MTH204 ABSTRACT ALGEBRA

INSTRUCTOR: SANTOSH NADIMPALLI

1. Lecture: Groups as symmetries

In mathematics we study many structures and often the symmetries of these structures determine the underlying geometry. In this lecture we will study the symmetries of some regular polyhedron in Euclidean spaces. For any X in $\mathbb{R}^n$, let $W(X)$ be the set

$$\{T \in O(n) : T(x) \in x, \text{for all } x \in X\}.$$

If the span of X is equal to $\mathbb{R}^n$, then clearly $W(X)$ is a finite set. From a structural point of view, the set $W(X)$ has the following properties: the identity element belongs to $W(X)$, given any two element T_1 and T_2, the element T_1T_2 belongs to $W(X)$, and finally $T_1(T_2T_3) = (T_1T_2)T_3$, for any three linear operators T_1, T_2, T_3. We will later call any set G with a binary operator which satisfies these three conditions as a group. In this lecture, we will just concentrate on the structure of $W(X)$, for some interesting $W(X)$.

Let X be a regular n-gon in $\mathbb{R}^2$. Let σ be an element of $W(X)$ with $\det(\sigma) = -1$. Let τ be any reflection of the plane which preserves X, and such an element obviously exists. Then, the element $\tau\sigma$ has determinant 1, and thus a rotation of the plane. All rotations of a plane which preserve X are generated by the rotation linear transformation $\theta : \mathbb{R}^2 \to \mathbb{R}^2$ with angle of rotation $2\pi/n$. Thus, the set $W(X)$ is equal to

$$\{\tau^i\theta^j : i \in \{0, 1\}, j \in \{0, \dots, n-1\}\}.$$

Note that

$$\tau\theta = \theta^{-1}\tau. \tag{1.1}$$

The above identity completely determines what happens when you multiply $\tau^i\theta^j$ with $\tau^l\theta^l$. Now, given a set of symbols

$$\{1, \theta, \theta^2, \dots, \theta^{n-1}, \tau, \tau\theta, \dots, \tau\theta^{n-1}\}$$

there exists a unique associative multiplication on the above set which satisfies the condition (1.1). Thus the above list of symbols is the abstraction of the set of symmetries of a regular n-gon (see figure 1).

Let us now consider a tetrahedron $X \in \mathbb{R}^n$ with its centre of mass at the origin.

How do we describe the set $W(X)$?

Date: January 24, 2022.

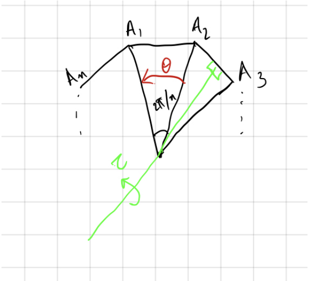

Figure 1. Generators

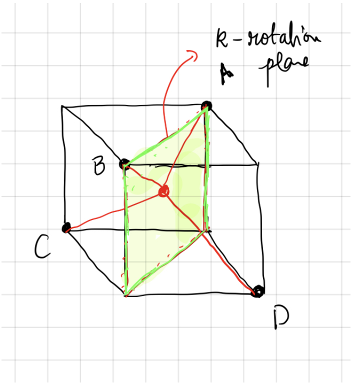

Figure 2. π-Rotation

Any element of $W(X)$ with determinat 1 must preserve a line called the axis of rotation. We denote by $R_{l,\theta}$, the rotation of the three dimensional euclidean space $\mathbb{R}^3$ with l as the axis of rotation–passing through the origin–and θ is the angle of rotation in $l^{\perp}$. If l is a line joining a vertex to the barycentre of the opposite face, then $R_{l,2\pi/3}$ belongs to $W(X)$. Let us fix such an axis l and let ι be the element $R_{l,2\pi/3}$. We may imagine a tetrahedron as vertices from two opposite faces of a cube. This provides with another rotation, say we denote it by κ (see figure 2).

This section is to be completed sometime soon.

2. Formal introduction to groups

2.1.

Definition 2.1. *A* **group** *is a pair $(G, .)$, where G is a set and "$.$" is a binary operation. which satisfies the following conditions*

1. *(Existence of identity) There exists an element $e \in G$ such that $e.g = g.e = 1$,*
2. *(Existence of inverse) For any $g \in G$, there exists an element g' such that $g.g' = g'.g = e$*
3. *(Associative law) For any g_1, g_2 and g_3 in G, we have $g_1.(g_2.g_3) = (g_1.g_2).g_3$.*

Note that an inverse of an element $g \in G$ is unique and is denoted by g^{-1} (It is worth proving this for yourself). The previous section provides a plethora of examples. However, let us recall a list of examples to work with. Notationally the "$.$" will be dropped in most circumstances.

