Some additional definitions:

Definition 0.1. *Let $f : A \mapsto B$ be the function. Then, we say A is the **domain** of f and B is the **codomain** of f.*

Definition 0.2. *Let $f : A \mapsto B$ is a function. We say f is **injective** (or an injection) if for all $a, a' \in A$ such that $a \neq a'$, $f(a) \neq f(a')$.*

Definition 0.3. *Let $f : A \mapsto B$ is a function. We say f is **surjective** (or a surjection) if for all $b \in B$, there exists $a \in A$ such that $f(a) = b$.*

Definition 0.4. *Let $f : A \mapsto B$ is a function. We say f is **bijective** (or a bijection) if f is injective and surjective.*

Definition 0.5. *Let $f : A \mapsto B$ be a function, $U \in A$ and $U' \in B$. Then, we call $f(U) = \{f(x) : x \in A\}$ the **image** of U and $f^{-1}(U') = \{x \in A : f(x) \in U'\}$ the **preimage** of U'. Note that the preimage of any subset of the codomain is always defined even if f is not invertible.*

Theorem 0.1. *A function f has an inverse such that $f \cdot f^{-1} = e$ and $f^{-1} \cdot f = e$ where e is the identity map (a function that sends everything to itself) if and only if f is bijective.*

Definition 0.6. *$\#S$ denotes the **cardinality** of a set S, which can be thought of as the size of the set. We say $\#S = \#T$ for sets T, S if there exists a bijection between the two sets, and $\#S \leq \#T$ if there exists an injection mapping S into T.*

1 Introductory group theory

This package is mostly for if anyone is interested in seeing how induction can be applied in other areas of math. The goal of this document is to investigate some more advanced mathematics, and how induction could be applied to prove useful results in maths. The examples using induction are bolded. Knowledge up to Chapter 7 or 8 will be sufficient along with the additional definitions above.

Formally, a group is defined as follows:

Definition 1.1. *1 A **group** is a set G closed under a binary operation $\cdot$ such that*

- *The operation is **associative**, meaning that for all $g_1, g_2, g_3 \in G$, $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$*
- *There exists a unique $e \in G$ called **the identity** such that for all $g \in G$, $g \cdot e = e \cdot g = g$*
- *For all $g \in G$, there exists a unique g^{-1} called **the inverse of** g such that $g^{-1} \cdot g = g \cdot g^{-1} = e$*

*A group is called **abelian** if for all $g, h \in G$, $gh = hg$.*

There are many examples of groups, they are practically everywhere.

- $\mathbb{Z}$ and $\mathbb{Z}_n$ which denote the integers mod n form a group under addition.
- The set of integers coprime to n under $\mod n$ forms a group under multiplication.
- $GL_n(\mathbb{R})$, the set of $n \times n$ invertible real matrices, forms a group under matrix multiplication.
- S_n from Q1 in the exercises forms a group under function composition as the operation.
- D_n, the set of symmetries on a regular $n-$gon forms a group under composition of rotations or reflections.
- $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$, known as the quaternion group, forms a group under multiplication.

Groups are very useful in many fields of mathematics especially given how omnipresent they are. Groups can even be contained in other groups.

Definition 1.2. *A* ***subgroup*** *H is a group entirely contained in G equipped with the same operation as G. A (left) coset of H is $xH = \{xh : h \in H\}$ where $x \in G$ is a fixed element. The index of H denoted $[G : H]$ is the number of distinct cosets of G.*

- The set of even integers form a subgroup of $\mathbb{Z}$ under addition. There are two cosets, the odd and even integers respectively.
- D_n is a subgroup of S_n. There are $\frac{(n-1)!}{2}$ cosets which consist of a permutation in S_n composing with everything in D_n.
- $SL_n(\mathbb{R})$, the set of $n \times n$ matrices with determinant 1, form a subgroup of $GL_n(\mathbb{R})$. There are infinite cosets which contain a matrix in $GL_n(\mathbb{R})$ being multiplied by everything in $SL_n(\mathbb{R})$.
- $\{1, -1, i, -i\}$ under multiplication is a subgroup of Q_8. There are 2 cosets, $\{1, -1, i, -i\}$ and $\{j, -j, k, -k\}$.

