Important Results - MATH 456

Ralph Sarkis 260729917

January 12, 2018

1 Basic Concepts

Definition 1.1 (Some important groups)**.** S_n denotes the group of permutations of a set of size n, it is called the symmetric group. A_n denotes the even permutations in S_n, it is called the alternating group. The dihedral group is the set of symmetrices of a regular n-gon on the plane: $D_n = \langle x^n = y^2 = 1, yxy = x^{-1} \rangle$.

Theorem 1.2 (Lagrange)**.** *Let H be a subgroup of G, then $[G : H] = \frac{|G|}{|H|}$, this is the index of H in G.*

Proof idea. Observe that cosets form equivalence classes so G is a disjoin union of them, also each coset has the size of H, the result follows. □

Corollary 1.3. *The order of any subgroup $H \leq G$ divides the order of the group G, the order of any element also divides $|G|$.*

Proposition 1.4. *If $\mathbb{F}$ is a finite field, then $\mathbb{F}^\times$ is a cyclic group.*

Proof idea. Denote $q = |\mathbb{F}|$, show that for every h dividing $q - 1$, there is at most one group of order h (it uses the roots of $x^h - 1$). For each divisor h of $q - 1$ with an element of order h, we have $\phi(h)$ elements of order h. We get that there must be an element of each order that divides $q - 1$ to get enough elements, in particular, we get an element of order $q - 1$. □

Proposition 1.5. *If $\mathbb{L}$ is a finite field containing $\mathbb{F}$, a field with q elements, then Ł has order a power of q.*

Proof idea. Think of $\mathbb{L}$ as a vector space over $\mathbb{F}$, as $\mathbb{L}$ is finite, it must have dimension $n < \infty$, implying that $\mathbb{L}$ is isomorphic to $\mathbb{F}^n$ as a vector space. □

Definition 1.6 (Centralizer and normalizer)**.** Let $H \leq G$, the centralizer is $\text{Cent}_G(H) = \{g \in G \mid \forall h \in H, gh = hg\}$. The normalizer is $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$.

Definition 1.7 (Commutator)**.** The commutator subgroup of G is $G' = [G, G] = \{[x, y] = xyx^{-1}y^{-1} \mid x, y \in G\}$.

Proposition 1.8. *The commutator subgroup is a normal subgroup and $G^{ab} = G/G'$ is abelian. Moreover, G/N being abelian implies that $N \supseteq G'$.*

Proof idea. For the first part, we use the fact that for any $g, a, b \in G$, we have $gabg^{-1} = gag^{-1}gbg^{-1}$, $g[x, y]g^{-1} = [gxg^{-1}, gyg^{-1}]$, then see that $gG'g^{-1} \subseteq G'$. For the second part, use $yx = xy(y^{-1}x^{-1}yx)$ and $y^{-1}x^{-1}yx \in G'$ to prove G^{ab} is abelian and $xyN = yxN$ to show $[x, y] \in N$ for any x, y. $\square$

Proposition 1.9. *Let $B < G$ and $N \lhd G$, then $B \cap N \lhd B$, $BN = NB < G$ and $|BN| = \frac{|B| \cdot |N|}{|B \cap N|}$. If B is also normal, then $BN \lhd G$ and $B \cap N \lhd G$.*

Proof idea. Just use the definitions. For the cardinality part, let $f : B \times N \to BN$ with $f(b, n) = bn$, then show that $f^{-1}(x)$ has size $|B \cap N|$. $\square$

2 Isomorphism Theorems

Proposition 2.1. *Let $f : G \to H$ be a group homomorphism, then $A < G \implies f(A) < H$, $B < H \implies f^{-1}(B) < G$ and $B \lhd H \implies f^{-1}(B) \lhd G$.*

Proof idea. Just need to check the definitions. $\square$

Lemma 2.2. *Let f be a group homomorphism, then f is injective if and only if* $\ker(f)$*. Moreover, the fiber of any element in the image is a coset of* $\ker(f)$*.*

Theorem 2.3 (First isomorphism theorem)**.** *Let $f : G \to H$ be a homomorphism, $K \lhd G$, and $K \subseteq \ker(f) = N$, then there is a unique homomorphism $F : G/K \to H$ such that the following diagram commutes:*

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi_K"'] & H \\ G/K \arrow[ur, dashed, "F"'] & \end{tikzcd}$$

Proof idea. The map is $F : G/K \to H$ with $F(gK) = f(g)$, it is unique because π_K is surjective. $\square$

Corollary 2.4. $G/N \cong \text{Im}(f)$.

Proof idea. Take $K = N$. $\square$

Corollary 2.5. *If* $(|G|, |H|) = 1$, *then* f *is trivial (i.e.* $\ker(f) = G$*).*

Proof idea. We know that $|G/N|$ divides $|G|$, but also divides $|H|$ since $G/N \cong \operatorname{Im}(f)$, this implies $|G/N| = 1$. □

Corollary 2.6 (Chinese remainder theorem). *Let* $m, n \in \mathbb{N}$ *with* $(m, n) = 1$, *we have* $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Proof idea. Take $f : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ with $f(x) = (x \pmod m, x \pmod n)$ and look at the kernel. □

Theorem 2.7 (Second isomorphism theorem). *Let* $B < G$ *and* $N \lhd G$ *be subgroups, then* $BN/N \cong B/(B \cap N)$.

