Chapter 1

Symmetries, groups, and group actions

1.1 Lecture 1.

Group theory is all about symmetries of *objects*. Every *object* is a set with certain *properties*. A *symmetry* of an object X is a function $f : X \to X$ which preserves all the *properties* of X.

1.1.1 Symmetric group.

Suppose X is just a set. Then symmetries of X is

$$S_X := \{\sigma : X \to X \mid \sigma \text{ is a bijection}\}.$$

Notice that σ is in S_X exactly when it is invertible. Hence, for every $\sigma \in S_X$, σ^{-1} exists and it is in S_X. We also notice that if f and g are bijections, then $f \circ g$ is also a bijection. Clearly the identity function id_X is in S_X. Therefore, S_X is a group under the function composition. The group $(S_X, \circ)$ is called the *symmetric group* of X. The symmetric group of $\{1, \ldots, n\}$ is denoted by S_n. Notice that the cardinality of S_n is $n!$. The cardinality of a group G is called the *order* of G.

1.1.2 Symmetries of a graph.

Suppose X is an undirected graph with the set of vertices V and the set of edges E. A symmetry of X is a bijection $f : V \to V$ such that for every $v, w \in V$

$$\{v, w\} \in E \Leftrightarrow \{f(v), f(w)\} \in E;$$

this means v and w are connected precisely when $f(v)$ and $f(w)$ are. A symmetry of a graph X is called an *automorphism* of X. The set of all automorphisms of X is denoted by $\mathrm{Aut}(X)$. Notice that the identity function id_V is an automorphism of X. If $f \in \mathrm{Aut}(X)$, then $f : V \to V$ is an invertible function. Notice that for every $v, w \in V$,

$$\{f^{-1}(v), f^{-1}(w)\} \in E \Leftrightarrow \{f(f^{-1}(v)), f(f^{-1}(w))\} \in E \Leftrightarrow \{v, w\} \in E.$$

Thus, $f^{-1} \in \mathrm{Aut}(X)$. If $f, g \in \mathrm{Aut}(X)$, then $f \circ g$ is a bijection as f and g are; moreover for every $v, w \in V$, we have

$$\{v, w\} \in E \Leftrightarrow \{g(v), g(w)\} \in E \Leftrightarrow \{f(g(v)), f(g(w))\} \in E;$$

this means $f \circ g \in \mathrm{Aut}(X)$. (With the same type of argument, one can show that the set of symmetries of any object is a group, and historically this was one of the main motivation of mathematicians to study group theory.)

1.1.3 Dihedral group.

Let X_n be a cycle with n vertices. For convenience, we let

$$\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$$

be the set of vertices of X_n. We let the set E_n of edges of X_n be

$$E_n = \{\{i, i+1\} \mid i \in \mathbb{Z}/n\mathbb{Z}\}.$$

This means for $i, j \in \mathbb{Z}/n\mathbb{Z}$, we have

$$\{i, j\} \in E_n \Leftrightarrow i - j = \pm 1 + n\mathbb{Z}.$$

From this point of an n-cycle can be viewed as a *Cayley graph* of the cyclic group $\mathbb{Z}/n\mathbb{Z}$ with respect to the set $\{\pm 1 + n\mathbb{Z}\}$. (The *Cayley graph* of a group G with respect to a subset S is a graph whose set of vertices is G and for every $g_1, g_2 \in G$,

$$\{g_1, g_2\} \in E \Leftrightarrow g_2 = sg_1 \text{ for some } s \in S;$$

in order to make sure that this is an undirected graph, we are assuming that S is a symmetric set; that means if $s \in S$, then $s^{-1} \in S$.) Here, we want to understand the group of automorphisms of X_n. Looking at a regular n-gon, one can see certain symmetries given by rotations and reflections. Using the labeling in terms of the elements of $\mathbb{Z}/n\mathbb{Z}$ a rotation by angle $2\pi/n$ is given by function

$$\sigma : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad \sigma(i) := i + 1,$$

and a reflection about the x-axis is given by

$$\tau : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad \tau(i) := -i.$$

Applying these automorphisms one after another, one still gets automorphisms of X_n. Applying only σ many times, how many new automorphisms do we get? (Let's recall that the *order* of an element g in a group is $n \in \mathbb{Z}^+ \cup \{\infty\}$ if n is the smallest positive integer such that g^n is the identity. The order of g is denoted by $o(g)$, and if $o(g)$ is finite, then $\{e, g, \ldots, g^{n-1}\}$ is a group of order $o(g)$ and $g^i = g^j$ precisely when $i \equiv j \pmod{o(g)}$. The smallest subgroup of G which contains g is

$$\{g^i \mid i \in \mathbb{Z}\},$$

it is called the cyclic subgroup generated by g and it is denoted by $\langle g \rangle$. We have that $o(g) = |\langle g \rangle|$.) Notice that $\sigma^j(a) = a + j$ for every $a \in \mathbb{Z}/n\mathbb{Z}$, and so σ^j is the identity map precisely when $n|j$. Hence, $o(\sigma) = n$. We also observe that τ^2 is the identity map (and τ is not identity), and so $o(\tau) = 2$. Applying these automorphisms one after another, we obtain that

$$\{\mathrm{id}, \sigma, \ldots, \sigma^{n-1}\} \cup \{\tau, \sigma\tau, \ldots, \sigma^{n-1}\tau\} \subseteq \mathrm{Aut}(X_n).$$

1.2 Lecture 2

1.2.1 Dihedral group (continuation)

In the previous lecture, we were studying the symmetries of an n-cycle. For $\phi \in \mathrm{Aut}(X_n)$, suppose $\phi(0) = j$. Then $\phi(0) = \sigma^j(0)$. Then $\sigma^{-j} \circ \phi$ is an automorphism of X_n which sends 0 to 0. Since the only neighbors of 0 are 1 and

-1. We obtain that $\sigma^{-j} \circ \phi(1)$ is either 1 or -1. Because $\tau(0) = 0$ and $\tau(-1) = 1$, we deduce that either

$$\sigma^{-j} \circ \phi(0) = 0 \text{ and } \sigma^{-j} \circ \phi(1) = 1, \tag{1.1}$$

or

$$\tau \circ \sigma^{-j} \circ \phi(0) = 0 \text{ and } \tau \circ \sigma^{-j} \circ \phi(1) = 1. \tag{1.2}$$

Rigidity. *Suppose $\theta \in \mathrm{Aut}(X_n)$, $\theta(0) = 0$, and $\theta(1) = 1$. Then θ is the identity map.*

Proof of the Rigidity Property. By induction on i, we show that $\theta(i) = i$. The base of induction follows from the assumption. Suppose $\theta(j) = j$ for every integer j in $[0, i]$. We have to show that $\theta(i+1) = i+1$. Notice that the only neighbors of i's are $i-1$ and $i+1$. By the induction hypothesis, $\theta(i) = i$, and so $\theta(i+1)$ is either $i-1$ or $i+1$. By the induction hypothesis $\theta(i-1) = i-1$, and so $\theta(i+1) \neq i-1$. Therefore, $\theta(i+1) = i+1$. This finishes the proof of the rigidity property. □

By the Rigidity Property, (1.1), and (1.2), we obtain that either

$$\sigma^{-j} \circ \phi = \mathrm{id}$$

or

$$\tau \circ \sigma^{-j} \circ \phi = \mathrm{id}\,.$$

The former implies that $\phi = \sigma^j$, and the latter implies that $\phi = \sigma^j \circ \tau$. Hence

$$\mathrm{Aut}(X_n) = \{\mathrm{id}, \sigma, \ldots, \sigma^{n-1}\} \cup \{\tau, \sigma\tau, \ldots, \sigma^{n-1}\tau\}.$$