Groups can also come in different sizes, some are infinite, some are finite.

Definition 1.3. *The* ***order of a group*** *G, denoted $\#G$, is the number of elements in a group. The* ***order of an element*** *g, denoted $\#g$, is the smallest natural number n such that $g^n = e$ where e is the identity.*

We will specifically be interested in finite groups, i.e. groups with finite order. A lot of the times, knowing something about the order of the element can tell us about the order of the group, and vice versa, which we will see in the next section. Furthermore, we will introduce the notion of an isomorphism, which is a way to treat two different groups as the same.

Definition 1.4. *Let G, H be groups equipped with $\cdot$ and $\diamond$. An* ***isomorphism*** *is a bijection $\varphi : G \mapsto H$ such that for all $g, h \in G$, $\varphi(g \cdot h) = \varphi(g) \diamond \varphi(h)$. If there exists an isomorphism that maps G to H, then we say G and H are isomorphic.*

This definition tells us that if two groups are isomorphic, then we can treat multiplication in one group as the same as the multiplication in the other group. It tells us that the structure of the group, how things multiply, the properties of the group etc. are the same. Moreover, we can also new groups from existing groups via something called a direct product.

Definition 1.5. *Let G, H be groups equipped with $\cdot$ and $\diamond$ as operations respectively. We define $G \times H = \{(g, h) : g \in G, h \in H\}$ as the **(external) direct product** of G and H where multiplication is defined as $(g, h) \cdot (g', h') = (g \cdot g', h \diamond h')$.*

We can also construct a group as a direct product of subgroups of the group at times.

Definition 1.6. *Let G be a group with subgroups H, K such that*

- $G = HK = \{hk : h \in H, k \in K\}$
- $H \cap K = \{e\}$
- *For all $h \in H$ and $k \in K$, $hk = kh$*

*Then, G is called an **internal direct product** of H and K and moreover, $G \cong H \times K$.*

Here are some potentially interesting results, some of which can be surprising:

- Let $\mathbb{R}$ be the group of the reals under addition and $(\mathbb{R}^+, \cdot)$ be the group of positive reals under multiplication. Then, $\mathbb{R} \cong (\mathbb{R}^+, \cdot)$ with $\varphi(x) = e^x$ being an isomorphism.
- Let a cyclic group $\langle g \rangle = \left\{g^k : k \in \mathbb{N}\right\}$ be a group equipped with $\cdot$ as the operation. Then, if $\langle g \rangle$ is infinite, $\langle g \rangle \cong \mathbb{Z}$ where $\mathbb{Z}$ denotes the integers under addition and if $\langle g \rangle$ is finite with k elements, $\langle g \rangle \cong \mathbb{Z}_k$ where $\mathbb{Z}_k$ is the group of integers under addition mod k.
- Every finite group is isomorphic to a subgroup of S_n (Cayley's Theorem).
- $\{1, -1, i, -i\}$ under multiplication is isomorphic to $\mathbb{Z}_4$.
- $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$ but $\mathbb{Z}_4 \not\cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

2 Finitely generated abelian groups

We are going to examine a specific type of group called finitely generated abelian groups. To begin, we will examine the very special case where the group is generated by 1 element, namely $\langle g \rangle$ (See the examples above), and then we will move onto defining finitely generated abelian groups and more general results. We know if $\langle g \rangle$ is infinite, $\langle g \rangle \cong \mathbb{Z}$. Surprisingly, for finite cases, it gets more complicated. Suppose $\langle g \rangle \cong \mathbb{Z}_n$ where $n \in \mathbb{N}$. If $n = 1$, then $\langle g \rangle = \{e\}$ which is the trivial group of only 1 element. Otherwise, we can relate the group structure of integers under addition mod n to the prime factorisation of n.

1. **Prove that for all $n \geq 2 \in \mathbb{N}$, $\mathbb{Z}_n \cong \prod_{i=1}^{r} \mathbb{Z}_{{p_i}^{e_i}}$.**

Proof. Let $n \geq 2 \in \mathbb{N}$. We prove by strong mathematical induction on n.