Proof idea. Let $f : BN \to B/(B \cap N)$ with $f(bn) = b \cdot B \cap N$ and use FIT. □

Theorem 2.8 (Correspondence theorem). *Let* $f : G \to H$ *be a surjective homomorphism, then* f *induces a bijection between the subgroups of* G *containing* $\ker(f)$ *and the subgroups of* H. *Moreover, let* $\ker(f) < G_1 < G_2$, *then* $G_1 \lhd G_2$ *if and only if* $f(G_1) \lhd f(G_2)$ *giving* $G_2/G_1 \cong f(G_2)/f(G_1)$.

Proof idea. The first and second part uses definitions, the last part uses the composition $G_2 \to f(G_2) \to f(G_2)/f(G_1)$ that has kernel $f^{-1}(f(G_1)) = G_1$, then apply FIT. □

Theorem 2.9 (Third isomorphism theorem). *Let* H *and* K *be normal subgroups of* G *such that* $H \leq K$, *then* $(G/H)/(H/K) \cong G/K$.

Proof idea. Apply the correspondence theorem with $H = G/N$, $f = \pi_N$, $G_1 = K$ and $G_2 = G$. □

3 Group Actions

Lemma 3.1 (Orbit-Stabilizer formula). *Let* G *act on* S *and* $s \in S$, *then* $|\operatorname{Orb}(s)| = \frac{|G|}{|\operatorname{Stab}(s)|}$.

Proof idea. Let $\phi : G/\operatorname{Stab}(s) \to \operatorname{Orb}(s)$, be defined by $\phi(g \operatorname{Stab}(s)) = g * s$, show that this is well-defined and that this is an isomorphism. □

Proposition 3.2. *Let* G *act on* S *and* $s, t \in S$ *with* $t \in \operatorname{Orb}(s)$, *then* $\operatorname{Stab}_G(t)$ *is conjugate to* $\operatorname{Stab}_G(s)$.

Proof idea. Let $g \in G$ with $g * s = t$ and $h \in \operatorname{Stab}(s)$, then $ghg^{-1} * t = t$ and we get $g \operatorname{Stab}(s) g^{-1} \subseteq \operatorname{Stab}(t)$, we get the other direction similarly. □

Proposition 3.3. *Let* H *and* K *be two subgroups of* G *with finite index, then* $H \cap K$ *also has finite index in* G.

Proof idea. Let G act diagonally on $G/H \times G/K$, the stabilizer of (H, K) is $H \cap K$, then use the orbit-stabilizer formula. □

Lemma 3.4. *A group G acting on S is equivalent to a homomorphism $\phi : G \to \Sigma_S$, we say that this actions affords the permutation representation ϕ. Moreover,* $\ker(\phi) = \cap_{g\in G} \operatorname{Stab}(s)$.

Proof idea. For any $g \in G$ and $s \in S$, $\phi(g)(s) = g * s$, this is a homomorphism. □

Theorem 3.5 (Cayley)**.** *Every finite group is isomorphic to a subgroup of $S_{|G|}$.*

Proof idea. Let G act on itself by multiplication, the stabilizers are all trivial, so the permutation representation is injective, the result follows. □

Definition 3.6 (Coset representation)**.** Let $H \lhd G$, G acts on G/H affording the homomorphism $\phi : G \to S_m$ where $m = [G : H]$. ϕ is called the coset representation, $\ker(\phi) = \cap_{g\in G} gHg^{-1}$ is the maximal subgroup of H which is normal in G.

Proposition 3.7. *Let G be a finite group and $H < G$ of index p, where p is the minimal prime dividing the order of G, then H is normal in G.*

Proof idea. Consider the coset representation $\phi : G \to S_p$, we get $p = [G : H] \mid [G : \ker(\phi)]$ and $[G : \ker(\phi)] \mid p!$, leading to $[G : \ker(\phi)] = p$, or $H = K \implies H \lhd G$. □

Theorem 3.8 (Cauchy-Frobenius Formula)**.** *Let G act on a set S, then the number of ordbits is equal to $\frac{1}{|G|} \sum_{g\in G} \#Fix(g)$, where $\#Fix(g)$ denotes the number of fixed points of G.*

Proof idea. Write $T(g, s) = \begin{cases} 1 & g * s = s \\ 0 & g * s \neq s \end{cases}$ and observe that $\#\text{Fix}(g) = \sum_{s\in S} T(g, s)$ and $|\operatorname{Stab}(s)| = \sum_{g\in G} T(g, s)$. Now expand, rearrange and simplify $\sum_{g\in G} \#\text{Fix}(g)$. □

Corollary 3.9. *If G acts transitively on S, then there exists a $g \in G$ with no fixed points.*