To get a complete understanding of $\mathrm{Aut}(X_n)$, we have to compute $(\sigma^j \circ \tau) \circ \sigma^i$ and $(\sigma^j \circ \tau) \circ (\sigma^i \circ \tau)$. Notice that

$$(\sigma^j \circ \tau)(x) = \sigma^i(-x) = -x + j,$$

and so

$$((\sigma^j \circ \tau) \circ \sigma^i)(x) = (\sigma^j \circ \tau)(x+i) = -x - i + j = \sigma^{-i+j} \circ \tau(x).$$

This means $(\sigma^j \circ \tau) \circ \sigma^i = \sigma^{-i+j} \circ \tau$. Therefore,

$$(\sigma^j \circ \tau) \circ (\sigma^i \circ \tau) = \sigma^{-i+j}.$$

These equations give us a complete understanding of multiplication in $\mathrm{Aut}(X_n)$. One can use the particular equation, $\tau \circ \sigma = \sigma^{-1} \circ \tau$ in order to obtain the rest of the equations. For simplicity, we drop the $\circ$ notation. Notice that $\tau\sigma\tau^{-1} = \sigma^{-1}$ implies that $(\tau\sigma\tau^{-1})^i = \sigma^{-i}$ for every integer i. Hence,

$$\tau\sigma^i\tau^{-1} = \sigma^{-i}, \text{ and so } \sigma^{-i}\tau = \tau\sigma^i.$$

This group is called the dihedral group and it is denoted by D_{2n}. By the above argument, $D_{2n} = \langle\sigma\rangle \cup \langle\sigma\rangle\tau$, and so $\langle\sigma\rangle$ is a subgroup of order 2. Notice that for every i, j, the conjugation of σ^i by $\sigma^j\tau$ is

$$(\sigma^j\tau)\sigma^i(\sigma^j\tau)^{-1} = \sigma^j\tau\sigma^i\tau\sigma^{-j} = \sigma^j\sigma^{-i}\tau\tau\sigma^{-j} = \sigma^{-i}.$$

Hence $\langle\sigma\rangle$ is a *normal* subgroup of D_{2n}.

1.2.2 The automorphism group.

A symmetry of a group G is a bijection $f : G \to G$ which *preserves* properties of G. Let's recall that for two groups G and H, a function $f : G \to H$ is called a group *homomorphism* if $f(g_1g_2) = f(g_1)f(g_2)$ for every $g_1, g_2 \in G$. Notice that $f(e_G) = f(e_Ge_G) = f(e_G)f(e_G)$ implies that $f(e_G) = e_H$ where e_G and e_H are neutral elements of G and H, respectively. For every $g \in G$, we have

$$e_H = f(e_G) = f(gg^{-1}) = f(g)f(g^{-1}),$$

and so $f(g^{-1}) = f(g)^{-1}$. Hence, a group homomorphism *preserves* all the algebraic properties of a group. Hence, a symmetry of a group is a bijective group homomorphism from G to itself. Such a function is called an *automorphism* of G. The set of all automorphisms of G is denoted by $\mathrm{Aut}(G)$.

Lemma 1. *For a group G, the set $\mathrm{Aut}(G)$ forms a group under the function composition.*

Proof. The identity function id_G is in $\mathrm{Aut}(G)$, and it satisfies the properties of a neutral element with respect to the function composition.

For every $\theta \in \mathrm{Aut}(G)$, θ^{-1} exists as a function. Next we discuss why it is a group homomorphism. For every $g_1, g_2 \in G$, we have to show $\theta^{-1}(g_1g_2) = \theta^{-1}(g_1)\theta^{-1}(g_2)$. Notice that $\theta(\theta^{-1}(g_1g_2)) = g_1g_2$ and

$$\theta(\theta^{-1}(g_1)\theta^{-1}(g_2)) = \theta(\theta^{-1}(g_1))\theta(\theta^{-1}(g_2)) = g_1g_2.$$

By these equalities and the assumption that θ is a bijection, we obtain that $\theta^{-1}(g_1 g_2) = \theta^{-1}(g_1)\theta^{-1}(g_2)$. Hence, $\theta^{-1} \in \mathrm{Aut}(G)$.

It is easy to see that the composite of two group homomorphisms is a group homomorphism. □

1.2.3 Group action

Next formulate a setting for viewing a group G as symmetries of an object X. We say G *acts on* X and right $G \curvearrowright X$ if there is a function

$$m : G \times X \to X, \quad m(g, x) := g \cdot x$$

with the following properties:

1. For every $x \in X$, $e \cdot x = x$ where e is the neutral element of G.
2. For every $g_1, g_2 \in G$, and $x \in X$, $g_2 \cdot (g_1 \cdot x) = (g_1 g_2) \cdot x$.

1.3 Lecture 3.

1.3.1 Group actions (continuation)

An important meta-example is that the group of symmetries of an object X acts on X. We write the details for the special case of the symmetric group S_X.

Example 2 (Meta-example)**.** *For every object X, the group of symmetries of X acts on X. This meta-examples is the source of many examples. For instance, $S_X \curvearrowright X$, for a group G, $\mathrm{Aut}(G) \curvearrowright G$, and for a graph X, $\mathrm{Aut}(X) \curvearrowright V_X$ where V_X is the set of vertices of X. Next, we check the details of how S_X acts on X.*

Example 3. *Suppose X is a non-empty set. Then the following defines an action of the symmetric group S_X on X. For every $\sigma \in S_X$ and $x \in X$, let $\sigma \cdot x := \sigma(x)$.*

Proof. For every $x \in X$,

$$\mathrm{id}_X \cdot x = \mathrm{id}_X(x) = x,$$

and for every $\sigma_1, \sigma_2 \in S_X$,

$$\sigma_1 \cdot (\sigma_2 \cdot x) = \sigma_1(\sigma_2(x)) = (\sigma_1 \circ \sigma_2)(x) = (\sigma_1 \circ \sigma_2) \cdot x.$$

□

Example 4. *For every group G, the set of all automorphisms of G is denoted by $\mathrm{Aut}(G)$ and it is easy to see that it forms a group under the function composition. Then the following defines an action of $\mathrm{Aut}(G)$ on G: for every $\theta \in \mathrm{Aut}(G)$ and $x \in G$, $\theta \cdot x := \theta(x)$.*

Proof. □

Example 5 (Left-translations)**.** *Suppose G is a group and H is a subgroup of G. Then G acts on G/H by the left translations; that means for every $g \in G$ and $g'H \in G/H$, we let*

$$g \cdot (g'H) := (gg')H,$$

and it defines an action.

Proof. For every $g'H \in G/H$, we have

$$e \cdot (g'H) = (eg')H = g'H,$$

where e is the neutral element of G. For every $g_1, g_2 \in G$, and $gH \in G/H$, the following holds

$$g_1 \cdot (g_2 \cdot gH) = g_1 \cdot ((g_2 g)H) = (g_1(g_2 g))H = ((g_1 g_2)g)H = (g_1 g_2) \cdot (gH).$$

This shows that the given function is a group action of G on G/H. □

Example 6 (Conjugation)**.** *Suppose G is a group. Then G acts on itself by conjugation. That means for every $g \in G$ and $x \in G$, we set $g \cdot x := gxg^{-1}$, and this defines a group action of G on itself.*

Proof. For every $g \in G$, $e \cdot g = ege^{-1} = g$. For every $g_1, g_2, x \in G$, we have

$$g_1 \cdot (g_2 \cdot x) = g_1 \cdot (g_2 x g_2^{-1}) = g_1(g_2 x g_2^{-1})g_1^{-1} = (g_1 g_2)x(g_1 g_2)^{-1} = (g_1 g_2) \cdot x.$$

□

Example(Left-translation action on the space of functions) From every action on a finite set X, we can get a linear unitary action. For a finite set X, let

$$L^2(X) := \{f \mid f : X \to \mathbb{C}\},$$

and for $f \in L^2(X)$, let

$$\|f\|_2^2 := \sum_{x \in X} |f(x)|^2.$$

Notice that the set of functions $\{\delta_x \mid x \in X\}$ where

$$\delta_x(y) = \begin{cases} 1 & \text{if } y = x \\ 0 & \text{otherwise} \end{cases}$$

is an orthonormal basis of $L^2(X)$. It is easy to see that they are pairwise orthogonal, and for every $f \in L^2(X)$, we have

$$f = \sum_{x \in X} f(x)\delta_x;$$

and so $\dim_{\mathbb{C}} L^2(X) = |X|$.