- For the base case, consider $n = 2$. Then, for $\mathbb{Z}_2$, 2 is prime so the result holds.
- Assume that for all $2 \leq \ell \leq k$, $\mathbb{Z}_\ell \cong \prod_{i=1}^{r} \mathbb{Z}_{{p_i}^{e_i}}$. For $\mathbb{Z}_{k+1}$, by the fundamental theorem of arithmetic, we know $k + 1 = {p_1}^{e_1}{p_2}^{e_2} \dots {p_\ell}^{e_\ell} = {p_1}^{e_1}({p_2}^{e_2} \dots {p_\ell}^{e_\ell})$ where p_i are distinct primes.
  - If there is only one p_1, then the result holds.
  - If there are multiple p_i, we know by the Chinese remainder theorem that if u, v are relatively prime, then $\mathbb{Z}_{uv} \cong \mathbb{Z}_u \times \mathbb{Z}_v$, so, since ${p_1}^{e_1} < k + 1$ and ${p_2}^{e_2} \dots {p_\ell}^{e_\ell} < k + 1$ and they are coprime, we have that $\mathbb{Z}_{{p_1}^{e_1}}$ is isomorphic to itself and $\mathbb{Z}_{{p_2}^{e_2} \dots {p_\ell}^{e_\ell}}$ is isomorphic to $\prod_{i=2}^{r} \mathbb{Z}_{{p_i}^{e_i}}$ by our induction hypothesis, so we have $\mathbb{Z}_{k+1} \cong \mathbb{Z}_{{p_1}^{e_1}} \times \prod_{i=2}^{r} \mathbb{Z}_{{p_i}^{e_i}} = \prod_{i=1}^{r} \mathbb{Z}_{{p_i}^{e_i}}$

□

Since we have $\langle g \rangle \cong \mathbb{Z}_n$, we have that any group generated by one element can be decomposed into a direct product $\prod_{i=1}^{r} \mathbb{Z}_{{p_i}^{e_i}}$ or $\mathbb{Z}$ or $\{e\}$. We will now define finitely generated groups.

Definition 2.1. *A group G is* ***generated by*** *$S \subseteq G$, if for all $g \in G$, $g = g_{\alpha_1} g_{\alpha_2} \dots g_{\alpha_r}$ where for all g_{α_i}, $g_{\alpha_i} \in S \subseteq G$. We call elements of S as* ***generators*** *of G, and we write $G = \langle S \rangle$. If S is finite, then we say G is* ***finitely generated****. Suppose G is finitely generated with generators $g_1, g_2, \dots, g_n$. Then, we can write $G = \langle g_1, g_2, \dots, g_n \rangle$.*

A remark is that finitely generated groups need not to be finite. $\mathbb{Z}$ for example is a finitely generated group generated by 1, but it is an infinite group. A group generated by a single element, which we have seen in the examples after Definition 1.8, as it turns out, will be essential to our proofs moving forward. For the sake of clarity, we will define it here.

Definition 2.2. *A group G with $\cdot$ as the operation is called* ***cyclic*** *if it is generated by a single element g, that is, $G = \langle g \rangle = \left\{g^k : k \in \mathbb{N}\right\}$. Note that g^k denotes $g \cdot g \cdot g \cdot \dots$ with $\cdot$ being the operation of G.*

We are going to slowly work try to completely determine the structure of finitely generated abelian groups. We will first come up with more definitions and prove some basic group theory results.

Theorem 2.1 (Lagrange's theorem)**.** *Let G be a finite group and H be a subgroup of G. Then, $\#H \mid \#G$ and $\#G = \#H[G : H]$.*

Proof. Let G be a finite group and H be a subgroup of G. Notice we can map aH to H bijectively under the map $x \mapsto a^{-1}x$ which has the inverse $y \mapsto ay$, so $\#aH = \#H$. Notice the left cosets are the equivalence classes of the equivalence relation $x \sim y$ if and only if $x = yh$, so the left cosets form a partition on G and thus the union of distinct left cosets will be equal to G so $\#G = \#H[G : H]$ as required. □

Definition 2.3. *A subgroup K of G is called* ***normal*** *if for all $g \in G$, $gKg^{-1} = K$, and we denote $K \trianglelefteq G$ to indicate that K is normal in G (and $\triangleleft$ if K is stricly contained in G). G/K is then called a* ***quotient group*** *where the elements of G/K are cosets of K.*

Note that we can only form quotient groups over normal subgroups because otherwise our multiplication will not be well defined. Now, we will prove a theorem due to Cauchy for abelian groups.