Proof idea. Suppose $\#\text{Fix}(g) \geq 1$ for any g, use $\#\text{Fix}(e) = |S|$ and CFF to arrive at a contradiction. □

Proposition 3.10. *Let G act transitively on S, $s \in S$ and $K \lhd G$, the number of orbits of K on its action on S is $[G : K \operatorname{Stab}_G(s)]$.*

Proof idea. Observe that $g * K * s = K * s$ if and only if $k^{-1}g \in \operatorname{Stab}_G(s)$ if and only if $g \in K \operatorname{Stab}_G(s)$. Since the action of G on the K orbits is transitive, $G/(K \operatorname{Stab}_G(s))$ is in bijection with the K orbits. □

4 Symmetric Group

Lemma 4.1. *Two elements $\sigma, \tau \in S_n$ are conjugates if and only if they have the same cycle type.*

Proof idea. Use the fact that $\tau(i_1\, i_2 \ldots i_t)\tau^{-1} = (\tau(i_1)\; \tau(i_2) \ldots \tau(i_t))$ and find the τ that works in reverse. □

Corollary 4.2. *There are $p(n)$ conjugacy classes in S_N, where $p(n)$ denotes the number of partitions of n.*

Lemma 4.3. *The S_n-conjugacy class of an element $\sigma \in A_n$ is a disjoint union of $[S_n : A_n \operatorname{Cent}_{S_n}(\sigma)]$ A_n-conjugacy classes. In particular, there are two such conjugacy classes if there is an odd permutation commuting with σ, otherwise there is only one.*

Proof idea. Apply proposition 3.10 with $G = S_n$, $K = A_n$ and S being the conjugacy class of S_n. $\square$

Lemma 4.4. *Let $\sigma \in A_N$, then $\operatorname{Cent}_{S_n}(\sigma)$ contains odd permutation unless the disjoint cycle form of σ contains only odd cycles of different lengths.*

Lemma 4.5. *A normal subgroup $N \lhd G$ is a union of disjoint conjugacy classes.*

Proof idea. The conjugacy classes are orbits of a group action so they are disjoint, N being normal implies the conjugacy classes of all its elements are contained in N. $\square$

Lemma 4.6. *The alternating group A_5 is simple.*

Proof idea. Look at the cycle types and the size of each conjugacy class in A_5 by observing the conjugacy classes in S_5 as well. Conclude that a normal group can only have size 1 or 60. $\square$

Theorem 4.7. *The alternating groups A_n are simple for $n \geq 5$.*

Proof idea. Proof by induction, base case done above. Let $N \lhd A_n$, with $N \neq \{1\}$, show that for any i, there is a non-trivial $\rho \in N$ such that $\rho(i) = i$. Now, consider each copy of A_{n-1} that fixes an element i, call it G_i. Since G_i is simple and $N \cap G_i$ is normal in G_i, $N \cap G_i = G_i$, this shows that $N \supseteq \langle G_1, \dots, G_n \rangle = A_n$. $\square$

Proposition 4.8. *Suppose that A_n acts transitively on a set of size $m > 1$, then $m \geq n$.*

Proof idea. $\square$

Proposition 4.9. *Let $\sigma \neq 1$ be a permutation of S_n, $n \geq 3$, then the conjugacy class of σ has more than one element.*

5 p-groups, Cauchy's and Sylow's theorems

Lemma 5.1 (Class equation)**.** *Let G be a group, then we have the class equation:*

$$|G| = |Z(G)| + \sum_{\text{reps } x \notin Z(G)} \frac{|G|}{|\operatorname{Cent}_G(x)|}$$

Proposition 5.2. *If G has an even number of conjugacy classes, then G has even order.*

Proof idea. Observe that the inverse function f acts on the conjugacy classes and induces a bijection $\operatorname{Conj}(x) \leftrightarrow \operatorname{Conj}(x^{-1})$. Since f fixes $\operatorname{Conj}(1)$, it fixes another one, yielding a bijection on some $\operatorname{Conj}(x_0)$ with $x_0 \neq 1$. If $|G|$ were odd, $|\operatorname{Conj}(x_0)|$ must be odd but since $f^2 = 1$, this implies f fixes a point in $\operatorname{Conj}(x_0)$ which leads to a contradiction. □

Lemma 5.3. *For any $M \in \mathbb{N}$, up to isomorphisms, there are finitely many groups of order at most M.*

Proof idea. Consider the number of possible binary functions. □

Lemma 5.4. *Let $q \in \mathbb{Q}_{>0}$, and $k \in \mathbb{N}$, there are finitely many tuples of positive integers $(n_1, \dots, n_k)$ such that $q = \frac{1}{n_1} + \cdots + \frac{1}{n_k}$.*

Proof idea. Order the fractions in increasing order, deduce a bound for the last denominator and then use induction on $q - \frac{1}{n_k}$ and a tuple of $k-1$ integers. □

Theorem 5.5. *Let $N \in \mathbb{N}$, up to isomorphism, there are finitely many finite groups with N conjugacy classes.*