Suppose G acts on X. Then the following defines an action of G on $L^2(X)$, and we say G acts on $L^2(X)$ by left-translations. For all $g \in G$, $f \in L^2(X)$, and $x \in X$,

$$(g * f)(x) := f(g^{-1} \cdot x).$$

We start by showing why this is an action. For every $f \in L^2(X)$ and $x \in X$,

$$(e * f)(x) = f(e^{-1} \cdot x) = f(e \cdot x) = f(x);$$

and so $e * f = f$. For every $g_1, g_2 \in G$, $f \in L^2(X)$, and $x \in X$, we have

$$\begin{aligned}(g_1 * (g_2 * f))(x) =& f(g_2^{-1} \cdot (g_1^{-1} \cdot x)) \\ =& f((g_2^{-1} g_1^{-1}) \cdot x) \\ =& f((g_1 g_2)^{-1} \cdot x) = ((g_1 g_2) * f)(x);\end{aligned}$$

and so $g_1 * (g_2 * f) = (g_1 g_2) * f$.

This is a linear action: for every $g \in G$, f_i's in $L^2(X)$, complex numbers c_i's, and $x \in X$, we have

$$\left(g * (\sum_i c_i f_i)\right)(x) = (\sum_i c_i f_i)(g^{-1} \cdot x) = \sum_i c_i f_i(g^{-1} \cdot x) = \sum_i c_i (g * f)(x);$$

and so

$$g * (\sum_i c_i f_i) = \sum_i c_i \, g * f_i.$$

Finally we argue that this action preserves the norm. This argument relies on the fact that if G acts on X, then

$$x \mapsto g \cdot x$$

is a permutation of X for every $g \in G$. We will prove this next. Here, we use this fact to show that $\|g * f\|_2 = \|f\|_2$ for every $f \in L^2(X)$ and $g \in G$. We have

$$\|g * f\|_2^2 = \sum_{x \in X} |(g * f)(x)|^2 = \sum_{x \in X} |f(g^{-1} \cdot x)|^2.$$

Since $g^{-1} \cdot x$'s as x ranges in X is just a reordering of x's, we have

$$\sum_{x \in X} |f(g^{-1} \cdot x)|^2 = \sum_{x \in X} |f(x)|^2 = \|f\|_2^2.$$

We say that this is a unitary action of G. These are extremely important examples in the subject of representation theory.

Example 7. *As part of your homework assignment, you will show that*

$$\mathrm{SL}_2(\mathbb{R}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R}, ad - bc = 1 \right\}$$

acts on the upper-half plane

$$\mathscr{H} := \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$$

via Möbius transformations:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z := \frac{az + b}{cz + d}.$$

1.3.2 Parametrizing group actions and Cayley's theorem

As we mentioned earlier, a group action of G on X gives us a way to think about G as symmetries of X. This suggests that the action is factoring through the natural action of the symmetries of X. The next result makes this more precise.

Theorem 8. *Suppose G is a group and X is a non-empty set. Then the following maps are bijections between the set $\mathrm{Act}(G, X)$ of actions of G on X and the set of group homomorphisms $\mathrm{Hom}(G, S_X)$ from G to the symmetric group S_X.*

$$\Phi : \mathrm{Act}(G, X) \to \mathrm{Hom}(G, S_X),\ ((\Phi(m))(g))(x) := m(g, x),$$

$$\Psi : \mathrm{Hom}(G, S_X) \to \mathrm{Act}(G, X),\ ((\Psi(f))(g, x) := (f(g))(x).$$

Moreover Φ and Ψ are inverse of each other.

The group homomorphism $\Phi(m)$ is called the *induced* homomorphism by the action $m : G \times X \to X$. Similarly, the action $\Psi(f)$ is called the *induced* group action by the group homomorphism $f : G \to S_X$.

1.4 Lecture 4

In the previous lecture, we mentioned the bijection between actions of G on a set X and group homomorphisms from G to S_X. We start today's lecture by an outline of that theorem.

Outline of proof of Theorem 8. **Step 1.** *Suppose $g \cdot x := m(g, x)$ is an action of G on X. Then for a fixed $g \in G$, $\sigma_g : X \to X, \quad \sigma_g(x) := g \cdot x$ is a bijection.*

Proof of Step 1. Notice that for all $x \in X$,

$$(\sigma_g \circ \sigma_{g^{-1}})(x) = g \cdot (g^{-1} \cdot x) = (gg^{-1}) \cdot x = e \cdot x = x;$$

similarly $\sigma_{g^{-1}} \circ \sigma_g = \mathrm{id}_X$, and so σ_g is invertible. Hence, it is a bijection. □

Step 2. *Suppose $g \cdot x := m(g, x)$ is an action of G on X.. Then the function $\phi_m : G \to S_X, \quad \phi_m(g) := \sigma_g$ is a group homomorphism.*

Proof of Step 2. We have already proved that ϕ_m is a function. Notice that for every $g_1, g_2 \in G$ and $x \in X$, we have

$$(\sigma_{g_1} \circ \sigma_{g_2})(x) = g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x = \sigma_{g_1 g_2}.$$

This means that $\phi_m(g_1)\phi_m(g_2) = \phi_m(g_1 g_2)$. Hence ϕ_m is a group homomorphism. □

Remark Steps 1-3 imply that $\Phi : \mathrm{Act}(G, X) \to \mathrm{Hom}(G, S_X), \quad \Phi(m) := \phi_m$ is a well-defined function.

Step 4. *Suppose $f : G \to S_X$ is a group homomorphism. For $g \in G$ and $x \in X$, let $g \cdot x := (f(g))(x)$. Then $\cdot$ defines an action of G on X.*

Proof of Step 4. Notice that since f is a group homomorphism, $f(e) = \mathrm{id}_X$. Hence, for every $x \in X$,

$$e \cdot x = f(e)(x) = \mathrm{id}_X(x) = x.$$

For every $g_1, g_2 \in G$, and $x \in X$, we have

$$g_1 \cdot (g_2 \cdot x) = f(g_1)(f(g_2)(x)) = (f(g_1) \circ f(g_2))(x) = f(g_1 g_2)(x) = (g_1 g_2) \cdot x.$$

This finishes the proof this step. □

Step 5. $\Psi \circ \Phi = \mathrm{id}$.

Proof of Step 5. Suppose $m : G \times X \to X$ is an action. Then we have to prove that $\Psi(\phi_m) = m$. For all $g \in G$ and $x \in X$, we have

$$\Psi(\phi_m)(g, x) := \phi_m(g)(x) = m(g, x);$$

and so $\Phi(\phi_m) = m$. □

Step 6. $\Phi \circ \Psi = \mathrm{id}$.

Proof of Step 6. Suppose $f : G \to S_X$ is a group homomorphism. We have to prove that for all $g \in G$ $\Phi(\Psi(f)(g)) = f(g)$. Notice that for all $x \in X$,

$$\Phi(\Psi(f)(g))(x) = \Psi(f)(g, x) = (f(g))(x).$$

This finishes the proof. □

□

An important special case of Theorem 8 is Cayley's theorem.