1. The set of numbers with usual addition $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, any vector space V with its additive structure are examples of groups. These are examples of **abelian groups**. An abelian group in addition to the above axioms on sets satisfies
$$g_1.g_2 = g_2.g_1, \ \ g_1, g_2 \in G.$$
2. Let N be a positive integer and let $\mathbb{Z}/N\mathbb{Z}$ be the set $\{0, 1, 2, \dots, N-1\}$. For any $a, b \in \mathbb{Z}/N\mathbb{Z}$, we denote by $a.b$ the unique integer $c \in \mathbb{Z}/N\mathbb{Z}$ such that $N | a + b - c$. It is traditional practice to replace "$.$" notation for $+$ in this example to continue the $+$ operation in $\mathbb{Z}$.
3. If X is a regular n-gon, we denote by D_n the group $W(X)$, the group $W(X)$ is discussed in detail from the previous section.
4. Let $[n]$ be the set of integers $\{1, 2, \dots, n\}$. Let S_n be the set of bijections from $[n]$ to the set $[n]$. Note that S_n is a group for the group operation being the composition of functions.
5. The set of invertible linear transformations of a vector space V, denoted by $\mathrm{GL}(V)$, together with the composition of operators is an example of a group. If V is a finite dimensional example, we have several other related groups, like $\mathrm{SL}(V)$, the group of invertible linear transformations with determinant 1; if $B : V \times V \to k$ is a bilinear form then the set of orthogonal linear transformations, denoted by $O(V, B)$ is also a group under composition of linear transformations. In this example we

motivate the defintion of a **subgroup**. A subset H is a subgroup of a group G if $e \in H$ and for any two elements $h_1, h_2 \in H$, the element $h_1h_2 \in H$. Note that $\mathrm{SL}(V)$ and $O(V, B)$ are subgroups of $\mathrm{GL}(V)$. When k is a finite field, the groups $\mathrm{SL}(V)$, $\mathrm{O}(V, B)$ are interesting examples of finite groups.

A **group homomorphism** is a map $\phi : G_1 \to G_2$ such that $\phi(g_1g_2) = \phi(g_1)\phi(g_2)$, for all $g_1, g_2 \in G$ and $\phi(e_1) = e_2$, where e_1 and e_2 are identity elements of G_1 and G_2 respectively. Connected with any group homomorphism $\phi : G_1 \to G_2$, we may associate a subgroup of G_1, namely $\ker(\phi) = \{g \in G_1 : \phi(g) = e_2\}$, and a subgroup of G_2 being the image of the map ϕ. Clearly, ϕ is injective if and only if $\ker(\phi) = \{e_1\}$. If $\mathrm{img}(\phi) = G_2$, i.e., if ϕ is surjective, then ϕ^{-1} exists and can be easily verified to be a group homomorphism. Two groups G_1 and G_2 are said to be **isomorphic** if there exists two group homomorphisms $\phi_1 : G_1 \to G_2$ and $\phi_2 : G_2 \to G_1$ such that $\phi_1\phi_2 = \mathrm{id}$ and $\phi_2\phi_1 = \mathrm{id}$. If there exists a group homomorphism $\phi : G_1 \to G_2$, such that $\ker(\phi)$ is trivial and $\mathrm{img}(\phi) = G_2$, then G_1 and G_2 are isomorphic via the group homomorphisms ϕ and ϕ^{-1}.

2.2. The most important phenomena in group theory are understood from realising a group occurring as symmetries of some set. We now formally introduce the concept of group actions.

Definition 2.2. *Let G be a group and let X be a set. A group G acts on the set X if and only if for any $g \in G$, there exists a map $\rho_g : X \to X$ such that $\rho_e = \mathrm{id}_X$, and $\rho_{g_1g_2} = \rho_{g_1}\rho_{g_2}$, for all $g_1, g_2 \in G$.*

It follows immediately that the maps ρ_g is a bijection and giving the action of a group G on a set X is equivalent to saying that there is a group homomorphism $\rho : G \to \mathrm{Aut}(X)$, where $\mathrm{Aut}(X)$ is the group of bijection with the group structure being composition of maps. For simplicity we denote by $\rho_g(x)$ as gx. The action of a group G on a set X should be understood as a particular flow of points on a set X. Given a group action on a set X, we may define a relation on a set X by setting $x \sim y$ if there exists a $g \in G$ such that $\rho_g(x) = y$; the group axioms imply that the relation $\sim$ is an equivalence relation. Thus we get that

$$X = \coprod_{i \in I} \mathcal{O}_i,$$

here I is some indexing set and $\mathcal{O}_I$ is an equivalence class and also called as **orbit**. To indicate the geometric nature of the above concepts, we describe the following examples. If $|I| = 1$, then G is said to act **transitively** in other words for any two $x, y \in X$, if there exists a $g \in G$ such that $gx = y$. It is obvious that G acts transitively on any of the orbits.

If G acts transitively on any set X, then we may choose an element $x \in G$ and define a map

$$\phi : G \to X, g \mapsto g.x,\ \ g \in G.$$

Note that $G = \coprod_{y \in X} \phi^{-1}(y)$. Note that $\phi^{-1}(x)$ is a subgroup of G. Explicitly,

$$\phi^{-1}(x) = \{g \in G : g.x = x\}.$$

The set $\phi^{-1}(x)$ is called the **stabilizer** of x. For any other $y \in X$, choose a $g \in G$ such that $gx = y$. Such a g exists because G acts transitively on X. Now, for any $g' \in \phi^{-1}(y)$, we get that $gx = g'x$. Thus, we get that $g' \in gh$, where $h \in G_x$. If we denote the set $gh : h \in G_x$ by gG_x, then $\phi^{-1}(y) = gG_x$. Thus, there exists elements $g_y \in G$, for all $y \in X$ such that

$$G = \coprod_{y \in X} \phi^{-1}(y) = \coprod_{y \in Y} g_yG_x.$$

Moreover, $g_{y_1}G_x \cap g_{y_2}G_x$ is empty set. The above decomposition is the most fundamental tools in group theory and we shall demonstrate several important consequences.