Proof idea. Use the last lemma with the class equation. □

Lemma 5.6. *Let G be a p-group (i.e. $|G| = p^r, r \in \mathbb{N}$), then $Z(G) \neq \{1\}$.*

Proof idea. Write the class equation, then look at the equation in $\mathbb{Z}/p\mathbb{Z}$. □

Lemma 5.7. *Let G be a p-group and $H \neq \{1\}$ a normal subgroup, $H \cap Z(G) \neq \{1\}$.*

Proof idea. Write the class equation for the action of G on H by conjugation, then look at the equation in $\mathbb{Z}/p\mathbb{Z}$. □

Theorem 5.8. *Let G be a p-group, then the following holds:*

1. *For any $H \lhd G$, $H \neq G$, there exists $H^+ \lhd G$ such that $H < H^+$ and $[H^+ : H] = p$.*
2. *For any $H \lhd G$, $H \neq \{1\}$, there exists $H^- \lhd G$ such that $H^- < H$ and $[H^- : H] = p$.*

Proof idea.

1. Since G/H is a p-group, there is a non-trivial $x \in Z(G/H)$, the order of x is a power of p, so you can get y of order p. Let $K = \langle y \rangle \lhd G/H$, we then use the quotient map and the correspondence theorem to lift K to H^+.
2. Use induction, case $|G| = p$ is clear. Choose an element $x \in H \cap Z(G)$ of order p. Let $K = \langle x \rangle \lhd G$, note that $K \subseteq H$. If $H = K$, take $H^- = \{1\}$. Otherwise, apply induction on G/K to find $(H/K)^-$ and use the correspondence theorem to lift it to H^-.

□

Lemma 5.9. *Let G be any group and $H \subset Z(G)$ such that G/H is cyclic, then G is abelian.*

Proof idea. Let $g \in G$ be such that gH generates G/H. This implies that every element is of the form $g^i h$, show that these elements commute. $\square$

Definition 5.10 (Frattini subgroup)**.** The Frattini subgroup of a p-group G , denoted $\Phi(G)$, is the intersection of all the maximal subgroups of G.

Proposition 5.11. *Let G be a p-group, $\Phi(G) \lhd G$ is a non-trivial abelian group where every non-zero element is of order p. It is the largest quotient with this property. Also, $\Phi(G) = G^p G'$.*

Proof idea. Conjugation takes maximal subgroups to maximal subgroups so $\Phi(G)$ is normal. The index of a maximal subgroup H forces G/H to be abelian, so $H \supseteq G'$, implying $\Phi(G) \supseteq G'$ so $G/\Phi(G)$ is also abelian. Also, gH has order p so $g^p \in H$ and $H \supseteq G^p$ implying $\Phi(G) \supseteq G^p$. We get that $\Phi(G) \supseteq G^p G'$ and every non-trivial element has order p, this is true for any $N \lhd G$ with G/N abelian and elements killed by p. Then show $\Phi(G) \subseteq G^p G'$ by passing to a vector space over $\mathbb{F}_p$. $\square$

Lemma 5.12. *Let A be a finite abelian group with a prime $p \mid |A|$, A has an element of order p.*

Proof idea. We use induction, case $|A| = p$ is clear. Let N be a maximal subgroup of A, it is normal because A is abelian. If p divides $|N|$ use induction. Otherwise, take $x \in A \setminus N$ and let $B = \langle x \rangle$, show that $p \mid |B|$, so we can find an element of order p. $\square$

Proposition 5.13. *Let G be a non-commutative p-group and H be a normal subgroup such that G/H is abelian and $|H| = p$, then $H = G'$. If every element of G/H has order p, then $H = \Phi(G)$.*

Proof idea. By the definition of G', we have $G' \subseteq H$, but $G' \neq \{1\}$, so we must have $G' = H$. The second statement follows from proposition 5.11. $\square$

Proposition 5.14. *Let G be a group of order $p^r m$ where p is prime and $(p, m) = 1$, there exists a subgroup of order p^r.*

Proof idea. We use induction, the case $|G| = p$ is clear. If $p \mid |Z(G)|$, then take $N = \langle x \rangle \lhd G$, where x is of order p. Consider G/N, its order is $p^{r-1}m$, we can use induction and the correspondence theorem to lift a group of order p^r.

