nonzero. $GL_n(F)$ is a group under matrix multiplication, and is called the *general linear group of order n*.
We have the following results (which we shall not prove in these notes).

1. if F is a finite field, then $|F| = p^m$ for some prime p and integer m.
2. if $|F| = q < \infty$, then $|GL_n(F)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1})$.

1.5 Homomorphisms and Isomorphisms

We define homomorphisms and isomorphisms here, but shall discuss them much more in detail later on.

Definition 1.8. Let $(G, \star)$ and $(H, \diamond)$ be two groups. A map $\varphi : G \to H$ such that

$$\varphi(x \star y) = \varphi(x) \diamond \varphi(y) \text{ for all } x, y \in G$$

is called a *homomorphism.*

The above condition is often compactly written as

$$\varphi(xy) = \varphi(x)\varphi(y).$$

Definition 1.9. Let G, H be two groups and $\varphi : G \to H$ be a homomorphism. The *kernel* of φ is defined as follows.

$$\ker(\varphi) = \{g \in G \mid \varphi(g) = 1_H\}$$

where 1_H is the identity element of H.

Definition 1.10. Let G, H be two groups. A map $\varphi : G \to H$ is called an *isomorphism* and we say G and H are isomorphic if φ is a homomorphism and φ is a bijection. If G and H are isomorphic, we write $G \cong H$.

Intuitively, two groups being isomorphic mean that they have the same structure.

Exercise 1.14. Show that the relation $\cong$ is an equivalence relation.

Example. The map $f : \mathbb{R} \to \mathbb{R}^+$ given by $f(x) = e^x$ for all $x \in \mathbb{R}$ is an isomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}^+, \times)$.

Exercise 1.15. Let Ω and Δ be two finite sets. Show that $S_\Omega \cong S_\Delta$ if and only if $|\Omega| = |\Delta|$.

Isomorphisms are extremely useful in the study of abstract structures such as groups because if we want to study some group, it will do equally well to study a group that is isomorphic to this one.

Exercise 1.16. Let G and H be two groups and $\varphi : G \to H$ be an isomorphism. Then prove that

1. if G and H are finite, $|G| = |H|$.
2. G is abelian if and only if H is abelian.
3. for all $x \in G$, $|x| = |\varphi(x)|$.

We can deduce from the third part of the above exercise that $(\mathbb{R}, +)$ is not isomorphic to $(\mathbb{R}, \times)$ as -1 is of order 2 in $(\mathbb{R}, \times)$ but there is no element of order 2 in $(\mathbb{R}, +)$.

Exercise 1.17. Prove that $(\mathbb{R} - \{0\}, \times)$ is not isomorphic to $(\mathbb{C} - \{0\}, \times)$.

Exercise 1.18. Prove that the additive groups $\mathbb{Z}$ and $\mathbb{Q}$ are not isomorphic.

Exercise 1.19. Let G, H be groups and $\varphi : G \to H$ be a homomorphism. Prove that the image of G under φ is a subgroup of H.

1.6 Group Actions

We define group actions here, but shall discuss them much more in detail later on.

Definition 1.11. A group action of a group G on a set A is a map from $G \times A$ to A (written as $g \cdot a$ for all $g \in G, a \in A$) such that

1. $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ for all $g_1, g_2 \in G, a \in A$.
2. $1 \cdot a = a$ for all $a \in A$.

We say that G is a group acting on the set A in the above definition.
More precisely, this is called a *left* group action. We have a similar notion of a *right* group action.

Theorem 1.4. For some fixed $g \in G$, consider the map $\sigma_g : A \to A$ given by $\sigma_g(a) = g \cdot a$. Then σ_g is a permutation of A. Further, the map $G \to S_A$ given by $g \mapsto \sigma_g$ is a homomorphism.