Theorem 9 (Cayley's theorem)**.** *Every group G can be embedded into S_G.*

A subgroup of a symmetric group is called a *permutation group*. Cayley's theorem says that every group group can be realized as a permutation group.

Proof of Theorem 9. Let $\phi : G \to S_G$ be the induced group homomorphism of the action of G on itself by left-translations. That means for every $g \in G$, let

$$\phi(g) := \sigma_g \quad \text{where} \quad \sigma_g : G \to G,\ \sigma_g(x) := gx.$$

Claim. *ϕ is injective.*

Proof of Claim. In order to show a group homomorphism is injective, it is necessary and sufficient to show that its kernel is trivial. Suppose g is in the kernel of ϕ. Then $\phi(g)(x) = x$ for all $x \in G$. Thie means $gx = x$ for all $x \in G$. Hence, $g = e$. □

□

Example 10. *Suppose G is a group which acts non-trivially on a set X and $|G| > |X|!$. Then G is not a simple group.*

Proof. Let $\phi : G \to S_X$ be the induced group homomorphism. Then $G/\ker\phi$ can be embedded into S_X. Since $|G| > |S_X|$ and $G \curvearrowright X$ non-trivially, we deduce that $\ker\phi$ is a non-trivial proper normal subgroup. Hence, G is not simple. □

1.5 Lecture 5

Example 11. *Suppose G is a finite group and p is the smallest prime factor of G. If H is a subgroup of G that is of index p, then H is a normal subgroup.*

Proof. Let $\phi : G \to S_p$ be the induced group homomorphism of the left-translation action of G on G/H. Notice that if g is in the kernel of ϕ, then $gH = H$; and so $g \in H$. This means the kernel of ϕ is a subgroup of H. Hence, $[G : \ker\phi]$ is a multiple of $[G : H] = p$. We also know that the order of the image of ϕ divides both $|G|$ and $|S_p|$. Since p is the smallest prime factor of $|G|$, $\gcd(|G|, p!) = p$. Therefore, $[G : \ker\phi]$ divides p. Altogether, we obtain that

$$[G : \ker\phi] = [G : H] = p \quad \text{and} \quad \ker\phi \subseteq H;$$

and so $H = \ker\phi$, which implies that H is a normal subgroup of G. □

For other applications, it is useful to understand the *kernel* of the action of G on G/H by left-translations. The *kernel* of an action $G \curvearrowright X$ is

$$\{g \in G \mid \forall x \in X, g \cdot x = x\}.$$

This is the same as the kernel of the induced group homomorphism of the given group action.

Lemma 12. *Suppose H is a subgroup of G. Then the following statements hold.*

1. *The kernel of action $G \curvearrowright G/H$ by left-translation is*

$$\mathrm{cor}_G(H) := \bigcap_{x \in G} xHx^{-1}.$$

   This is called the normal core *of H in G.*

2. *The normal core of H in G is the largest normal subgroup of G which is contained in H.*

Proof. Notice that g is in the kernel of the left-translation action on G/H if and only if for all $x \in G$, $gxH = xH$. Hence, g is in the kernel of this action precisely when $x^{-1}gx \in H$ for all $x \in G$. This is equivalent to saying that $g \in xHx^{-1}$ for all $x \in G$. Hence, the kernel of this action is

$$\mathrm{cor}_G(H) := \bigcap_{x \in G} xHx^{-1}.$$

Because, $\mathrm{cor}_G(H)$ is the kernel of the induced group homomorphism from G to $S_{G/H}$, it is a normal subgroup of G, and it is clearly a subgroup of H.

Next, suppose N is a normal subgroup of G and $N \subseteq H$. Then for all $x \in G$,

$$xNx^{-1} \subseteq xHx^{-1} \quad \text{which implies that} \quad N \subseteq xHx^{-1}.$$

Hence,

$$N \subseteq \bigcap_{x \in G} xHx^{-1} \quad \text{which means that} \quad N \subseteq \mathrm{cor}_G(H).$$

□

Chapter 2

Orbits, stabilizers, and fixed points

Suppose G acts on a set X. For a given $x \in X$, we can ask what points of X are *similar* to x via *symmetries* given by G. The set of points in X that are *G-similar* to x is called the *G-orbit of x*, and it is denoted by $G \cdot x$ or $\mathscr{O}_x$.

Some elements of G might not move x. The set

$$G_x := \{g \in G \mid g \cdot x = x\}$$

is called the stabilizer of x. Next we show that G_x is a subgroup of G; sometimes we refer to G_x as *the stabilizer subgroup of G* with respect to x.

Lemma 13. *Suppose G acts on X. Then for every x, the stabilizer of x is a subgroup of G.*

Proof. Notice that $e \cdot x = x$, and so $e \in G_x$. Suppose $g_1, g_2 \in G_x$. Then $g_2 \cdot x = x$. Applying g_2^{-1} to both sides, we obtain that

$$g_2^{-1} \cdot x = g_2^{-1} \cdot (g_2 \cdot x) = e \cdot x = x.$$

This implies that

$$g_1 \cdot (g_2^{-1} \cdot x) = g_1 \cdot x = x;$$

and so $(g_1 g_2^{-1}) \cdot x = x$. Hence, $g_1 g_2^{-1} \in G_x$. Therefore by the subgroup criterion, G_x is a subgroup of G. □

In general the stabilizer subgroups can vary drastically, but when x and y are in the same orbit, then the stabilizer subgroups are conjugates.

Lemma 14. *Suppose G acts on X. Then for every $g \in G$ and $x \in X$,*

$$G_{g\cdot x} = gG_xg^{-1}.$$

Proof. Notice that $g' \in G_{g\cdot x}$ if and only if $g' \cdot (g \cdot x) = (g \cdot x)$. Applying g^{-1} to both sides, we obtain that $g' \in G_{g\cdot x}$ exactly when

$$(g^{-1}g'g) \cdot x = x.$$

Hence, $g' \in G_{g\cdot x}$ precisely when $g^{-1}g'g \in G_x$. Conjugating the latter inclusion, we obtain that

$$g' \in G_{g\cdot x} \Leftrightarrow g' \in gG_xg^{-1}.$$

This means $G_{g\cdot x} = gG_xg^{-1}$. □

For a group action $G \curvearrowright X$ and $g \in G$, it is very useful to study the set of fixed points of g. We let

$$\mathrm{Fix}(g) := \{x \in X \mid g \cdot x = x\}$$

Sometimes we denote $\mathrm{Fix}(g)$ by X^g. There are tight relations between the collection $\{G_x\}_{x\in X}$ of the stabilizer groups and the collection $\{X^g\}_{g\in G}$ of the set of fixed points.

Lemma 15. *Suppose $G \curvearrowright X$. Then for all $g, g' \in G$,*

$$\mathrm{Fix}(gg'g^{-1}) = g \cdot \mathrm{Fix}(g');$$

in particular, $|\mathrm{Fix}(gg'g^{-1})| = |\mathrm{Fix}(g')|$.

Proof. Notice that $x \in \mathrm{Fix}(gg'g^{-1})$ if and only if $(gg'g^{-1}) \cdot x = x$. Applying g^{-1} to the both sides and using properties of group actions, we obtain that

$$g' \cdot (g^{-1} \cdot x) = g^{-1} \cdot x.$$

Hence, $x \in \mathrm{Fix}(gg'g^{-1})$ exactly when $g^{-1} \cdot x \in \mathrm{Fix}(g')$. Applying g to the both sides of the latter inclusion, we conclude that

$$x \in \mathrm{Fix}(gg'g^{-1}) \Leftrightarrow x \in g \cdot \mathrm{Fix}(g').$$

This implies that $\mathrm{Fix}(gg'g^{-1}) = g \cdot \mathrm{Fix}(g')$.