In the case where $p \nmid |Z(G)|$. Consider the class equation modulo p, and find that $\mathrm{Cent}_G(x)$ is a proper subgroup of order divisible by p^r so we can use induction. $\square$

Corollary 5.15. *Let $p_1^{a_1} \cdots p_k^{a_k}$ be the prime factorization of $|G|$ and P_i be a subgroup of size $p_i^{a_i}$, then $G = \langle P_1, \ldots, P_k \rangle$.*

Proof idea. The order of $\langle P_1, \ldots, P_k \rangle$ is divisible by the order of the group. $\square$

Corollary 5.16 (Cauchy's theorem)**.** *Let G be finite with $p \mid |G|$, then G has an element of order p.*

Proof idea. We find a subgroup of order p^r, find an element of order p^b and then transform it to an element of order p. $\square$

Lemma 5.17. *Let P be a maximal p-subgroup of G and Q be any q-subgroup of G, where q is a different prime. $Q \cap P = Q \cap N_G(P)$.*

Proof idea. Since $P \subseteq N_G(P)$, we have $Q \cap P \subseteq Q \cap N_G(P) =: H$. For the other direction, see that HP is a p-subgroup of $N_G(P)$ but it must be P since P is maximal. This yields $H \subseteq P$ and the result follows. $\square$

Theorem 5.18 (Sylow). *Let G be a group of order $p^r m$ where p is prime and $(p, m) = 1$, the following holds:*

1. *Every maximal p-subgroup has order p^r (they are called p-Sylow subgroups).*
2. *All p-Sylow subgroups are conjugate to each other.*
3. *Let $n_p = |\operatorname{Syl}_p(G)|$, then $n_p \equiv 1 \pmod p$ and $n_p \mid m$.*

Proof idea. Let $S = \{P_1, \ldots, P_a\}$ be the set of conjugates of some p-Sylow P. Let Q, any p-subgroup, act by conjugation on S, the size of $\operatorname{Orb}(P_i)$ is $\frac{|Q|}{|\operatorname{Stab}_Q(P_i)|} = \frac{|Q|}{|Q \cap P_i|}$. We see that the sizes are a power of p unless $Q \subseteq P_i$, in that case, the size is one.

If we take $Q = P_1$, we know that only the orbit of P_1 has size 1 because P_1 is maximal. Hence, S being the disjoin union of orbits has size congruent to 1 modulo p. Suppose towards a contradiction that Q is a maximal subgroup not in S and let it act on S. We get that all the orbits are congruent to 0 modulo p, contradicting our previous statement. Lastly, if we use the orbit stabilizer formula on the action of G by conjugation on the set of maximal subgroups, we get $a = \frac{|G|}{|N_G(P)|}$, so a divides $|G|$. $\square$

Lemma 5.19. *Let G be finite, $p \neq q$ be two primes dividing $|G|$ and $P \in \operatorname{Syl}_p(G), Q \in \operatorname{Syl}_q(G)$, then $P \cap Q = \{1\}$.*

Proof idea. The size of $P \cap Q$ divides $|P|$ and $|Q|$, since $(p, q) = 1$, we must have $|P \cap Q| = 1$. $\square$

Lemma 5.20. *Let G be any group and $A, B \lhd G$, then for any $a \in A$ and $b \in B$, $ab = ba$.*

Proof idea. Note that $aba^{-1}b^{-1}$ is in both A and B so it must be 1, the result follows. $\square$

Proposition 5.21. *Let$p_1^{a_1} \cdots p_k^{a_k}$ be the prime factorization of $|G|$ and P_i be a p_i-Sylow subgroup. $G = P_1 \times \cdots \times P_k$ if and only if for any i, $P_i \lhd G$.*

Proof idea. Suppose all the P_i are normal, then take $f : P_1 \times \cdots \times P_k \to G$ be defined by $f(x_1, \ldots, x_k) = x_1 x_2 \cdots x_k$. Since P_i and P_j commute for $i \neq j$, f is a homomorphism, then show it is bijective. $\square$

Proposition 5.22. *Let G be finite, $H \lhd G$ and P be a p-Sylow subgroup of G. $P \cap H$ is a maximal p-subgroup and HP/H is a p-Sylow subgroup of G/H.*

Proof idea. Show that $|Q \cap H| = |P \cap H|$ for any p-Sylow Q of G. Since a p-Sylow of H is contained in a p-Sylow of G, we see by cardinality that $H \cap P$ must be a p-Sylow of H. For the second part, calculate the size of HP/H and G/H. □

Definition 5.23 (Nilpotent groups)**.** A nilpotent group only has normal Sylow subgroups. Equivalently, for any prime p dividing the order of the group, there is a unique p-Sylow subgroup.

6 Composition Series and Solvable Groups

Definition 6.1. A normal series for G is a series of subgroups $G = G_0 \triangleright \cdots \triangleright G_n = \{1\}$ (it is usually strictly descending, namely $G_i \neq G_j$ for $i \neq j$).

Definition 6.2. A composition series for G is a normal series such that G_{i-1}/G_i is non-trivial and simple for all $i \in \{1, \ldots, n\}$. The quotients are called the composition factors, they are considered up to isomorphism but with multiplicity.

Definition 6.3. A group G is called solvable if it has a normal series in which all the composition factors are abelian.