Proof. Consider $\sigma_{g^{-1}} : A \to A$. We shall show that $\sigma_{g^{-1}}$ is an inverse of σ_g. To see this, note that

$$\sigma_{g^{-1}} \circ \sigma_g(a) = g^{-1} \cdot (g \cdot a) = (g^{-1} g) \cdot a = 1 \cdot a = a \text{ for all } g \in G$$

so $\sigma_{g^{-1}} \circ \sigma_g$ is the identity map on A. Similarly, $\sigma_g \circ \sigma_g^{-1}$ is also the identity map on A. As σ_g has a two-sided inverse, it is a bijection and thus a permutation of A.
To see that the given map is a homomorphism, note that

$$\sigma_{g_1} \circ \sigma_{g_2}(a) = g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a = \sigma_{g_1 g_2}(a) \text{ for all } g_1, g_2 \in G, a \in A.$$

and $1 \cdot a = a$ for all $a \in A$. ■

Definition 1.12. Let a group G act on a set A. We define the kernel of the group action as

$$\{g \in G \mid g \cdot a = a \text{ for all } a \in A\}$$

Note that any group acts on itself by the group operation itself. This action is called the *left regular action* of G on itself.
If a group G acts on a set A and distinct elements of G induce distinct permutations, the action is said to be *faithful*.

§2 Subgroups

2.1 Definitions and Basics

Although we have defined subgroups in section 1, we repeat the definition here.

Definition 2.1. Let G be a group. A subset H of G is a subgroup of G if H is nonempty and it is closed under products and inverses. That is, $x, y \in H$ implies $x^{-1} \in H$ and $xy \in H$. If H is a subgroup of G, we write $H \leq G$.

If $H \leq G$ and $H \neq G$, we write $H < G$.

Example. $\mathbb{Z} \leq \mathbb{Q}$ and $\mathbb{Q} \leq \mathbb{R}$ under the operation of addition.
If $G = D_{2n}$, $H = \{1, r, r^2, \ldots, r^{n-1}\}$ is a subgroup of G.

Note that the relation $\leq$ is transitive. That is, if $K \leq H$ and $H \leq G$, then $K \leq G$.

Theorem 2.1 (Subgroup Criterion)**.** A subset H of a group G is a subgroup if and only if

1. $H \neq \emptyset$.
2. for all $x, y \in H$, $xy^{-1} \in H$.

Further, if H is finite, then it suffices to check that H is nonempty and is closed under multiplication.

Proof. If $H \leq G$, the two given statements clearly hold as H contains the identity of G and is closed under inverses and multiplication.
To prove the converse, let x be any element of H (which exists as $H \neq \emptyset$). We have $xx^{-1} \in H \implies 1 \in H$. As H contains 1, for any element h of H, H contains $1h^{-1} = h^{-1}$, that is, it is closed under inverses. For any x and y in H, as $y^{-1} \in H$, we have that $x(y^{-1})^{-1} = xy \in H$, that is, H is closed under multiplication.
To prove the second part, we see that $x, x^2, x^3, \ldots \in H$ for any $x \in H$. Using 1.3, we see that x is of finite order n. Then $x^{-1} = x^{n-1} \in H$ so H is closed under inverses. ■

Exercise 2.1. Let G be a group and H, K be subgroups of G. Show that $H \cap K$ is also a subgroup of G.

Exercise 2.2. Let G be a group and H, K be subgroups of G. Show that $H \cup K$ is a subgroup if and only if $H \subseteq K$ or $K \subseteq H$.

Exercise 2.3. Let G be a group of order $n > 2$. Show that G cannot have a subgroup H of order $n - 1$.

Exercise 2.4. Let G be a group. Let $H = \{g \in G \mid |g| < \infty\}$. Show that $H \leq G$ if G is abelian. In this case, H is called the *torsion subgroup* of G. Give an example where G is non-abelian and H is not a subgroup of G.

Exercise 2.5. Let H be a subgroup of $\mathbb{Q}$ under addition with the property that $\frac{1}{x} \in H$ for every nonzero $x \in H$. Show that $H = \{0\}$ or $\mathbb{Q}$.

2.2 Centralizers, Normalizers, Stabilizers and Kernels

We now introduce some important subgroups.

Definition 2.2. Let G be a group and A be any nonempty subset of A. Define

$$C_G(A) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}.$$

This subset is called the *centralizer* of A in G.