Theorem 2.2 (Cauchy's theorem - the Abelian case)**.** *Let G be a finite abelian group with order n. Then, if p is a prime such that $p \mid n$, there exists an element of order p in G.*

2. Prove Cauchy's theorem for finite abelian groups.

Proof. Let G be an a finite abelian group and let p be a prime. We proceed with strong induction on n and show that this holds for all $pn \in \mathbb{N}$ where pn is the order of G.

- For the base case, let $n = 1$. Then, $\#G = p$. By Lagrange's theorem, we know that any subgroup $H \subseteq G$ must have an order that divides p, so $H = \{e\}$ or $H = G$. Since $\#G \neq 1$, it follows that there exists $g \in G$ such that $g \neq e$. Consider $\langle g \rangle$, which must have more than one element. From before, it follows that $\langle g \rangle = G$ so $\#\langle g \rangle = p$ and it follows that g has order p. Hence, the base case holds.
- For the inductive step, assume the result holds for all $p\ell$ where $1 \leq \ell \leq k$. For G with order $p(k+1)$, take $g \in G$ such that $g \neq e$ and consider $H = \langle g \rangle$.
  - Assume $p \mid \#H$. Then, let $g \in H$ and assume $\#g = m$. It follows that $g^{\frac{m}{p}}$ has order p so the base case holds.
  - Now assume $p \nmid \#H$. Since H is abelian, then G/H is an abelian quotient group. Notice $\#G = \#H[G : H] = \#H\#G/H$ and $p \mid G$ but $p \nmid \#H$ so $p \mid \#G/H$. Since $g \neq e$, $\#H \neq 1$ and $\#G/H < \#G$ and by the inductive hypothesis, we have that there exists an element of order p in G/H, call it $g'H$. Suppose $\#g' = m$. Then, notice $(g')^m H = (g'H)^m = H$ so $p \mid m$ and it follows that $g^{m/p}$ has order p so the result follows.

  Since the base case and the inductive hypothesis hold, by the principle of mathematical induction, the result holds for all $n \in \mathbb{N}$.

□

We will come up with one more definition and prove another lemma.

Definition 2.4. *Let G be a group and p be a prime. Then, G is called a $p-$**group** if for all $g \in G$, $\#g = p^n$ for some $n \in \mathbb{N}$.*

Lemma 2.1. *Let p be a prime and G be finite and abelian. G has order $\#G = p^n$ if and only if for all $g \in G$, g has order p^s for some $s \geq 0$.*

Proof. Let p be a prime and G be finite and abelian. We prove each direction in turn.

- For one direction, assume $\#G = p^n > 1$. Let $g \in G$ and notice $\#\langle g \rangle = \#g$ and since $\langle g \rangle$ is a subgroup of G, by Lagrange's theorem, $\#g \mid p^n$ so $\#g = p^s$ for some $s \geq 0$.

- For the other direction, we take the contrapositive and hence assume $\#G \neq p^n$. Then, G is either the trivial group $\{1\}$, or the order of G has another prime factor q. By Cauchy's theorem for abelian groups, we know we can find an element with order $q \neq p^n$ for all n as required.

□

The above tells us that finite abelian $p-$groups must also have order p^n, and if a finite abelian group has order p^n, then it is also necessarily a $p-$group.

3. **Prove that if G is a finite abelian $p-$group and let $g \in G$ have maximal order, then, there exists a subgroup $H \subseteq G$ such that G is the internal direct product $\langle g \rangle \times H$**

   Proof. Let G be a finite abelian $p-$group. We proceed with strong induction on the order of G.