Lemma 6.4. *Any strictly descending normal series can be refined to a composition series. Moreover, if the composition factors are abelian, the refinement has composition factors isomorphic to $\mathbb{Z}/p\mathbb{Z}$ for some prime p.*

Proof idea. Note that the quotients are non trivial and that $|G|$ is the product of the orders of the quotients. Hence, a strictly descending normal series has bounded length. Assume that the series is not a composition series, take G_{i-1}/G_i that is not simple and take a non-trivial normal subgroup H', lift it to G_{i-1} and extend the series to $\cdots G_{i-1} \triangleright H \triangleright G_i \cdots$, the first part follows. For the second part, note that our construction still has abelian quotients. Also, finite abelian simple groups are isomorphic to $\mathbb{Z}/p\mathbb{Z}$. □

Corollary 6.5. *A group G is solvable if and only if it has a composition series with composition factors being cyclic groups of prime order.*

Theorem 6.6 (Jordan-Hölder)**.** *Let G be finite, any two composition series for G have the same composition factors (considered with multiplicity).*

Examples 6.7. Any abelian group is solvable, p-groups are solvable, groups of order pq are solvable, groups of order p^2q are solvable, groups of order pqr are solvable and the product of solvable groups are solvable.

Proposition 6.8. *Let G be solvable and $K < G$, K is solvable.*

Proof idea. Intersect K with the groups in the normal series with abelian quotients for G, we get a normal series with abelian quotients but for K. □

Definition 6.9. A short exact sequence is a sequence of group and homomorphism $1 \to G_1 \xrightarrow{f} G_2 \xrightarrow{g} G_3 \to 1$ with f injective, g surjective and $\mathrm{Im}(f) = \ker(g)$.

Proposition 6.10. *Let $1 \to K \to G \to H \to 1$ be a short exact sequence, G is solvable if and only if K and H are solvable.*

Proof idea. Assume that G is solvable, then $f(K)$ is solvable (hence K as well). If G_i are the groups in the normal series for G, let $H_i = g(G_i)$ be the ones for H, then show that this is a normal series with abelian factors.

Assume K and H are solvable. Let $J_i = g^{-1}(H_i)$ and $J_i = f(K_{i-n})$ for the rest, J_i is a normal series with abelian quotients. □

Theorem 6.11. *Every group of order less than 60 is solvable.*

Theorem 6.12 (Burnside)**.** *Every group of order $p^a q^b$ is solvable.*

Theorem 6.13 (Feit-Thompson)**.** *Every finite group of odd order is solvable.*

7 Finitely Generated Abelian Groups and Semidirect Products

Definition 7.1. A group G is called finitely many generated if there are elements $g_1, \ldots, g_n$ in G such that $G = \langle g_1, \cdots, g_n \rangle$.

Lemma 7.2. *An abelian group G is finitely generated if for some positive integer n, there is a surjective homomorphism from $\mathbb{Z}^n$ to G.*

Theorem 7.3 (Structure theorem)**.** *Let G be a finitely generated abelian group, then there exists unique $r \in \mathbb{N}$ and $n_1, \ldots, n_t \in \mathbb{N}_{>1}$ such that $G \cong \mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_t\mathbb{Z}$.*

Definition 7.4. Let G be a group and B and N be subgroups of G such that $G = NB$, $N \cap B = \{1\}$ and $N \lhd G$. We say that G is a semidirect product of N and B. Also, if N and B are groups and $\phi : B \to \mathrm{Aut}(N)$ is a group homomorphism, we define $N \rtimes_\phi B$ to be the semidirect product of N and B relative to ϕ. It is the group $N \times B$ with the following operation:

$$(n_1, b_1) \cdot (n_2, b_2) = (n_1 \phi(b_1)(n_2), b_1 b_2)$$

Proposition 7.5. *$N \rtimes_\phi B \cong N \times B$ if and only if ϕ is trivial.*

Proof idea. Use the definitions. □

Proposition 7.6. *$N \rtimes_\phi B$ is abelian if and only if both N and B are abelian and ϕ is trivial.*

Proof idea. Use the definitions. □

Proposition 7.7. *Let N and B be groups and ϕ and ψ be homomorphisms $B \to \mathrm{Aut}(N)$, then $N \rtimes_\phi B \cong N \rtimes_\psi B$ if and only if there exists automorphisms $f \in \mathrm{Aut}(N)$ and $g \in \mathrm{Aut}(B)$ such that $\forall b \in B, \psi(b) = f \circ \phi(g(b)) \circ f^{-1}$. The isomorphism between the two semidirect products is $(n, b) \mapsto (f(n), g^{-1}(b))$.*

Proof idea. Just verify that the map seen is an isomorphism. □

Lemma 7.8. *Let $n \in \mathbb{N}$, $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.*

Proof idea. For any $a \in \mathbb{Z}/n\mathbb{Z}$ such that $(a, n) = 1$, show that $f_a(x) = ax$ is in $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$, then show that $a \mapsto f_a$ is an isomorphism. □

Proposition 7.9. *If $p \mid (q-1)$, there is a unique non-abelian group of order pq.*

Proof idea. We know that any q-Sylow Q is normal. Let P be any p-Sylow, G is a semidirect product of Q and P. There is a non-abelian semidirect product when ϕ maps 1 to $a \mapsto ha$, where h is an element of order p of $(\mathbb{Z}/q\mathbb{Z})^\times$. It is clear that any other homomorphism that works will just have a different h, but then we can transform it as in proposition 7.7 to get the isomorphism. □

8 Complex Representation of Finite Groups

Definition 8.1 (Representation)**.** Let G be a finite group, V be a finite dimensional vector space over $\mathbb{C}$ and $\rho : G \to \mathrm{Aut}(V)$ be a group homomorphism, (ρ, V) is called a finite representation of G.