2.2.1. The group G acts on itself in some interesting ways. We will first consider the following three actions: left multiplication, right multiplication and conjugation actions: for $g \in G$, we denote by $l_g : G \to G$, the map $l_g(h) = gh$ and $r_g : G \to G$, the map $r_g(h) = hg^{-1}$. Let $ad_g : G \to G$ be the map $ad_g(h) = ghg^{-1}$. Note that the associations $g \mapsto l_g$, $g \mapsto r_g$ and $g \mapsto ad_g$ are group actions.

There are some immediate consequences of these facts: Note that the map $G \mapsto \mathrm{Aut}(G)$, where $\mathrm{Aut}(G)$ is the set theoretic bijections of G, is an injective map. If G is a finite group, then G is isomorphic to a subgroup of the symmetry group S_n, where $n = |G|$. This n may not be optimal element. For example dihedral group embeds into S_{2k}. However, the size of S_{2k} is $2k!$, which is roughly e^{2k} and D_{2k} has size $2k$.

Consider a finite group G. The conjugation action of G on G is the association $g \mapsto ad_g$. Equivalence classes for this action are called conjugacy classes and are of the form $\{ghg^{-1} : g \in G\}$ for some $h \in G$; we denote by $\mathcal{O}_h$ the conjugacy class which contains the element h. We note that $|\mathcal{O}_h$ if and only if $hg = gh$, for all $g \in G$. The set of elements $h \in G$ such that $gh = hg$ forms a subgroup and is called the centre of G, to be denoted by $Z(G)$. The G stabilizer for this action is called the centraliser of h, denoted by $C_G(h)$;

$$C_G(h) = \{g \in G : gh = hg\}.$$

Hence the cardinality of G is equal to $|G|/|C_G(h)|$. Thus if we pick $h_i \in \mathcal{O}_i$, we get that

$$|G| = |Z(G)| + \sum_{|\mathcal{O}_i|>1} \frac{|G|}{|C_G(h_i)|}. \tag{2.1}$$

The above formula is sometimes called the **class equation**. If G is a finite group of cardinality p^n, for some prime number p, then we get that $p||Z(G)|$.

2.2.2. Let us consider a group G and a subgroup H of G. The group H acts on G via left multiplication. Note that any orbit for this action is of the form Hg, for some $g \in G$. There exists a family of $\{g_i : i \in I\}$ such that

$$|G| = \coprod_{g_i} Hg_i. \tag{2.2}$$

Being an equivalence classes, $Hg_1 \cap Hg_2$ is either empty or $Hg_1 = Hg_2$. Note that the map $g \mapsto gg_1^{-1}g_2$ induces a bijection between Hg_1 and Hg_2. If $|I| < \infty$, then H is said to have finite index in G. If G is a finite group and if H is a subgroup of G, then $|G| = |I||H|$. Thus, $|H|$ divides the cardinality of $|G|$. The set of cosets $\{Hg_i : i \in I\}$ is denoted by G/H. As an immediate application, any group of prime cardinality, i.e., $|G|$ is a prime number say p, is cyclic. Since, the group generated by any non-trivial element must be the whole group.

2.2.3. The group G acts on the set of cosets G/H, by right multiplication $\bar{r}_g(Hg_i) = Hg_j$, where $g_ig \in Hg_j$ (it is advised to check that this is a group action). The kernel of the homomorphism $\bar{r} : G \to \mathrm{Aut}(G/H)$ given by $g \mapsto \bar{r}_g$ is given by

$$\bigcap_{g \in G} gHg^{-1}.$$

If this subgroup is the trivial group, then $\bar{r}_g$ embeds G as a subgroup of much smaller symmetric group $S_{|G/H|}$.

2.3. In this section, we will discuss a certain group structure on the set of cosets G/H, when H satisfies some conditions. Let us consider two cosets Hg_1 and Hg_2 and say we get a product

$$Hg_1Hg_2 = Hg_1g_2.$$

However, we need to check that the above definition does not depend on the choice of the family $\{g_i : i \in I\}$. Assume that $Hg_1 = Hg_1'$ and $Hg_2 = Hg_2'$. Notice that

$$g_1 = h_1g_1', g_2 = h_2g_2'.$$

Hence we have,

$$g_1g_2 = h_1g_1'h_2g_2' = h_1g_1'h_2(g_1')^{-1}g_1'g_2'.$$

If $g_1'h_2(g_1')^{-1} \in H$, then we get that $Hg_1g_2 = Hg_1'g_2'$. Thus we make the following definition:

Definition 2.3. *A subgroup H of a group G is called normal if for any $g \in G$ and $h \in H$, the elements $ghg^{-1} \in H$.*

$$\begin{tikzcd}
G \arrow[r, "\phi"] \arrow[dr, "\pi"'] & H \\
& G/N \arrow[u, "\tilde{\phi}"']
\end{tikzcd}$$

Figure 3. First Isomorphism theorem

Thus, if H is a normal subgroup of G, then the set of cosets G/H becomes a group via the binary operation:

$$Hg_1.Hg_2 = Hg_1g_2.$$

Moreover, we have a homomorphism $\pi : G \to G/H$, given by $g \mapsto Hg$. Note that the kernel of the above homomorphism is equal to H.