Since $gag^{-1} = g$ if and only if $ga = ag$, $C_G(A)$ is the set of all elements that commute with every element of A.
Now observe that $C_G(A)$ is a subgroup of G as first of all, $1 \in C_G(A)$ so $C_G(A) \neq \emptyset$, and second of all, if $x, y \in C_G(A)$, we have $xax^{-1} = a$ and $yay^{-1} = a$, that is, $y^{-1}ay = a$ for all $a \in A$. We then have $a = xax^{-1} = x(y^{-1}ay)x^{-1} = (xy^{-1})a(xy^{-1})^{-1}$ so $xy^{-1} \in C_G(A)$. Thus, $C_G(A) \leq G$.

Definition 2.3. Let G be a group. Define

$$Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}.$$

This subset is called the *center* of G.

$Z(G)$ is the set of all elements that commute with every element of G.
As $Z(G) = C_G(G)$, we have $Z(G) \leq G$.

Definition 2.4. Let G be a group and A be a subset of G. Define $gAg^{-1} = \{gag^{-1} \mid a \in A\}$. Define

$$N_G(A) = \{g \in G \mid gAg^{-1} = A\}.$$

This set is called the *normalizer* of A in G.

The proof that $N_G(A) \leq G$ is similar to that we used to prove that $C_G(A) \leq G$.
Note that $C_G(A) \leq N_G(A)$.

For A, let
$\bar{A} = \{a_1{}^{\epsilon_1} a_2{}^{\epsilon_2} \cdots a_n{}^{\epsilon_n} \mid n \in \mathbb{Z}, n \geq 0 \text{ and } a_i \in A, \epsilon_i = \pm 1 \text{ for each } i\}$
where $\bar{A} = 1$ if $A = \emptyset$.
Then, $\bar{A} = \langle A \rangle$, where $\langle A \rangle$ represents the subgroup of G generated by A (the minimal subgroup of G that contains A). Note that the a_i's can be identical.
Lagrange's Theorem:
If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$ and the number of left cosets of H in G equals $\frac{|G|}{|H|}$.
Proof outline: The set of left cosets of H in G partition G. By definition of a left coset, the map $H \mapsto gH$ defined by $h \mapsto gh$ is a surjection from H to the left coset gH. The left cancellation law implies this map is injective since $gh_1 = gh_2 \implies h_1 = h_2$. This proves that H and gH have the same order, $|gH| = |H| = n$. Since G is partitioned into k disjoint subsets each of which has cardinality n, $|G| = kn$. Thus, $k = \frac{|G|}{|H|}$.
Note: The converse of Lagrange's Theorem (If $k \in \mathbb{Z}^+$ such that $k \mid |G|$, then there exists a subgroup of G of order k) holds if G is a finite abelian group.
To define a homomorphism from a group G to G', it is not enough to define the value of φ at the generators of G, we must also ensure that the relations are satisfied. That is, if we have a relation $r = 1$, where r is some combination of generators, then we must also have that $\varphi(r) = 1$.
Let N be a subgroup of G. The following are equivalent:

- i $N \trianglelefteq G$ (N is a normal subgroup of G)
- ii $N_G(N) = G$ ($N_G(N)$ is the normalizer in G of N)
- iii $gN = Ng$ for all $g \in G$
- iv the operation of left cosets of N in G described by $uN \cdot vN = (uv)N$ (which is well-defined if and only if $gng^{-1} \in N$ for all $g \in G$ and all $n \in N$) makes the set of left cosets into a group.
- v $gNg^{-1} \subseteq N$ for all $g \in G$ (this happens if and only if $gNg^{-1} = N$)
- vi N is the kernel of some homomorphism.