Definition 8.2 (Morphism of representation)**.** Let (ρ, V) and (τ, W) be representations of a finite group G, a linear map $T : V_1 \to V_2$ is called a morphism of ρ_1 to ρ_2 if for any $g \in G$, $\rho_2(g) \circ T = T \circ \rho_1(g)$. We will denote $\mathrm{Hom}_G(V_1, V_2)$ to be the subspace of $\mathrm{Hom}(V_1, V_2)$ with linear maps satisfying this property.

Definition 8.3 (Character group)**.** For a group G, the character group of G, denoted G^*, is the set of group homomorphisms from G to $\mathbb{C}^\times$.

Proposition 8.4. *The following are properties of the character group.*

1. $(H \times G)^* \cong H^* \times G^*$.
2. $(\mathbb{Z}/n\mathbb{Z})^* \cong \mathbb{Z}/n\mathbb{Z}$.
3. *If G is finite and abelian, $G^* \cong G$.*
4. *For a general group G, $G^* = (G/G')^*$.*

Proof idea. 1. Define the map $\phi : (H \times G)^* \to H^* \times G^*$ with $f \mapsto (f(\cdot, 1), f(1, \cdot))$. Show that it is an isomorphism.

2. Observe that $f \in (\mathbb{Z}/n\mathbb{Z})^*$ is only defined by where it sends the generator, and it must send it to a generator of the group of nth roots of unity (this group is isomorphic to $\mathbb{Z}/n\mathbb{Z}$).

3. Use the structure theorem and the two previous points.

4. Show that if $f \in G^*$, then $f([x,y]) = 1$ and so $G' \subseteq \ker(f)$, then the result follows from the first isomorphism theorem.

$\square$

Theorem 8.5. *Let (ρ, V) be a representation of G, there exists a inner product that is G-invariant (i.e. for all $v, w \in V$, $\langle \rho(g)v, \rho(g)w \rangle = \langle v, w \rangle$).*

Proof idea. Take any inner product $(\cdot,\cdot)$ and let $\langle u, v \rangle = \frac{1}{|G|} \sum_{g \in G} (\rho(g)u, \rho(g)v)$, verify that $\langle \cdot, \cdot \rangle$ is G-invariant. $\square$

Theorem 8.6. *Any representation decomposes as a sum of irreducible representations.*

Proof idea. Argue by induction. If U is a subrepresentation, then $U^\perp$ (w.r.t. a G-invariant inner product) is also a subrepresentation. $\square$

Theorem 8.7. *Let G be an abelian group, every representation of G decomposes into a direct sum of 1-dimensional representations.*

Proof idea. First prove that $\rho(g)$ is diagonalizable. Then use the fact that commuting diagonalizable linear operator are simultaneously diagonalizable. $\square$

Lemma 8.8 (Schur)**.** *Let (ρ, V) and (τ, W) be irreducible representations of G, we have the following:*

$$\mathrm{Hom}_G(V, W) \cong \begin{cases} 0 & \rho \not\cong \tau \\ \mathbb{C} & \rho \cong \tau \end{cases}$$

Proof idea. Note that if $T \in \mathrm{Hom}_G(V, W)$, $\ker(T)$ and $\mathrm{Im}(T)$ are subrepresentations, this implies T is either trivial or an isomorphism. Now, look at an eigenspace of T and show that it must be equal to the whole vector space. $\square$

Definition 8.9. Let (ρ, V) and (τ, W) be representations of $G, \sigma : G \to \mathrm{Aut}(\mathrm{Hom}(V, W))$ is a new representation with $\sigma(g)T = \tau(g) \circ T \circ \rho(g^{-1})$.

Theorem 8.10. *We get that for any $g \in G$, $\chi_\sigma(g) = \overline{\chi_\rho(g)}\chi_\tau(g)$.*

Proof idea. No need to learn it. $\square$

Definition 8.11. Let (ρ, V) be a representation of G, define the projection operator as $\pi_\rho : V \to V$ with $\pi_\rho = \frac{1}{|G|} \sum_{g \in G} \rho(g)$.