Next we begin with arbitrary homomorphism $\phi : G \to G$. Note that the group $\ker(\phi)$ is a normal subgroup of G. *Hence, normal subgroups arise as kernels of group homomorphisms.* Let N be a normal subgroup of G which is contained in $\ker(\phi)$. Then we can construct $\tilde{\phi}$ such that the following map in figure 3 commutes: The map $\tilde{\phi}$ is given by setting $\tilde{\phi}(gN) = \phi(g)$. If $gN = g'N$, then $g^{-1}g' \in N$, and in particular $g^{-1}g' \in N$. Thus, we get that $\phi(g) = \phi(g')$ and the map $\tilde{\phi}$ is well defined. In particular if N is equal to $\ker(\phi)$ we get that $\tilde{\phi} : G/\ker(\phi) \to \mathrm{img}(\phi)$ is an isomorphism. It is an exercise to show that there is a one to one correspondence between subgroups of G which contain N and subgroups of G/N. The correspondence being

$$H \mapsto \pi^{-1}(H).$$

Let H and K be two subgroups of G such that H is a normal subgroup of G. Then the set $HK = \{hk : h \in H, k \in K\}$ is a subgroup of G. Moroever, we have

$$HK/H \simeq K/K \cap H.$$

The isomorphism being $kH \mapsto k(K \cap H)$.

2.4. Let G be a finite group and let $x \in G$ be any element such that $x \neq \mathrm{id}$. The least positive integer n such that $x^n = \mathrm{id}$ is called the **order** of x. If $x \neq e$ is an element of order n, then we get a natural isomorphism

$$\mathbb{Z}/n\mathbb{Z} \to G, \ 1 \mapsto x.$$

The image of the isomorphism being $\{e, x, \ldots, x^{n-1}\}$. Any group G such that $G = \{x^k : k \geq 0\}$ is called a **cyclic** group. If G is a finite group, then G is isomorphic to $\mathbb{Z}/|G|\mathbb{Z}$, otherwise G is isomorphic to $\mathbb{Z}$.

If p is any integer such that $p||G|$, then we can show that G has an element of order p in G; this result sometimes goes by the name **Cauchy's theorem**. Let us give two different proofs of this fact. The first one uses the class equation (2.1). Let us try to use induction on the cardinality of G to prove this statement. To describe the induction step, we observe that if $p \not| |G|$, then $p \not| |G|/|C_G(h_i)|$, for some h_i. Note that $|G| < |C_G(h_i)|1$ and hence we are done by induction hypothesis. Assume that $p||Z(G)|$, and we are again done if $|Z(G)| < |G|$. Thus, we need to prove this result for just abelian groups. Let G be a finite abelian group such that $p||G|$. I leave it an exercise to prove this result for cyclic groups. In general consider any element x such that $H = \{e, x, \ldots, x^k\}$ is a proper subset of G. Then, we have a surjective homomorphism

$$\pi : G \to G/H.$$

such that $|G/H| < |G|$. We may as well assume that $p \not| |H|$. Now, consider an element $y \in H$ such that order of y is p. Let $\tilde{y} \in \pi^{-1}(y)$. Now, the group $K = \{\tilde{y}^k : k \geq 0\}$ is a cyclic subgroup of G such that $p||K|$. Thus, there exists an element z of order p from the cauchy's theorem for cyclic groups.

2.5. Finally, it is time to discuss different ways to construct groups starting with given sequence of groups. Given a family groups $\{G_i : i \in I\}$, then we can consider

$$\prod_{i\in I} G_i := \{f : I \to \cup G_i : f(i) \in G_i\}.$$

The above set is a group by defining $[f_1.f_2](g) = f_1(g)f_2(g)$. If I is a finite set $\prod_{i\in I} G_i$ just constitutes the set of n-tuples $\{(g_1, \dots, g_n) : g_i \in G_i\}$ and the product structure being coordinate wise multiplication. Note that G_i embeds in $\prod_{i\in I} G_i$ by setting $g \mapsto f_g$, where $f_g(i) = g$ and $f_g(j) = e_j$, for $i \neq j$. Here, e_j is the identity element of G_j. By abuse of notation, we say that G_i is a subgroup of $\prod_{i\in I} G_i$. If $I = \{1, 2\}$, then G_1 is identified by $\{(g, e_2) : g \in G_1\}$ and G_2 is identified by $\{(e_1, g) : g \in G_2\}$ and $G_1 \times G_2$ is equal to G_1G_2 via this identification. Note that G_1 and G_2 commutes with each and has trivial intersection.