If $G = \langle S \rangle$, then if N is a normal subgroup of G, $\frac{G}{N} = \langle \frac{S}{N} \rangle$.
$A \trianglelefteq B$ and $B \trianglelefteq C$ does *not* imply that $A \trianglelefteq C$. For example, $\langle s \rangle \trianglelefteq \langle s, r^2 \rangle \trianglelefteq D_8$ but $\langle s \rangle$ is not normal in D_8.
In abelian groups, every subgroup is normal.
If $\frac{G}{Z(G)}$ is cyclic, G is abelian.
Cauchy's Theorem: If G is a finite group and p is a prime dividing $|G|$, then G has an element of order p. (Page 96 Q9, Dummit and Foote)
If H and K are subgroups of a group, HK is a subgroup if and only if $HK = KH$.
If H and K are subgroups of G and $H \leq N_G(K)$, then HK is a subgroup of G. In particular, if $K \trianglelefteq G$ then $HK \leq G$ for any $H \leq G$.
Let $H \leq G$. The set of left cosets of H in G is in bijection with the set of right cosets of H in G ($x \mapsto x^{-1}$ maps each left coset to a right coset).

1. *The First Isomorphism Theorem*: If $\varphi : G \to H$ is a homomorphism of groups, then $\ker\varphi \trianglelefteq G$ and $G/\ker\varphi \cong \varphi(G)$.

   Corollary: $|G : \ker\varphi| = |\varphi(G)|$. φ is injective if and only if $\ker\varphi = 1$.

2. *The Second or Diamond Isomorphism Theorem*: Let G be a group, let H and K be subgroups of G and assume $H \leq N_G(K)$. Then $HK \leq G$, $K \trianglelefteq HK$, $H \cap K \trianglelefteq H$ and $HK/K \cong H/H \cap K$. This theorem's name can be understood from Fig. 1.

3. *The Third Isomorphism Theorem*: Let G be a group and H and K be normal subgroups of G with $H \leq K$. Then $K/H \trianglelefteq G/H$ and $(G/H)/(K/H) \cong G/K$.

   The Fourth or Lattice Isomorphism Theorem: Let G be a group and let N be a normal subgroup of G. Then there is a bijection from the set of subgroups A of G which contain N onto the set of subgroups

$$
\begin{tikzcd}
& G \arrow[d] & \\
& HK \arrow[dl] \arrow[dr, "\trianglelefteq"] & \\
H \arrow[dr, "\trianglelefteq"'] & & K \arrow[dl] \\
& H \cap K \arrow[d] & \\
& \{1\} &
\end{tikzcd}
$$

Figure 1: Diamond Isomorphism Theorem

$\overline{A} = A/N$ of G/N. In particular, every subgroup of $\overline{G}$ is of the form A/N for some subgroup A of G containing N (namely, its preimage in G under the natural projection homomorphism from G to G/N). This bijection has the following properties: for all $A, B \leq G$ with $N \leq A$ and $N \leq B$,

i $A \leq B$ if and only if $\overline{A} \leq \overline{B}$,

ii if $A \leq B$, then $|B : A| = |\overline{B} : \overline{A}|$,

iii $\overline{\langle A, B\rangle} = \langle \overline{A}, \overline{B}\rangle$,

iv $\overline{A \cap B} = \overline{A} \cap \overline{B}$

v $A \trianglelefteq G$ if and only if $\overline{A} \trianglelefteq \overline{G}$

If H is a normal subgroup of G of prime index p then for all $K \leq G$, either

i $K \leq H$ or

ii $G = HK$ and $|K : H \cap K| = p$.

In a group G, a sequence of subgroups

$$1 = N_0 \leq N_1 \leq N_2 \leq \cdots \leq N_{k-1} \leq N_k = G$$

is called a *composition series* if $N_i \trianglelefteq N_{i+1}$ and N_{i+1}/N_i is a simple group, $0 \leq i \leq k-1$. If the above sequence is a composition series, the quotient groups N_{i+1}/N_i are called *composition factors* of G.
Jordan-Hölder Theorem: Let G be a finite group with $G \neq 1$. Then

i G has a composition series.

ii The composition factors in a composition series are unique. Namely, if $1 = N_0 \leq N_1 \leq N_2 \leq \cdots \leq N_{r-1} \leq N_r = G$ and $1 = M_0 \leq M_1 \leq M_2 \leq \cdots \leq M_{s-1} \leq M_s = G$, then $r = s$ and there is some permutation π of $\{1, 2, \cdots, r\}$ such that $M_{\pi(i)}/M_{\pi(i)-1} \cong N_i/N_{i-1}$. Note that the series itself need not be unique, but the composition factors are unique.