Since the action of g on X is a bijection, we have that $|g \cdot \mathrm{Fix}(g')| = |\mathrm{Fix}(g')|$.

□

Notice that the last statement means that $|\mathrm{Fix}(g)|$ only depends on the conjugacy class of g. A function on G is called a *class function* if its value at $x \in G$ depends only on the conjugacy class. By Lemma 15, for every group action $G \curvearrowright X$, $g \mapsto |\mathrm{Fix}(g)|$ is a class function.

Notice that the G-orbit of x is the set of all points that are *similar* to x, and so $\{\mathscr{O}_x\}_{x\in X}$ should be a partition. Next, we prove this statement.

Lemma 16. *Suppose G acts on x. Then for $x_1, x_2 \in X$, the following statements are equivalent.*

1. *For some $g \in G$, $x_2 = g \cdot x_1$.*
2. *$\mathscr{O}_{x_1} \cap \mathscr{O}_{x_2} \neq \varnothing$.*
3. *$\mathscr{O}_{x_1} = \mathscr{O}_{x_2}$.*

Proof. (1) $\Rightarrow$ (2). Notice that $x_2 = e \cdot x_2 \in \mathscr{O}_{x_2}$, and $x_2 = g \cdot x_1 \in \mathscr{O}_{x_1}$. Hence, $x_2 \in \mathscr{O}_{x_1} \cap \mathscr{O}_{x_2}$.

(2) $\Rightarrow$ (3). By symmetry it is enough to prove that $\mathscr{O}_{x_1} \subseteq \mathscr{O}_{x_2}$. (To be continued!) □

2.1 Lecture 6.

2.1.1 The Orbit-Stabilizer Theorem

In the previous lecture, we were in the middle of the proof of the following lemma.

Lemma 17. *Suppose G acts on x. Then for $x_1, x_2 \in X$, the following statements are equivalent.*

1. *For some $g \in G$, $x_2 = g \cdot x_1$.*
2. *$\mathscr{O}_{x_1} \cap \mathscr{O}_{x_2} \neq \varnothing$.*
3. *$\mathscr{O}_{x_1} = \mathscr{O}_{x_2}$.*

Proof. (1) $\Rightarrow$ (2). Notice that $x_2 = e \cdot x_2 \in \mathscr{O}_{x_2}$, and $x_2 = g \cdot x_1 \in \mathscr{O}_{x_1}$. Hence, $x_2 \in \mathscr{O}_{x_1} \cap \mathscr{O}_{x_2}$.

(2) $\Rightarrow$ (3). By symmetry it is enough to prove that $\mathscr{O}_{x_1} \subseteq \mathscr{O}_{x_2}$. Suppose $x \in \mathscr{O}_{x_1} \cap \mathscr{O}_{x_2}$. This means there are $g_1, g_2 \in G$ such that

$$x = g_1 \cdot x_1 \quad \text{and} \quad x = g_2 \cdot x_2.$$

Then for every $y \in \mathscr{O}_{x_1}$, the following holds.

$$\begin{aligned} y =& g \cdot x_1 \quad \text{for some } g \in G \\ =& g(\cdot g_1^{-1} \cdot x) \\ =& g(\cdot g_1^{-1} \cdot (g_2 \cdot x_2)) \\ =& (g g_1^{-1} g_2) \cdot x_2 \in \mathscr{O}_{x_2}. \end{aligned}$$

Hence $\mathscr{O}_{x_1} \subseteq \mathscr{O}_{x_2}$. Similarly we have that $\mathscr{O}_{x_2} \subseteq \mathscr{O}_{x_1}$. □

The set of all orbits is denoted by ${}_G\backslash^X$.

Lemma 18. *Suppose G acts on X. Then*

$${}_G\backslash^X := \{\mathscr{O}_x \mid x \in X\}$$

is a partition of X.

Proof. By Lemma 17, we have that two distinct orbits are disjoint. So it is remained to show that the union of elements of ${}_G\backslash^X$ is X. Notice that for every $x \in X$, $x = e \cdot x \in \mathscr{O}_x$. Hence x is the union of elements of ${}_G\backslash^X$. □

Lemma 18 implies that if X is a finite set, then

$$|X| = \sum_{\mathscr{O} \in {}_G\backslash^X} |\mathscr{O}|. \tag{2.1}$$

The function $\pi : X \to {}_G\backslash^X$, $\pi(x) := \mathscr{O}_x$ is called the *quotient map*. A function $s : {}_G\backslash^X \to X$ is called a *section* of the quotient map π if for every $\mathscr{O} \in {}_G\backslash^X$,

$$\mathscr{O}_{s(\mathscr{O})} = \mathscr{O}.$$

Alternatively, we can say the $s(\mathscr{O})$ is an element of $\mathscr{O}$. The existence of a section is based on the *axiom of choice*. It can be said that $\{s(\mathscr{O}) \mid \mathscr{O} \in {}_G\backslash^X\}$ is a set of *representatives* of G-orbits.

Notice that $|\mathscr{O}_x| = 1$ precisely when

$$x \in \mathrm{Fix}(G) := \{y \in X \mid \forall g \in G, g \cdot y = y\}.$$

The set of G-fixed points of X is also denoted by X^G.

Suppose s is a section of the quotient map $\pi : X \to_G \backslash^X$. Suppose

$$\{x_1, \ldots, x_k\} = \mathrm{Im}(s) \setminus \mathrm{Fix}(G).$$

This means $\{x_1, \ldots, x_k\}$ is a set of representatives of G-orbits that have at least two elements. Then by (2.1), we obtain

$$|X| = \sum_{x \in \mathrm{Im}(s)} |\mathscr{O}_x| = \sum_{x \in \mathrm{Fix}(G)} 1 + \sum_{i=1}^{k} |\mathscr{O}_{x_i}| = |\mathrm{Fix}(G)| + \sum_{i=1}^{k} |\mathscr{O}_{x_i}|. \tag{2.2}$$

Next, we learn how to find the cardinality of an orbit.

Theorem 19 (Orbit-stabilizer)**.** *Suppose G acts on X. Then the following is a bijection*

$$\theta : G/G_x \to \mathscr{O}_x, \quad \theta(gG_x) := g \cdot x.$$

Proof. **Well-defined**. First we discuss why θ is well-defined.

$$\begin{aligned} g_1 G_x = g_2 G_x &\Leftrightarrow g_2^{-1} g_1 \in G_x \\ &\Leftrightarrow (g_2^{-1} g_1) \cdot x = x \\ &\Leftrightarrow g_2 \cdot ((g_2^{-1} g_1) \cdot x) = g_2 \cdot x \\ &\Leftrightarrow g_1 \cdot x = g_2 \cdot x. \end{aligned}$$

Injective.

$$\begin{aligned} \theta(g_1 G_x) = \theta(g_2 G_x) &\Leftrightarrow g_1 \cdot x = g_2 \cdot x \\ &\Leftrightarrow (g_2^{-1} g_1) \cdot x = x \\ &\Leftrightarrow g_2^{-1} g_1 \in G_x \\ &\Leftrightarrow g_1 G_x = g_2 G_x. \end{aligned}$$

Surjective. For every $y \in \mathscr{O}_x$, there exists $g \in G$ such that $y = g \cdot x$, and so $y = \theta(gG_x)$. □

By the Orbit-Stabilizer Theorem, we obtain that if x is a finite set, then $|\mathscr{O}_x = [G : G_x]$ divides $|G|$. By (2.2), we have

$$|X| = |X^G| + \sum_{i=1}^{k} [G : G_{x_i}] \tag{2.3}$$

where x_i's are representative of G-orbits that have at least 2 elements.