Let G be a group and let H and K be two subgroups of G such that K normalises H, i.e., $khk^{-1} \in H$, for all $k \in K$ and $h \in H$. This is just saying that K is contained in the largest subgroup of G which normalises H, i.e, $K \subseteq N_G(H)$ where

$$N_G(H) = \{g \in G : ghg^{-1} \in H, h \in H\}.$$

Note that the set KH is a subgroup of G, as

$$k_1h_1k_2h_2 = k_1k_2(k_2)^{-1}h_1k_2h_2, k_2(k_2)^{-1}h_1 \in H.$$

Moreover, if K centralises H, i.e., if $khk^{-1} = h$, for all $k \in K$ and $h \in H$, and if $K \cap H$ is trivial group then the map

$$K \times H \to KH; (k, h) \mapsto kh$$

is an isomorphism.

2.6. In this section, we will prove a range of results which will be called Sylow's theorems. Let G be a finite group of cardinality p^kn, where $(p, n) = 1$. Any subgroup G with p^k cardinality is called a p-Sylow subgroup of G.

Theorem 2.4. *Let G be a finite group and let $|G| = p^kn$, where $(p, n) = 1$. Then there exists a group P of cardinality p^k. Given any p-subgroup H is G, there exists a $g \in G$ such that $H \subseteq gPg^{-1}$. If N_p is the number of p-Sylow subgroups of G, then $N_p = 1 + kp$ for some integer k.*

Remark 2.5. *Given any two p-Sylow subgroups P_1 and P_2, using the above theorem there exists a $g \in G$ such that $gP_1g^{-1} = P_2$.*

Before, we prove this result, let us look at the example of $\mathrm{GL}_k(\mathbb{F}_p)$. Let $N_k(\mathbb{F}_p)$ be the group of upper triangular matrices with all its diagonal entries equal to 1. Note that $N_k(\mathbb{F}_p)$ is a p-Sylow subgroup of $\mathrm{GL}_k(\mathbb{F}_p)$.

Lemma 2.6. *Assume that H is a subgroup of G and suppose P is a p-Sylow subgroup of G. There exists a $g \in G$ such that $H \cap gPg^{-1}$ is a p-Sylow subgroup of H.*

Proof. Consider the (right) action of H on the (left) cosets $X = G/P$. Thus, we get that

$$|X| = |X^H| + \sum_{|\mathcal{O}_i|>1} |\mathcal{O}_i|$$

If $hgP = gP$, then $h \in gPg^{-1}$. Thus, the H-stabilizer of gP is equal to $H \cap gPg^{-1}$. Now, we have

$$|\mathcal{O}_i| = |H|/|H \cap gPg^{-1}|.$$

Note that p does not devide $|X|$. If p does not devide $|H|/|H \cap gPg^{-1}|$, then $H \cap gPg^{-1}$ is a p-Sylow subgroup of H. Otherwise p divides each of $|H|/|H \cap gPg^{-1}|$ and thus $|X^H| \neq 0$. If $gP \in X^H$, then $hgP = gP$, for all $h \in H$, and hence $H \subseteq gPg^{-1}$, and hence H is a p-group. □

Proof of theorem 2.4. Every finite group embeds into $\mathrm{GL}_k(\mathbb{F}_p)$, for some k and for any p. Thus, every finite group G has a p-Sylow subgroup, say P. If Q is any p-subgroup of G, then we set $H = Q$ in the above lemma. Hence, any two p-Sylow subgroups are conjugate in G. Let S_p be the set of p-Sylow subgroups of G. The group G acts on S_p by setting $\rho_g(P) = gPg^{-1}$. The group G acts transitively on the set S_p. Hence, we get that $N_p = |G|/|N_G(P)$, where $N_G(P) = \{g \in G : gPg^{-1} = P\}$. Let K be the group $N_G(P)$, and let the group P act on $X = G/N_G(P)$. By orbit stabilizer theorem, we get that

$$|X| \equiv |X^P| \pmod{p}.$$

Note that $gN_G(P) \in X^P$ if and only if $gPg^{-1} \in N_G(P)$. Now P is normal in $N_G(P)$, thus from the previous statement we get that $gPg^{-1} = P$. Hence $g \in N_G(P)$. Thus, $|X^P| = 1$. □

There are several other ways to prove Sylow's theorems. However, this proof indicates very interesting use of general linear groups. This method is similar to that of Suzuki's book on group theory.

2.7. **Exercises.** [All copied from some or the other sources]

2.7.1. Give an example of an infinite group G such that any proper subgroup of G is a finite group. What about uncountable groups G?

2.7.2. Give an example of an infinite group G such that $x^5 = e$, for all $x \in G$.

2.7.3. Let $\mathbb{Z}[1/p]$ be the group (under usual addition) of rational numbers of the form x/p^n, for some $x \in \mathbb{Z}$ and $n \geq 0$. Given two primes $p \neq l$, prove or disprove that $\mathbb{Z}[1/p]$ is isomorphic to $\mathbb{Z}[1/l]$.