Feit-Thompson: If G is a simple group of odd order, then $G \cong Z_p$ for some prime p.
A group G is *solvable* if there is a composition series of G such that every composition factor of G is abelian.
Let G be a finite group. The following are equivalent:

i G is solvable.

ii G has a composition series such that every composition factor is cyclic.

iii All composition factors of G are of prime order.

iv G has a chain of subgroups: $1 = N_0 \leq N_1 \leq N_2 \leq \cdots \leq N_{t-1} \leq N_t = G$ such that each N_i is a normal subgroup of G and N_{i+1}/N_i is abelian, $0 \leq i \leq t-1$.

v For every divisor n of $|G|$ such that $\left(n, \frac{|G|}{n}\right) = 1$, G has a subgroup of order n.

vi There exists a normal subgroup N of G such that both N and G/N are solvable.

The permutation σ is odd if and only if the number of cycles of even length in its cycle decomposition is odd.
A_n, the alternating group of degree n, is a non-abelian simple group for all $n \geq 5$.
An action of G on A may also be viewed as a faithful action of $G/\ker\varphi$ on A.
Let G be a group acting on a nonempty set A. For each $g \in G$, the map $\sigma_g : A \to A$ defined by $\sigma_g(a) = g \cdot a$ is a permutation of A. There is a homomorphism associated with this action of G on A given as $\varphi : G \to S_A$ defined by $\varphi(g) = \sigma_g$ called the *permutation representation* associated with this action. The kernel of this action is the same as the kernel of φ.

Definition 2.5. If G is a group, a *permutation representation* of G is any homomorphism of G into the symmetric group S_A for some nonempty set A. We shall say that the given action *affords* or *induces* the associated permutation representation of G.

Let G be a group acting on the nonempty set A. The relation on A defined by $a \sim b$ if and only if $a = g \cdot b$ for some $g \in G$ is an equivalence relation. For each $a \in A$, the number of elements in the equivalence class containing a is $|G : G_a|$, where G_a is the stabilizer of a.
Let G be a group, let H be a subgroup of G and let G act by left multiplication on the set A of left cosets of H in G. Let π_H be the associated permutation representation afforded by this action. Then

i G acts transitively on A.

ii the stabilizer in G of the point $1H \in A$ is the subgroup H.

iii the kernel of the action (i.e., the kernel of π_H) is $\cap_{x \in G} xHx^{-1}$ and $\ker\pi_H$ is the largest normal subgroup of G contained in H.

Cayley's Theorem: If G is a group of order n, then G is isomorphic to a subgroup of S_n.
Proof: Just put $H = \{1\}$ in the previous point to get a homomorphism from G to S_G. Since the kernel is contained in $H = \{1\}$, G is isomorphic to its image in S_G.
If G is a finite group and p is the smallest prime dividing $|G|$, any subgroup of index p is normal. Note that, however, a group need not necessarily have a subgroup of index p.

Proof. We have $H \leq G$ and $|G : H| = p$. Let π_H be the permutation representation given by multiplication on the set of left cosets of H in G. Let $K = \ker\pi_H$ and $|H : K| = k$. Then $|G : K| = |G : H||H : K|$ As there are p left cosets of H in G, we have that G/K is isomorphic to a subgroup of S_p (the image of G under π_H). This implies $pk \mid p!$ and $k \mid (p-1)!$. The minimality of p implies that $|H : K| = 1$ and $H = K \trianglelefteq G$. ■

Two subsets S and T of G are said to be conjugate in G if there exists $g \in G$ such that $T = gSg^{-1}$.
The number of conjugates of a subset S of G is the index of the normalizer of S, $|G : N_G(S)|$. It follows that the number of conjugates of an element s of G is the index of the centralizer of s, $|G : C_G(s)|$. (as $N_G(\{s\}) = C_G(s)$)
The Class Equation: Let G be a finite group and let $g_1, g_2, \cdots g_r$ be representatives of the distinct conjugacy classes of G not contained in the center $Z(G)$ of G. Then

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|$$

Note that this is useless for abelian groups.
If p is a prime and P is a group of prime power order p^α for some integer $\alpha \geq 1$, then P has a nontrivial center: $Z(P) \neq \{1\}$.