2.1.2 Conjugacy classes and class equation

Consider the action of G on itself by conjugations. Then for every $x \in G$, the G-orbit of x is the conjugacy class $\mathrm{Cl}(x)$ of x. The stabilizer of x under the conjugation action is

$$G_x := \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\} = C_G(x)$$

the centralizer of x. Hence, by the orbit-stabilizer theorem, we have that for every $x \in G$

$$|\mathrm{Cl}(x)| = [G : C_G(x)].$$

Notice that

$$\mathrm{Fix}(G) := \{x \in G \mid \forall g \in G, gxg^{-1} = x\} = \{x \in G \mid \forall g \in G, gx = xg\} = Z(G)$$

is the center of G. Hence, by (2.3),

$$|G| = |Z(G)| + \sum_{i=1}^{k} [G : C_G(x_i)], \tag{2.4}$$

where x_i's are representative of conjugacy class that have at least 2 elements. The equation 2.4 is called the *class equation*.

2.1.3 Conjugates of a subgroup

Suppose G is a group. Let X be the set of all the subgroups of G. Notice that G acts on X by conjugation. Then for every subgroup H of G, the G-orbit of H is the set of all conjugates of H. The stabilizer of H is

$$N_G(H) := \{g \in G \mid gHg^{-1} = H\}.$$

This is called the *normalizer* of H in G. Then by the orbit-stabilizer theorem, we obtain that the number of conjugates of H is $[G : N_G(H)]$.

2.1.4 Action of finite p-groups.

Suppose P is a group and $|P| = p^n$ where p is a prime number and n is a positive integer. Suppose P acts on a finite set X. Then by (2.3),

$$|X| = |X^P| + \sum_{i=1}^{k} [P : P_{x_i}]$$

where x_i's are representatives of P-orbits that have at least 2 elements. Notice that $[P : P_{x_i}]$ divides $|P| = p^n$, and so $[P : P_{x_i}] = p^{n_i}$ for some non-negative integer $n_i \leq n$. Because the P-orbit of x_i has at least 2 elements, n_i is positive. Hence, $p|[P : P_{x_i}]$ for every i. Thus,

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

Let's summarize this in the next proposition.

Proposition 20. *Suppose P is a group, $|P| = p^n$ where p is prime and n is a positive integer, and P acts on a finite set X. Then*

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

This proposition plays an important role in proving Sylow theorems.

Chapter 3

Sylow's theorems

3.1 Lecture 6 (continue)

3.1.1 Cauchy's theorem

Theorem 21. *Suppose G is a finite group and p is a prime factor of $|G|$. Then G has an element of order p.*

This is one of the key properties of finite groups, and it will be used to prove Sylow's theorems. We would like to *solve* the equation $g^p = e$. For polynomial equations, one of the techniques of solving higher degree equations is to add new variables and create a *multi-linear* version of the equation. In the following proof, we use a similar idea.

Proof. Let $X := \{(g_0, \ldots, g_{p-1}) \in G^p \mid g_0 g_1 \cdots g_{p-1} = e\}$. Notice that after fixing the first $p-1$ components, we can solve for the last component and get a unique element

$$g_{p-1} := (g_0 \cdots g_{p-2})^{-1}.$$

Hence, $|X| = |G|^{p-1}$; in particular, p divides $|X|$.

Notice that if $(g_0, \ldots, g_{p-1}) \in X$, then $g_0 \cdots g_{p-1} = e$. Thus for every integer i in $[0, p-1]$,

$$e = (g_0 \cdots g_i)^{-1}(g_0 \ldots g_{p-1})(g_0 \cdots g_i) = g_{i+1} \cdots g_p g_0 \cdots g_i,$$

which means $(g_{i+1}, \ldots, g_{p-1}, g_0, \ldots, g_i) \in X$. Hence, the following defines an

action of $\mathbb{Z}/p\mathbb{Z}$ on X:

$$i \cdot (g_0, \ldots, g_{p-1}) := (g_i, \ldots, g_{p-1}, g_0, \ldots, g_{i-1}).$$

Therefore by Proposition 20,

$$|X| \equiv |X^{\mathbb{Z}/p\mathbb{Z}}| \pmod{p}.$$

Since $p||X|$, we deduce that $p||X^{\mathbb{Z}/p\mathbb{Z}}|$. Notice that

$$\begin{aligned}(g_0, \ldots g_{p-1}) \in X^{\mathbb{Z}/p\mathbb{Z}} &\Leftrightarrow \forall i \in \mathbb{Z}/p\mathbb{Z}, i \cdot (g_0, \ldots g_{p-1}) = (g_0, \ldots g_{p-1}), g_0 \cdots g_{p-1} = e \\ &\Leftrightarrow \forall i \in \mathbb{Z}/p\mathbb{Z}, g_i = g_0, g_0^p = e.\end{aligned}$$

In particular, $(e, \ldots, e) \in X^{\mathbb{Z}/p\mathbb{Z}}$. Because $|X^{\mathbb{Z}/p\mathbb{Z}}|$ is a multiple of p and at least 1, we deduce that $|X^{\mathbb{Z}/p\mathbb{Z}}| \geq p > 1$. Hence there exists $g \neq e$ such that $(g, \ldots, g) \in X^{\mathbb{Z}/p\mathbb{Z}}$. This implies that $o(g) = p$. □

3.2 Lecture 7.

The following is an important corollary of Cauchy's theorem.

Proposition 22. *Suppose G is a finite group and the order of every element is a power of a prime p. Then $|G|$ is a power of p.*

Proof. Suppose to the contrary that there exists a prime $\ell \neq p$ which divides $|G|$. Then by the Cauchy theorem, G has an element of order ℓ which is a contradiction as ℓ is not a power of p. □

A group G (not necessarily finite) is called a *p-group* if every the order of every element of G is a power of p. We just proved that the order of every finite p-group is a power of p. By Lagrange's theorem, if the order of a finite group is a power of a prime p, then G is a p-group.

Before we get to Sylow's thoerems, let's point out another application of important result on actions of finite p-groups, Proposition 20.

Lemma 23. *Suppose G is a finite p-group and N is a non-trivial normal subgroup of G. Then $Z(G) \cap N \neq \{1\}$ where $Z(G)$ is the center of G.*

Proof. Consider the action of G on N by conjugations. Then by Proposition 20, we have

$$|N| \equiv |N^G| \pmod{p}. \tag{3.1}$$

Since N is a non-trivial normal subgroup of G and $|G|$ is a power of p, p divides $|N|$. Therefore, by (3.1), $p||N^G|$. Notice that $x \in N^G$ if and only if $x \in N$ and for all $g \in G$, $gxg^{-1} = x$. This means $N^G = N \cap Z(G)$. Altogether, we obtain that p divides $|Z(G) \cap N|$. In particular, we deduce that $Z(G) \cap N \neq \{1\}$. □

The following result is an important consequence of Lemma 23. It will be used later to show that a finite p-group is *nilpotent*.

Corollary 24. *Suppose G is a group and $|G| = p^n$ for a prime p and positive integer n. Then $Z(G) \neq \{1\}$.*

3.2.1 The first and the second Sylow theorems.

By Lagrange's theorem, we know that if H is a subgroup of a finite group G, then $|H|$ divides $|G|$. We would like to understand to what extent the converse holds. By the Cauchy theorem, the converse holds for prime factors of $|G|$. We continue with the powers of primes, and will proceed inductively. Suppose p^k divides $|G|$, and we have already found a subgroup P_{k-1} of order p^{k-1}. Can we extend P_{k-1} further and find a subgroup P_k of order p^k?