2.7.4. Show that the group $\mathbb{R}/\mathbb{Z}$ is isomorphic to S^1, the unit circle. Are the groups $\mathbb{R}/\mathbb{Q}$ and $\mathbb{R}/\mathbb{Z}$ isomorphic?

2.7.5. What are the automorphism group of $\mathbb{Z}/N\mathbb{Z}$? Let G be a group such that for any $d||G|$, there exists a unique subgroup of order d. Then show that G is cyclic.

2.7.6. Let G be a group and let H be a subgroup of index 2 in G. Show that H is normal in G.

2.7.7. Let G be a group and let $Z(G)$ be the centre of G. If $G/Z(G)$ is cyclic then prove that G is abelian.

2.7.8. What are the subgroups of S_3 and S_4? Which of these groups are normal? What is the centre of S_n? Describe the cardinality of conjugacy classes in S_n. What is the cardinality of the set of p-Sylow subgroups of S_6.

2.7.9. Let P be a p-sylow subgroup of a finite group G. Show that $N_G(N_G(P)) = N_G(P)$ (we have already used this fact). If N is a normal subgroup of G and if Q is a p-Sylow subgroup of N then show that $G = NN_G(Q)$.

2.7.10. A group G is said to be **simple**, if the only normal subgroups of G are $\{e\}$ and G. For any group G we denote by PG the group $G/Z(G)$. Show that $\mathrm{PSL}_2(\mathbb{F}_p)$, for $p > 5$ is a simple group. What happens if $p \in \{2, 3\}$.

2.7.11. What are the number of p-sylow subgroups of $\mathrm{PSL}_n(\mathbb{F}_p)$? Let G be a finite simple group with $p+1$ number of p-Sylow subgroups. Show that p^2 does not devide $|G|$. Show that $|G|$ divides $p(p^2-1)$. Should G be isomorphic to $\mathrm{PSL}_2(\mathbb{F}_p)$? (The later part follows from a result of Frobenius on trasitive permutation actions on $p+1$ symbols, however, I am not completely sure of this: Let P be a p-Sylow subgroup of G. Since P is not a normal subgroup of G, we get that $G = PgP \coprod P$.)

2.7.12. *From Bourbaki Algebra I.* Let G and G' be two groups, and let $f : G \to G'$ be a map such that for any $a, b \in G$ we have either $f(ab) = f(a)f(b)$ or $f(ab) = f(b)f(a)$. In this series of exercies, we will show that $f(ab) = f(a)f(b)$ for all $a, b \in G$ or $f(ab) = f(b)f(a)$, for all $a, b \in G$. Show the following:

1. Show that the set $f^{-1}(e)$ is a normal subgroup of G. Show that it is enough to prove the above statement for injective maps f.

2. If $ab = ba$ shcow that $f(a)f(b) = f(b)f(a)$ (Consider $f(a^2b)$ and $f(a^2b^2)$).

3. Show that if $f(ab) = f(a)f(b)$, then $f(ba) = f(b)f(a)$.

4. Show that $f(aba) = f(a)f(b)f(a)$.

5. Let A be the set $\{a \in G : f(ab) = f(a)f(b), \forall b \in G\}$ and let B be the set $\{a \in G : f(ab) = f(b)f(a) : \forall b \in G\}$. Show that $A \neq G$, $B \neq G$ and $G = A \cup B$ is impossible.

6. If $A \cup B = G$, then there exists $a, b, c \in G$ such that

$$f(ab) = f(a)f(b) \neq f(b)f(a),\ f(ac) = f(c)f(a) \neq f(a)f(c).$$

Show that

$$f(c)f(a)f(b) = f(b)f(a)f(c).$$

7. Considering $f(abac)$ show that $A \cup B = G$.

2.7.13. *From Bourbaki Algebra I.* If G be a finite group of order n, the number of automorphisms of G is bounded by $n^{log_2 n}$.

2.7.14. *From Bourbaki Algebra I.* Recall that a homomorphism $f : G \to G$ is called an endomorphism of the group G. If an endomorphism is an isomorphism, then f is called an automorphism. The set of automorphisms of the group G is denoted by $\mathrm{Aut}(G)$. The automorphism of the form $\mathrm{ad}_h : G \mapsto G$, given by the map $g \mapsto hgh^{-1}$ are called an inner automorphism. The set of inner automorphisms $\mathrm{Inn}(G)$ forms a subgroup of $\mathrm{Aut}(G)$.

1. If an automorphism σ commutes with all elements of $\mathrm{Inn}(G)$, then show that $x\sigma^{-1}(x) \in Z(G)$. From now,

assume that G is a non-abelian simple group.

2. Let $s \in \mathrm{Aut}(\mathrm{Aut}(G))$. Show that $s(\mathrm{inn}(G)) = G$.

3. Let $s \in \mathrm{Aut}(\mathrm{Aut}(G))$ and let $s(ad_g) = ad_g$, for all $g \in G$. Show that $s = e$.

4. Show that $\mathrm{Aut}(\mathrm{Aut}(G)) = \mathrm{Inn}(\mathrm{Aut}(G))$.

2.7.15. *From Bourbaki Algebra I.*

1. Let G be a group and let H be a subgroup such that $|G/H| = n$. Let $N = \bigcap_{g \in G} gHg^{-1}$. Show that $|G/N| | n!$.