   - For the base case, assume G has order p. We show $G = \langle g \rangle$ where $g \neq e$. By Lagrange's theorem, we know that any subgroup of G must have an order that divides $\#G = p$, so the subgroups can only have order 1 or 2. Now let $g \neq e$ so $\langle g \rangle \neq \{e\}$. Then, $\#\langle g \rangle = p$ so $G = \#\langle g \rangle$. It follows that we can simply take the direct product $\langle g \rangle \times \{e\}$ since both subgroups are normal, have e as the intersection, and their elements commute. Hence, $G \cong \langle g \rangle \times \{e\}$ and G is the internal product of $\langle g \rangle$ and $\{e\}$.
   - For the inductive step, assume that for G with order $1 \leq \ell \leq k$, there exists $H \subseteq G$ such that $G \cong \langle g \rangle \times H$. For G' with order $k+1$, let $g \in G'$ be the element with maximal order p^m.
     - If $\langle g \rangle = G'$, then $G' \cong \langle g \rangle \cap \{e\}$ where $H = \{e\}$.
     - If $\langle g \rangle \neq G'$, then consider $G'/\langle g \rangle$. Choose $a\langle g \rangle \in G'/\langle g \rangle$ to be the element with minimal order > 1, so $a \notin \langle g \rangle$. Since $\#a^p < \#a$, by the minimality of $a\langle g \rangle$, we have $a^p \in \langle g \rangle$ so $a^p = g^r$ for some $r \in \mathbb{N}$. Since g has order p^m which is the maximal order, $a^{p^m} = e = (a^p)^{p^{m-1}} = (g^r)^{p^{m-1}} = g^{rp^{m-1}}$ so $p^m \mid rp^{m-1}$ and thus $p \mid r$ and $r = ps$ for some s. Let $b = g^{-s}a$ and notice $b \notin \langle g \rangle$ and $b^p = g^{-ps}a^p = g^{-ps}g^r = e$ so $\#b = p$. Choose $H = \langle b \rangle$ and notice $H \cap \langle g \rangle = \{e\}$. Consider $gH \in G'/H$. If $(gH)^{p^s} = H$ then $g^{p^s} \in H$ but since $H \cap \langle g \rangle = \{e\}$, $g^{p^s} = e$ so $p^m \mid p^s$ and gH has order p^m. Notice $\#G'/H < \#G'$. By the inductive hypothesis, there exists a subgroup K of G'/H such that $G'/H \cong \langle gH \rangle \times K$ with G'/H being an internal direct product. Let φ be the natural map $G' \mapsto G'/H$ where $g \mapsto gH$, and let $J = \varphi^{-1}(K)$. Then, notice $J = \{k \in G' : kH \in K\}$, so J is a subgroup in G' that contains K. I claim $G' \cong \langle g \rangle \times J$ and G' is an internal direct product.
       - We first show $G' = \langle g \rangle J$. Since G' is closed under multiplication, we know $G' \supseteq \langle g \rangle J$ so it suffices to check $G' \subseteq \langle g \rangle J$. Let $x \in G'$, so $xH = (yH)(kH)$ where $y \in \langle g \rangle H$ and $k \in J$ from $G'/H \cong \langle gH \rangle \times K$. It follows

that $x = g^i hkh' = g^i k'$ by the normality of K and $k' \in K \subseteq J$, so $x \in \langle g \rangle J$. Hence, $G' \subseteq \langle g \rangle J$ and $G' = \langle g \rangle J$.

$*$ Now we check $\langle g \rangle \cap J = \{e\}$. If $h \in \langle g \rangle \cap J$, then $hH = \langle gH \rangle \cap K$ in G'/H so $h \in \langle g \rangle \cap H$ and $h = e$.

$*$ Finally, we check $g^i j = jg^i$, but this is evident since G' is abelian.

It follows that $G' \cong \langle g \rangle \times J$ and is an internal direct product so the inductive step holds.