Proposition 25 (Extension if there is room)**.** *Suppose G is a finite group, P is a p-subgroup of G where p is prime, and p divides $[G : P]$. Then the following statements hold.*

1. *The order of $N_G(P)/P$ is divisible by p.*
2. *There exists a subgroup Q of G such that $P \trianglelefteq Q$ and $|Q/P| = p$.*

Proof. (1) Let $X := G/P$ and consider the action of P on X by the left-translations. Then $|X| \equiv |X^P| \pmod{p}$. Notice that xP in X^P if and only if

$$\forall g \in P, gxP = xP \Leftrightarrow \forall g \in P, x^{-1}gx \in P \Leftrightarrow x^{-1}Px \subseteq P \Leftrightarrow x \in N_G(P).$$

Therefore $X^P = N_G(P)/P$. Because $p|[G : P]$, $p||X|$; and so $p||X^P|$. Hence, p divides $|N_G(P)/P|$. (2) Since P is a normal subgroup of $N_G(P)$, $N_G(P)/P$

is a group. By part (1), p divides the order of $N_G(P)/P$. Hence, by Cauchy's theorem, $N_G(P)/P$ has a subgroup $\overline{Q}$ of order p. By the correspondence theorem, there exists a subgroup Q of $N_G(P)$ which contains P and $\overline{Q} = Q/P$. Hence, P is a normal subgroup of Q and $|Q/P| = p$. □

Now, we are ready to prove Sylow's first theorem.

Theorem 26 (Sylow's first theorem)**.** *Suppose G is a finite group, p is a prime and p^k divides $|G|$. Then there exists a chain of subgroups*

$$P_1 \trianglelefteq P_2 \trianglelefteq \cdots \trianglelefteq P_k \leq G$$

such that $|P_i| = p^i$ for every integer $1 \leq i \leq k$.

Proof. We proceed by induction on k. The base of induction follows from Cauchy's theorem. The induction step follows from Proposition 25 (the proposition on *extension if there is room*). □

Suppose G is a finite group and p is a prime number. Suppose k is the largest non-negative integer such that p^k divides the order of $|G|$. Then a subgroup P of order p^k of G is called a *Sylow* p-subgroup of G. The set of all Sylow p-subgroups of G is denoted by $\mathrm{Syl}_p(G)$. By Sylow's first theorem, $\mathrm{Syl}_p(G)$ is always non-empty.

Notice that if θ is an automorphism of a finite group G and P is a Sylow p-subgroup of G, then $|\theta(P)| = |P|$; and so $\theta(P)$ is a Sylow p-subgroup of G, as well. This means the automorphism group of G acts on $\mathrm{Syl}(G)$.

Another remark is that starting with every p-subgroup of G, we can apply the *extension if there is room* Proposition repeatedly till we reach to a Sylow p-subgroup. This means every p-subgroup of G is contained in a Sylow p-subgroup. Next, we prove Sylow's second theorem which is a refiner version of this result.

Theorem 27 (Sylow's second theorem)**.** *Suppose G is a finite group, p is a prime, Q is a p-subgroup of G, and P_0 is a Sylow p-subgroup of G. Then there exists $x \in G$ such that $Q \subseteq xP_0x^{-1}$. In particular, Sylow p-subgroups are conjugate of each other.*

Proof. Let $X := G/P_0$ and consider the action of Q on G/P_0 by left-translations. Since Q is a finite p-group, by Proposition 20 we have

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

Since P_0 is a Sylow p-subgroup of G, $|G/P_0|$ is not a multiple of p. Hence, p does not divide $|X|$, which implies that p does not divide $|X^Q|$. In particular, X^Q is not empty. Suppose $xP_0 \in X^Q$. Then for all $g \in Q$, $gxP_0 = xP_0$. This holds precisely when

$$\forall g \in Q, x^{-1}gx \in P_0 \Leftrightarrow x^{-1}Qx \subseteq P_0 \Leftrightarrow Q \subseteq xP_0x^{-1}.$$

□

Notice that G acts on $\mathrm{Syl}_p(G)$ by conjugation. Because every two Sylow p-subgroups are conjugate, the G-action on $\mathrm{Syl}_p(G)$ has only one orbit. We say an action $G \curvearrowright X$ is *transitive* if there is only one orbit; alternatively we can say when every two points are G-similar. So we say the conjugation action of G on $\mathrm{Syl}_p(G)$ is transitive.

Corollary 28. *Suppose G is a finite group. Suppose G has a normal Sylow p-subgroup P. Then $\mathrm{Syl}_p(G) = \{P\}$.*

Proof. By Sylow's second theorem, every Sylow p-subgroup of G is a conjugate of P. Because P is a normal subgroup, $xPx^{-1} = P$ for all $x \in G$. Hence, $\mathrm{Syl}_p(G) = \{P\}$. □

Lemma 29. *Suppose G is a finite group and P is a Sylow p-subgroup. Then $\mathrm{Syl}_p(N_G(P)) = \{P\}$.*

Proof. Notice that P is a subgroup of $N_G(P)$ and $|N_G(P)/P|$ divides $|G/P|$. Since P is a Sylow p-subgroup, p does not divide $|G/P|$. Therefore, p does not divide $|N_G(P)/P|$. Thus, P is a Sylow p-subgroup of $N_G(P)$. Because P is a normal Sylow p-subgroup of $N_G(P)$, by the previous Corollary $\mathrm{Syl}_p(N_G(P)) = \{P\}$. □

Proposition 30. *Suppose G is a finite group and P is a Sylow p-subgroup. Then $N_G(N_G(P)) = N_G(P)$.*

Proof. For every $g \in G$, gPg^{-1} is a Sylow p-subgroup of G. Hence, by Lemma 29, $\mathrm{Syl}_p(N_G(gPg^{-1})) = \{gPg^{-1}\}$. Notice that $N_G(gPg^{-1}) = gN_G(P)g^{-1}$, and so for every $g \in N_G(N_G(P))$, we have $N_G(gPg^{-1}) = N_G(P)$. Therefore,

$$\{gPg^{-1}\} = \mathrm{Syl}_p(N_G(gPg^{-1})) = \mathrm{Syl}_p(N_G(P)) = \{P\}.$$

Hence, $gPg^{-1} = P$, which means $g \in N_G(P)$. This means

$$N_G(N_G(P)) \subseteq N_G(P).$$

Because $N_G(P) \subseteq N_G(N_G(P))$, the claim follows. □

3.3 Lecture 8.

Theorem 31 (Sylow's third theorem)**.** *Suppose p is a prime and G is a finite group. Then $|\mathrm{Syl}_p(G)| \equiv 1 \pmod{p}$.*

Proof. Suppose P_0 is a Sylow p-subgroup of G. If $P_0 = \{1\}$, there is nothing to prove. So suppose P_0 is a non-trivial p-group and consider the conjugation action of P_0 on $\mathrm{Syl}_p(G)$. Then by our main proposition on the action of finite p-groups, we have that

$$|\mathrm{Syl}_p(G)| \equiv |\mathrm{Syl}_p(G)^{P_0}| \pmod{p}. \tag{3.2}$$

Notice that $P \in \mathrm{Syl}_p(G)^{P_0}$ precisely when for all $g \in P_0$, $gPg^{-1} = P$, which means $g \in N_G(P)$. This means

$$\mathrm{Syl}_p(G)^{P_0} = \{P \in \mathrm{Syl}_p(G) \mid P_0 \subseteq N_G(P)\}.$$

Hence if P is fixed under conjugation by elements of P_0, then P_0 is a Sylow p-subgroup of $N_G(P)$. But by Lemma 29, $N_G(P)$ has only one Sylow p-subgroup and that is P. Therefore $\mathrm{Syl}_p(G)^{P_0} = \{P_0\}$. Hence, by (3.2),

$$|\mathrm{Syl}_p(G)| \equiv 1 \pmod{p}.$$

□

3.3.1 Groups of order pq

In this subsection, we assume that G is order pq where $p < q$ are two primes, and investigate its group structure.