2. With the same notations in part (1), a subgroup H is called **residually finite** if N is trivial group $\{e\}$. If G is a residually finite group if and only if G is a subgroup of a product of finite groups.

3. If G is finnitely generated, i.e., $G = \langle S \rangle$ for some finite subset S of G, then show that the set P_m consisting of subgroups of G of index m is a finite set.

4. Let G be a finitely generated subgroup, and let $f : G \to G$ be a surjective endomorphism. For any m, show that the map $H \mapsto f^{-1}(H)$ is a bijection of P_m onto P_m. Show that $\ker(f)$ is contained in every subgroup H of G with finite index. Deduce that if G is residually finite then f is a bijection.

2.7.16. *From Bourbaki Algebra I.* Let H be a subgroup of G of finite index. Assume that G is the union of conjugates of H. Show that H is equal to G. Give a counter example of the case where $|G/H|$ is not finite. (Hint: Use the previous exercise to reduce this to the finite group case, and then use a counting argument)

2.7.17.

1. Let p be a prime number and let $x, y \in G$. Assume that $yxy^{-1} = x^n$ for some integer n and $x^p = e$. Show that $y^p x y^{-p} = x^n$ and deduce that y^{p-1} commutes with x.

2. Let G be a group for all of whose elements not e are of order p and conjugate to one another. Show that $|G| \leq 2$.

2.7.18. *From Bourbaki Algebra I.* Let A and B be two subgroups of a finite group G, let N_A and N_B be their normalizers respectively. Let ν_A and ν_B be the indicies of N_A and N_B respectively. Let r_A be the number of conjugates of A which contain B and r_B be the number of conjugates of B which contain A. Show that $\nu_A r_B = \nu_B r_A$.

2.7.19. *From Bourbaki Algebra I.* Let G be a group of permutations of a finite set E. For $s \in G$, we set $\chi(s)$ the number of fixed points of s, i.e., $\chi(s) = |\{x \in E : s(x) = x\}|$.

1. Show that $\sum_{s \in G} \chi(s) = |G|t$, where t is the number of orbits of G in E. (This is a very useful technique in many counting arguments, called the **Burnside's lemma** in literature)

2. Let $x \in E$, and $G_x = \{g \in G : gx = x\}$. If $G_x \neq \{e\}$ for all $x \in E$, and if $\chi(s) = k$, for all $s \in G$, then show that $k \leq t \leq 2k$.

3. Suppose that G operates transitively on E and let $x \in E$ be fixed. Show that $\sum_{s \in G} \chi(s)^2 = |G|t_x$, where t_x is the number of orbits of H in E.

3. Symmetric and alternating groups

3.1. In this section, we study symmetric groups, especially their conjugacy classes, etc. Later part of this section, we will study the normal subgroups of S_n and the group $\mathrm{Aut}(S_n)$ (the set of group group isomorphisms of S_n). Let σ be an element of S_n. Let $\langle \sigma \rangle$ act on $[n]$ by permuting its elements. Let $[n] = \coprod_{i=1}^{r} X_i$, where X_i is an orbit for the action of $\langle \sigma \rangle$. We may write

$$X_i = \{n_{i1}, n_{i2}, \dots, n_{ik}\}.$$

where $n_{ij} = \sigma(n_{i(j+1)})$, for all $j \leq k-1$ and $\sigma(n_{ik}) = n_{i1}$. We denote by $(a_1 a_2 \dots a_k)$ the permutation which takes

$$a_1 \mapsto a_2, a_2 \mapsto a_3, \dots, a_{k-1} \mapsto a_k; a_k \mapsto a_1,$$

and the rest of elements of the set $[n]$ are fixed by it. Note that

$$\sigma = \prod_{i=1}^{r} (n_{i1}, \dots, n_{ik_i}).$$

If we set $\sigma_i = \prod_{i=1}^{r} (n_{i1}, \dots, n_{ik_i})$, then σ_i and σ_j commute with each other. The above decomposition is called the cycle decompostion of σ. The partition $k_1 + k_2 + \cdots + k_r = n$ is called the cycle type of σ.

3.2. Let τ be any permutaiton and σ be a permutation and we continue to use the notations from the previous paragraph. The permutation $\tau\sigma\tau^{-1}$ has the same cycle type as σ. Moreover, if σ and σ' has the same cycle type then there exists a τ such that $\tau\sigma\tau^{-1} = \sigma'$. This follows from the following commutative diagram

$$\begin{tikzcd}
{[n]} \arrow[r, "\sigma"] \arrow[d, "\tau"'] & {[n]} \arrow[d, "\tau"] \\
{[n]} \arrow[r, "\tau\sigma\tau^{-1}"] & {[n]}
\end{tikzcd}$$