Corollary 2.2. If $|P| = p^2$ for some prime p, then P is abelian. More precisely, P is isomorphic to either Z_{p^2} or $Z_p \times Z_p$.

Let τ, σ be members of the symmetric group S_n. Then, $\tau\sigma\tau^{-1}$ is obtained from σ by replacing each entry i in the cycle decomposition of σ with $\tau(i)$.
If $\sigma \in S_n$ is the product of disjoint cycles of lengths $n_1, n_2, \cdots, n_r$ with $n_1 \leq n_2 \leq \cdots \leq n_r$ (including its 1-cycles) then the integers $n_1, n_2, \cdots, n_r$ are called the cycle type of σ.
Two elements of S_n are conjugate if and only if they have the same cycle type. The number of conjugacy classes of S_n equals the number of partitions of n.
If σ is an m-cycle in S_n, then $C_{S_n}(\sigma) = \{\sigma^i\tau \mid 0 \leq i \leq m-1, \tau \in S_{n-m}\}$ where S_{n-m} denotes the subgroup of S_n which fixes the integers appearing in the m-cycle σ. $|C_{S_n}(\sigma)| = m \cdot (n-m)!$.
If $H \trianglelefteq G$, then for every conjugacy class $\mathcal{K}$ of G, either $\mathcal{K} \subseteq H$ or $\mathcal{K} \cap H = \emptyset$.
If $Z(G)$ is of index n, any conjugacy class of G is of order atmost n.
Assume $H \trianglelefteq G$, $\mathcal{K}$ is a conjugacy class of G contained in H and $x \in \mathcal{K}$. Then, $\mathcal{K}$ is a union of k conjugacy classes of equal size in H, where $k = |G : HC_G(x)|$.
Let $H \trianglelefteq G$. Then G acts by conjugation on H as automorphisms of H. More specifically, the action of G on H by conjugation is defined for each $g \in G$ by $h \mapsto ghg^{-1}$ for each $h \in H$. For each $g \in G$, conjugation by g is an automorphism of H. The permutation representation afforded by this action is a homomorphism of G into $\mathrm{Aut}(H)$ with kernel $C_G(H)$. In particular, $G/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$.

Corollary 2.3. For any $H \leq G$, $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$. In particular, putting $H = G$, $G/Z(G)$ is isomorphic to a subgroup of $\mathrm{Aut}(G)$.

Let G be a group and $g \in G$. Conjugation by g is called an *inner automorphism* of G and the subgroup of $\mathrm{Aut}(G)$ consisting of all inner automorphisms of G is called $\mathrm{Inn}(G)$. We have that $\mathrm{Inn}(G) \cong G/Z(G)$ and $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$ ($\mathrm{Aut}(G)/\mathrm{Inn}(G)$ is called the outer isomorphism group of G)
$\mathrm{Aut}(Z_n) \cong (\mathbb{Z}/n\mathbb{Z})^\times$

Definition 2.6. A subgroup H of G is called *characteristic* in G, denoted by $H \operatorname{char} G$, if every automorphism of G maps H to itself, i.e., $\sigma(H) = H$ for all $\sigma \in \mathrm{Aut}(G)$.

Then,

i characteristic subgroups are normal,

ii if H is the unique subgroup of G of a given order, then $H \operatorname{char} G$,

iii if $K \operatorname{char} H$ and $H \trianglelefteq G$, then $K \trianglelefteq G$ and

iv if $K \operatorname{char} H$ and $H \operatorname{char} G$, then $K \operatorname{char} G$.

Let G be a group of order pq, where p and q are primes (not necessarily distinct) with $p \leq q$. If $p \nmid q-1$, G is cyclic. The proof that G is abelian is as follows.