By the principle of mathematical induction, the result holds for all finite abelian $p-$groups. □

Lemma 2.2. *Let G_{mn} be an abelian group of order mn where* $\gcd(m,n) = 1$. *Then, G_{mn} is the internal direct product $G_m \times G_n$ where G_m is the set of elements with orders dividing m and G_n is the set of elements with order dividing n.*

Proof. G_m, G_n are subgroups and notice $G_m \cap G_n = \{e\}$. By Bézout's lemma, we have $am + bn = 1$ for some $a, b \in \mathbb{Z}$. Then, $g = g^{am+bn} = (g^m)^a (g^n)^b$ but $\#g^m \mid n$ since $g^m n = e$ and likewise $\#g^n \mid m$. Hence, $G_m G_n = G_{mn}$ so $G_{mn} \cong G_m \times G_n$. □

Theorem 2.3 (Fundamental theorem of Finite Abelian Groups)**.** *Any finite abelian group is a product of finite cyclic $p-$groups.*

Proof. Write $\#G$ as its prime factorisation. By induction on the previous lemma, $G \cong \prod_{i=1}^r G_i$ and G_i consists of elements of order a power of p_i, so G_i is cyclic for all i. Hence, the result follows. □

This induction is pretty straightforward so the details are left to the reader.

3 Sylow's Theorems

There are also other strong results that can be proven via induction. One of which would be the first theorem out of the Sylow theorems, which give very important insights into the structure of groups. To do this, we will introduce the notion of conjugacy class and centralizers.

Definition 3.1. *Let G be a group and $g \in G$. Then, the **conjugacy class of** x is* $\mathrm{Cl}(x) = \{gxg^{-1} | g \in G\}$.

Keep in mind, conjugacy classes do not need to be groups. Furthermore, conjugacy classes form a partition on G under the relation $a \sim b$ if and only if $a = gbg^{-1}$ for some $g \in G$, which means G can be viewed as a disjoint union of conjugacy classes.

Definition 3.2. *Let G be a group and $x \in G$. Then, the **centralizer of** x is $C(x) = \{g \in G | gx = xg\}$.*

Conjugacy classes and centralizers are very closely related. In particular, we have the equation $\#G = \#C(x)\#\text{Cl}(x)$ by a theorem called the orbit-stabilizer theorem which we will not discuss in this reading. We will consider one more definition.

Definition 3.3. *Let G be a group. Then, the **center of** G is $Z(G) = \{h | \forall g \in G, gh = hg\}$.*

In other words, the center of a group is the set of elements that commute with everything. It follows that if $g \in Z(G)$, $\text{Cl}(g) = \{g\}$ since for all $h \in G$ we have $hgh^{-1} = hh^{-1}g = g$ as g commutes with everything in G, and the converse implication holds as well. Now suppose G is a group. Then, it can be split up into a bunch of conjugacy classes and we can take a representative from each conjugacy class, call them $x_1, x_2, x_3 \ldots$ and form the set $\{x_1, x_2, x_3 \ldots\}$. Then, since $Z(G)$ is just the collection of elements whose conjugacy classes consist of 1 element, we can write out the equation

$$\#G = \#Z(G) + \sum_{x \in \{x_1, x_2, x_3 \ldots\} \setminus Z(G)} \#\text{Cl}(x)$$

This equation is often called the **class equation**. We will use this to prove Sylow's first theorem.

Theorem 3.1 (Sylow I)**.** *If p is prime and $p^k | \#G$, then G has a subgroup of order p^k.*

4. Prove Sylow I.

Proof. We proceed with strong mathematical induction on $\#G$.

- The base case is $\#G = p$ and is trivial.
- For the inductive step, assume the statement holds for all groups with order less than $\#G$. Then, notice either $p | \#Z(G)$ or $p \nmid \#Z(G)$.
  - If $p | \#Z(G)$, then by Cauchy's theorem for abelian groups there exists an element h with order p in $\#Z(G)$ and thus G. $H = \langle h \rangle$ is in $Z(G)$ and so is normal in G. Now, $\#G/H < \#G$ so by induction there exists a subgroup K such that $\#K = p^{k-1}$ in G/H so taking $\pi^{-1}(K) \leq G$ where π is the map $g \mapsto gH$ will give a subgroup of order p^k.
  - If $p \nmid \#Z(G)$, by the class equation, we know