The permutation τ just plays the role of changing labels on the symbols $\{1, 2, \dots, n\}$. Hence, conjugacy classes in S_n correspond to the partitions of n. Let λ be a partition of n which essentially means that a sum of the form

$$k_1 + 2k_2 \cdots + rk_r = n.$$

Let $\mathcal{O}_\lambda$ be the set of all permutations of the type n. Clearly $\mathcal{O}_\lambda$ is a conjugacy class of S_n. Assume λ is the partition $\sum_{i=1}^{r} ik_i = n$, then $|\mathcal{O}_\lambda|$ is equal to

$$\frac{1}{k_1 k_2 \dots k_n} \frac{n!}{k_1! k_2! \dots k!}.$$

3.3. In this section, we will explicitly write down subgroups of S_3 and S_4 and their normal subgroups. The group S_3 consists of the following elements

$$\{(1),(12),(23),(13),(123),(132)\}.$$

The only subgroups of S_3 are cyclic, and hence it is easy to see that $\{(1),(12)\}$, $\{(1),(13)\}$, $\{(1),(23)\}$ and $\{(1),(123),(132)\}$ are the only subgroups of S_3.

Now, consider the case of S_4. The partitions of 4 are $\lambda_1 : 1+1+1+1$, $\lambda_2 : 1+1+2$, $\lambda_3 : 1+3$, $\lambda_4 : 2+2$ and $\lambda_5 : 4$. Hence S_4 consists of 5 distinct conjugacy classes. The groups A_4 is a normal subgroup of S_4 and hence is the union of conjugacy classes in S_4. Hence A_4 consists of the conjugacy classes correspond to λ_1, λ_3 and λ_4. Hence A_4 is given by

$$\{(1),(123),(132),(234),(324),(124),(214),(134),(341),(12)(34),(23)(14),(13)(24)\}.$$

Note that $K = \{(1),(12)(34),(23)(14),(13)(24)\}$ is a subgroup of A_4 and is a normal subgroup of A_4. Hence, the group A_4 can be written as $K.L$, where L is any subgroup of order 3. Infact A_4 is the semi-direct product of K and L.

3.4. In this subsection, we want to prove that S_n is generated by atmost n-elements of order 2. We will give a "presentation" of the group S_n. Later we will do the same for the alternating group A_n.

Lemma 3.1. *The group S_n is generated by traspositions, i.e., elements of the form (ij). Moreover, the group S_n is generated by transpositions*

$$S = \{(i,i+1) : 1 \leq i \leq n-1\}.$$

The group S_n is generated by the set of elements $\{(1i) : 2 \leq i \leq n\}$, or by the set of elements of the form $\{(12),(123\dots n)\}$.

Proof. We already observed that S_n is generated by cycles $(a_1,a_2,\dots,a_k)$. Note that

$$(a_1,a_2,\dots,a_k) = (a_1,a_2)(a_2,a_3)\dots(a_{k-1},a_k).$$

Hence it is enough to show that (ij) is generated by the set S. We may assume that $i<j$. We may obtain $(i+1,j)$ by conjugate (ij) to $(i+1,j)$ by conjugating with $\tau_1 = (i,i+1)$, and then obtain $(i+2,j)$ by conjugating with $(i+1,i+2)$ and so on. Hence (ij) is contianed in the group generated by S. The other parts are left as exercises. □

Lemma 3.2. *The group A_n is generated by cycles of order 3. Moreover, A_n is generated by the set*

$$T = \{(123),(124),\dots(12n)\}.$$

The group A_{2n+1} is generated by (123) and $(12\dots n)$ and A_{2n} is generated by (123) and $(234\dots n)$.

Proof. The group A_n must be generated by elements of the form $(ij)(kl)$, for some $i,j,k,l \in [n]$. If $\{i,j\} \cap \{k,l\} \neq \emptyset$, then assume that $j=k$, and $(ij)(kl) = (ijl)$. Assume that $\{i,j\} \cap \{k,l\} = \emptyset$. We may write

$$(ij)(kl) = (ij)(jk)(jk)(kl) = (ijk)(jkl).$$

Since the group S_n is generated by $\{(1i) : 2 \leq i \leq n\}$, we can consider any element of the form $(1i)(1j) \in A_n$. Now we have

$$(1i)(1j) = (1i)(12)(12)(1j) = (i12)(21j).$$

The above identity proves the second part of the accretion. The later part is left as exercise. □

Theorem 3.3 (Suggested as an exercise in Bourbaki Algebra I). *Let $n>5$. Then A_n is a simple group.*

Proof. □

4. Applications to groups of small cardinality

4.1. Let G be a finite abelian group. Note that all p-sylow subgroups of G are normal and hence we get that

$$G = P_1 \times P_2 \times \cdots \times P_i.$$

where P_i is a p_i-abelian subgroup of G. Note that we have not used the existence of p-Sylow subgroups of abelian groups in the proof of Sylow's theorems and hence there is no circular arguments here. Now, we need to understand finite abelian p-groups. For any abelian group G and a subgroup H of G, we set

$$\overline{H} := \{g \in G : g^{p^m} \in H\}.$$

4.2. Groups of order p are isomorphic to the cyclic group $\mathbb{Z}/p\mathbb{Z}$. Let us consider the groups of order p^2. We proved using the class equation that $Z(G)$ is non-trivial for any p-group G. Thus, we get that $G/Z(G)$ is cyclic and hence $Z(G)$ is abelian p-group.

5. Solvable and Nilpotent subgroups

6. Group representations