Proof. If $Z(G) \neq 1$, then Lagrange's Theorem forces $G/Z(G)$ to be cyclic and hence G to be abelian. Hence we may assume $Z(G) = 1$.
If every nonidentity element of G has order p, then the centralizer of every nonidentity element has index q, so the class equation for G reads $pq = 1 + kq$. This is impossible since q divides pq and kq but not 1. Thus G contains an element x of order q.
Let $H = \langle x \rangle$. Since H has index p and p is the smallest prime that divides $|G|$, H is normal in G. Since $Z(G) = 1$, we must have $C_G(H) = H$. Thus $G/H = N_G(H)/C_G(H)$ is a group of order p isomorphic to a subgroup of $\mathrm{Aut}(H)$. But $\mathrm{Aut}(H)$ has order $\varphi(q) = q - 1$ which by Lagrange's Theorem would imply $p \mid q - 1$, contrary to the assumption. ■

It can further be checked that every such group is cyclic.
Descriptions of isomorphism types of some automorphism groups:

- The automorphism group of the cyclic group of order p^n is cyclic of order $p^{n-1}(p-1)$.
- For all $n \geq 3$ the automorphism type of the cyclic group of order 2^n is isomorphic to $Z_2 \times Z_{2^{n-2}}$, and in particular is not cyclic but has a cyclic subgroup of index 2.
- Let p be a prime and let V be an abelian group (written additively) with the property that $pv = 0$ for all $v \in V$. If $|V| = p^n$, then V is an n-dimensional vector space over the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. The automorphisms of V are precisely the nonsingular linear transformations from V to itself, that is,

  $$\text{Aut}(V) \cong GL(V) \cong GL_n(\mathbb{F}_p).$$

  In particular, the order of $\text{Aut}(V)$ is $(p^n-1)(p^n-p)(p^n-p^2)\cdots(p^n-p^{n-1})$.
- For all $n \neq 6$ we have $\text{Aut}(S_n) = \text{Inn}(S_n) \cong S_n$. For $n = 6$, we have $|\text{Aut}(S_6) : \text{Inn}(S_6)| = 2$.
- $\text{Aut}(D_8) \cong D_8$ and $\text{Aut}(Q_8) \cong S_4$.

Definition 2.7. Let G be a group and p be a prime.

- A group of order p^α for some $\alpha \geq 1$ is called a *p-group*.
- If G is a group of order $p^\alpha m$, where $p \nmid m$, then a subgroup of order p^α is called a *Sylow p-subgroup* of G.
- The set of Sylow p-subgroups will be denote by $Syl_p(G)$ and the number of Sylow p-subgroups of G will be denoted by $n_p(G)$ (or just n_p).

Sylow's Theorem: Let G be a group of order $p^\alpha m$ where p is a prime that does not divide m.

1. Sylow p-subgroups of G exist, i.e., $Syl_p(G) \neq \emptyset$.
2. If P is a Sylow p-subgroup of G and Q is any p-subgroup of G, then there exists $g \in G$ such that $Q \leq gPg^{-1}$, i.e., Q is contained in some conjugate of P. In particular, any two Sylow p-subgroups of G are conjugate in G.
3. The number of Sylow p-subgroups of G is of the form $1 + kp$, i.e.,

   $$n_p \equiv 1 \pmod{p}.$$

   Further, n_p is the index in G of the normalizer $N_G(P)$ for any Sylow p-subgroup P, hence

   $$n_p \mid m.$$

Any two Sylow p-subgroups of a group (for the same prime p) are isomorphic.
Let $P \in Syl_p(G)$. If Q is any p-subgroup of G, then $Q \cap N_G(P) = Q \cap P$.
Let P be a Sylow p-subgroup of G. Then the following are equivalent:

1. P is the unique Sylow p-subgroup of G, i.e., $n_p = 1$
2. $P \trianglelefteq G$
3. $P \operatorname{char} G$
4. All subgroups generated by elements of p-power order are p-groups, i.e., if X is any subset of G such that $|x|$ is a power of p for all $x \in X$, then $\langle X \rangle$ is a p-group.