Theorem 8.12. *If $\rho = \rho_1^{a_1} \oplus \cdots \oplus \rho_t^{a_t}$ where ρ_1 is the trivial representation, then*

$$\pi_\rho = Id_{V_1^{a_1}} \oplus 0 \oplus \cdots \oplus 0$$

From this, we get the following:

$$a_1 = Tr(\pi_\rho) = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g) = \langle \chi_\rho, \chi_1 \rangle$$

Proof idea. Note that $V^G = (V_1^{a_1})^G \oplus \cdots \oplus (V_1^{a_t})^G$ and that except for $i = 1$, $(V_i^{a_i})^G = \{0\}$ because it is a subrepresentation. The result follows. □

Theorem 8.13. *The characters of irreducible representations are orthogonal with respect to the G-invariant inner product.*

Proof idea. Use $\dim(\mathrm{Hom}(V, W)^G) = \frac{1}{|G|} \sum_{g \in G} \chi_\sigma(g) = \langle \chi_\rho, \chi_\tau \rangle$. Then use Schur's lemma. □

Proposition 8.14. *Here are some consequences of the last theorem.*

1. *A representation ρ decomposes into an irreducible representation: $\rho = \rho_1^{a_1} \oplus \cdots \oplus \rho_t^{a_t}$.*
2. $a_i = \langle \chi_\rho, \chi_{\rho_i} \rangle$.
3. *χ_ρ determines ρ up to isomorphism.*
4. $\rho^{reg} = \rho_1^{\dim(\rho_1)} \oplus \cdots \oplus \rho_t^{\dim(\rho_t)}$.
5. *ρ is irreducible if and only if $\|\chi_\rho\| = 1$.*
6. *There exists finitely many irreducible characters (hence representations).*

Proof idea.

1. Done above.
2. Follows from orthogonality of the irreducible characters.
3. Follows from the last part.
4. Follows from the fact that χ_{reg} is 0 everywhere but on the identity.
5. Follows from orthonormality of the irreducible characters.
6. Since they are orthonormal, they can be bigger than the dimension of $\mathrm{Class}(G)$.

□

Definition 8.15. We define a more general operator. Let $\alpha \in \mathrm{Class}(G)$, we define the operator $A_\rho = \sum_{g \in G} \alpha(g) \rho(g)$.

Lemma 8.16. *For two representations ρ and τ of G, $A_{\rho\oplus\tau} = A_\rho \oplus A_\tau$.*

Proof idea. Use the definitions. $\square$

Theorem 8.17. *Let $\chi_{\rho_1}, \ldots, \chi_{\rho_t}$ be the characters of all the irreducible representations of G, they form an orthonormal basis of $\mathrm{Class}(G)$, in particular, $t = h(G)$.*

Proof idea. Let $\beta \in \mathrm{Class}(G)$ be a function orthogonal to all irreducible characters. Let $\alpha = \overline{\beta}$ and for an irreducible representation ρ_i, show that $A_{\rho_i} \equiv 0$. Using the last lemma, we get $A_{\rho^{\mathrm{reg}}} \equiv 0$, which is equivalent to $\alpha = \overline{\beta} \equiv 0$. $\square$

Proposition 8.18. *Let $g, h \in G$ and $\{\chi_i \mid i \in \{1, \ldots, h(G)\}\}$ be the irreducible representations of G, then:*

$$\sum_{i=1}^{h(G)} \chi_i(g)\overline{\chi_i(h)} = \begin{cases} |\operatorname{Cent}_G(g)| & \textit{if } g \textit{ and } h \textit{ are conjugate} \\ 0 & \textit{otherwise} \end{cases}$$

Proof idea. Let g_i be the representative for the conjugacy classes and $c_i = |\operatorname{Conj}(g_i)|$, also let T be the character table (i.e. $(T)_{ij} = \chi_i(g_j)$) and $D = \operatorname{diag}\left(\frac{|c_1|}{n}, \ldots, \frac{|c_{h(G)}|}{n}\right)$. The row orthogonality condition says that $TDT^* = I_{h(G)}$, implying that $T^{-1} = DT^*$. We obtain $T^*T = D^{-1}\operatorname{diag}\left(\frac{n}{|c_1|}, \ldots, \frac{n}{|c_{h(G)}|}\right)$, showing the result since $\frac{|G|}{|\operatorname{Conj}(g)|} = |\operatorname{Cent}_G(g)|$. $\square$

Proposition 8.19. *For $n \geq 4$, the representation $\rho^{st,0}$ of A_n is irreducible.*

Proof idea. Recall that $\chi = \chi_1 + \chi_0$ where χ is the standard representation, χ_1 is the trivial one and $\chi_0 = \chi_{\rho^{st,0}}$. We will use $\|\chi\|^2 = \|\chi_1\|^2 + \langle\chi_1, \chi_0\rangle + \langle\chi_0, \chi_1\rangle + \|\chi_0\|^2$. Show that $\|\chi\|^2 = 2$, let A_n act diagonally on $\{1, \ldots, n\}^2$, show that there are two orbits, then use CFF with the fact that $\#\mathrm{Fix}(\sigma) = \chi(\sigma)$. Now, show that $\langle\chi_1, \chi_0\rangle = \langle\chi_0, \chi_1\rangle = 0$ and since χ_1 is irreducible, the result follows. $\square$

Proposition 8.20. *Let $z \in Z(G)$ and V be an irreducible representation of G, then z acts on V as a multiple of the identity.*

Proof idea. Let V_λ be an eigenspace of $\rho(z)$, show that V_λ is a non-trivial subrepresentation, hence equal to V. $\square$