    $$\#G = \#Z(G) + \sum_{x \in \{x_1, x_2, x_3 \ldots\} \setminus Z(G)} \#\text{Cl}(x)$$

    and $p | \#G$ but $p \nmid \#Z(G)$ implies there exists $\text{Cl}(x)$ such that $p \nmid \#\text{Cl}(x)$ and hence $p^k \nmid \#\text{Cl}(x)$. Notice $\#G = \#C(x)[G : C(x)] = \#C(x)\#\text{Cl}(x)$ by the orbit-stabilizer theorem and $p^k \mid G$ implies $p^k \mid C(x)$. By induction, since $\#C(x) < \#G$, $C(x)$ has a subgroup of order p^k and hence so does G.

By the principle of mathematical induction, the result follows. □

4 Exercises

These are pretty standard group theory results for the most part and you can more or less find all answers on Stack Exchange or similar websites.

1. We define a **permutation** on the set $X = \{1, 2, 3, \ldots, n\}$ as a bijection $f : X \mapsto X$ and let S_n be the set of permutations on X.

   (a) Prove that S_n is a group and has $n!$ elements.

   (b) We say $\sigma \in S_n$ is a **cycle** if σ is a function that maps $a_1 \mapsto a_2 \mapsto a_3 \mapsto \ldots \mapsto a_n \mapsto a_1$ and for all $b \in X$ such that $b \neq a_i$ for all i. We write this cycle as $(a_1 a_2 a_3 \ldots a_n)$, and we say two cycles are **disjoint** if they have no overlapping a_i. Prove that for all $\sigma \in S_n$, σ can be written as a product of disjoint cycles.

   (c) We say τ is a **transposition** if τ is a cycle of the form (ab) where $a \neq b$. Prove that the identity map e can only be written as a product of an even number of transpositions. (Hint: The inverse of a transposition is itself)

   (d) Assume that every permutation σ can be written as a product of transpositions. Prove that if σ can be written as an even product of transpositions, it cannot be written as an odd product of transpositions (The same holds vice versa. Hence, it makes sense to call permutations **even** or **odd**).

   (e) Let $n \geq 3$. Prove that every even permutation in S_n can be written as a product of $3-$cycle (abc) where $a \neq b \neq c$. (Essentially what you are proving is that the group of even permutations called A_n is generated by 3-cycles)

   (f) Assume that every permutation σ can be written as a product of transpositions. Prove that S_n is generated by $(12), (13), (14), \ldots, (1n)$.

   (g) Assume that every permutation σ can be written as a product of transpositions. Prove that S_n is generated by $(12), (23), (34), \ldots, (n-1\ n)$.

   (h) Prove that S_n is generated by $(12), (12 \ldots n)$ for $n \geq 3$. (Hint: Use (g))

2. (a) Prove that every finite $p-$group has order p^n.

   (b) We say a group G is **solvable** if there exists a finite series $\{1\} = G_n \lhd G_{n-1} \lhd \ldots \lhd G_2 \lhd G_1 \lhd G_0 = G$ where for all i, G_i/G_{i+1} is abelian. Prove that every finite $p-$group is solvable.

   (c) We define a **lower central series** as $\ldots \lhd G_2 \lhd G_1 \lhd G_0 = G$ where for each i, $G_i = [G_i, G]$ which is the group generated by all elements of the form ${g_i}^{-1} g^{-1} g_i g$ where $g_i \in G_i$ and $g \in G$. Let G, H be groups and $\varphi : G \mapsto H$ be a function such that $f(gg') = f(g)f(g')$ for all $g, g' \in G$. (such functions are called **homomorphisms**) where for all i, $\varphi(G_i) \leq K_i$. Prove that if φ is surjective, then $\varphi(G_i) = K_i$.

   (d) We say a group G is **nilpotent** if it has a lower central series that ends with $G_n = \{1\}$ for some $n \in \mathbb{N}$. Prove that every finite $p-$group is nilpotent. (Hint: Use part (c))

3. Do the actual induction and complete the proof for Theorem 2.3.