Claim 1. *Prove that G has a unique Sylow q-subgroup, and so G has a normal subgroup of order q.*

Proof. Let Q be a Sylow q-subgroup. Then Q is of index p which is the smallest prime factor of $|G|$. Hence, Q is a normal subgroup. Let's give an alternative proof based on Sylow's theorems. The alternative approach is useful in other examples.

Let $s_q := |\mathrm{Syl}_q(G)|$. By Sylow's third theorem, $s_q \equiv 1 \pmod{q}$. By Sylow's second theorem, s_q is the number of conjugates of Q. Hence, $s_q = [G : N_G(Q)]$. In particlar, s_q divides $|G| = pq$. Thus, $s_q | pq$ and $q | s_q - 1$, which implies that $s_q = 1$ (notice that since $p < q$, $q \nmid p - 1$). This means Q is unique Sylow q-subgroup of G; and so Q is a characteristic subgroup (that means $\theta(Q) = Q$ for all $\theta \in \mathrm{Aut}(G)$.) Hence, Q is a normal subgroup of G. □

Notice that a group of prime order is cyclic, and so Q is cyclic; in particular, it is an abelian group. Whenever we have a normal abelain group, the following lemma can be useful.

Lemma 32. *Suppose G is a group and A is an abelian normal subgroup of G. Then the following defines an action of G/A on A, gives us a group homomorphism from G/A to $\mathrm{Aut}(A)$: $gA \cdot a := gag^{-1}$ and $\theta : G/A \to \mathrm{Aut}(A)$,*

$$\theta(gA)(a) := gag^{-1}.$$

Proof. We start by proving that θ is well-defined. If $g_1 A = g_2 A$, then $g_1^{-1} g_2 \in A$. Because A is abelian and $g_1^{-1} g_2$ is in A, for all $a \in A$, we have $g_1^{-1} g_2 a = a g_1^{-1} g_2$. Hence, $g_1 a g_1^{-1} = g_2 a g_2^{-1}$. This implies that θ is well-defined.

For every $g_1, g_2 \in G$ and every $a \in A$,

$$\begin{aligned}\theta((g_1A)(g_2A))(a) =& (g_1g_2)a(g_1g_2)^{-1} \\ =& g_1(g_2ag_2^{-1})g_1^{-1} = (\theta(g_1) \circ \theta(g_2))(a);\end{aligned}$$

and so θ is a group homomorphism. Therefore, by Theorem 8,

$$gA \cdot a := \theta(gA)(a) = gag^{-1}$$

is a group action.

Alternatively, we could have said that G acts on A by conjugation, and since A is abelian, it acts on itself trivially, which means A is in the kernel of this action. Therefore the conjugation action of G on A factors through G/A. The last sentence is in the spirit of the first isomorphism theorem, which says that

if $f : G \to H$ is a group homomorphism, then $\overline{f} : G/\ker f \to \mathrm{Im}(f)$ given by $\overline{f}(g \ker f) := f(g)$ is a well-defined isomorphism. Hence, if N is a normal subgroup of G and $N \subseteq \ker f$, then $gA \to f(g)$ is a well-defined group homomorphism as it is the composite of $\pi : G/A \to G/\ker f, \pi(gA) := g \ker f$ and $\overline{f}$. □

Notice that in our example, Q is a cyclic group of order q and $|G/Q| = p$, and so it is a cyclic group of order p. Hence θ induces a group homomorphism from C_p to $\mathrm{Aut}(C_q)$. Let's recall that $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \simeq (\mathbb{Z}/q\mathbb{Z})^\times$, and so it has $q-1$ elements. Therefore, if $p \nmid q-1$, then there is no non-trivial group homomorphism from C_p to $\mathrm{Aut}(C_q)$. This means the group homomorphism θ is trivial, which implies that for all $g \in G$ and $a \in Q$, $gag^{-1} = a$. Altogether, we obtain:
If $|G| = pq$, $p < q$ are primes and $p \nmid q$, then G has a unique Sylow q-subgroup Q and $Q \subseteq Z(G)$.

Next, we show that $G = PQ$. Let's recall that for two subgroups H and K of G, $HK := \{hk \mid h \in H, k \in K\}$.

Lemma 33. *Suppose G is a finite group and H and K are two subgroups of G. Then the following holds.*

1. $|HK| = \frac{|H||K|}{|H \cap K|}$.
2. *HK is a subgroup if and only if $HK = KH$.*

Proof. Let $f : H/(H \cap K) \to G/K$, $f(h(H \cap K)) := hK$. Then f is a well-defined injective function. For every $h_1, h_2 \in H$, we have

$$\begin{aligned} h_1(H \cap K) = h_2(H \cap K) &\Leftrightarrow h_2^{-1}h_1 \in H \cap K \\ &\Leftrightarrow h_2^{-1}h_1 \cap K \\ &\Leftrightarrow h_1K = h_2K. \end{aligned}$$

Notice that the image of f is HK/K. Therefore $|H/(H \cap K)| = |HK/K|$. Notice that $\bigcup_{h \in H} hK = HK$, and so HK/K is a partition of HK. Because all the left cosets of K have the same cardinality, we obtain that $|HK| = |K||HK/K|$. Thus $|HK| = |K||HK/K| = |K||H/(H \cap K)|$; and so $|HK| = \frac{|K||H|}{|H \cap K|}$.

We use the subgroup criterion to prove the second part. Because $1 \in H$ and $1 \in K$, $1 = 1 \cdot 1 \in HK$. Suppose $h_1, h_2 \in H$ and $k_1, k_2 \in K$. We have to show

that $(h_1k_1)(h_2k_2)^{-1}$ is in HK. We have $(h_1k_1)(h_2k_2)^{-1} = h_1(k_1k_2^{-1})h_2^{-1}$. Since $HK = KH$, there are $h' \in H$ and $k' \in K$ such that $(k_1k_2^{-1})h_2^{-1} = h'k'$. Thus

$$(h_1k_1)(h_2k_2)^{-1} = (h_1h')k' \in HK.$$

This implies that HK is a subgroup.

For the converse direction, notice that because HK is a subgroup, we have $(HK)^{-1} = HK$. Then $HK = (HK)^{-1} = K^{-1}H^{-1} = KH$. □

Notice that $|P \cap Q|$ divides $|P| = p$ and $|Q| = q$, and so $P \cap Q = \{1\}$. Hence, by the previous lemma, we have

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = pq = |G|.$$

This implies that $G = PQ$. Suppose $P = \langle a \rangle$ and $Q = \rangle b\langle$. Then $G = \{a^ib^j \mid 0 \leq i < p, 0 \leq j < q\}$. Let

$$\theta : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \to G, \quad \theta(i,j) := a^ib^j.$$

Then using the fact that $Q \subseteq Z(G)$, one can check that θ is a surjective group homomorphism. As $|G| = |\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}|$, we obtain that θ is an isomorphism. Therefore, by the Chinese Remainder Theorem, we deduce that G is cyclic. Here is the summary of what we have proved.

Lemma 34. *Suppose $p < q$ are primes, $p \nmid q - 1$, and G is a group of order pq. Then G is cyclic.*

We come back to the case where $p|q - 1$. Later, as part of your HW assignments, you will prove that every group of order n is cyclic if and only if $\gcd(n, \phi(n)) = 1$.

3.4 Lecture 9.

3.4.1 Groups of order $p(p-1)$

Suppose p is an odd prime and G is a group of order $p(p-1)$. Prove that G has a normal subgroup of order p.

By Sylow's third theorem, $s_p \equiv 1 \pmod{p}$ where $s_p := |\mathrm{Syl}_p(G)|$. By Sylow's second theorem, $s_p = [G : N_G(P)]$ where P is a Sylow p-subgroup. Hence, $s_p | [G : P]$. Altogether, we have $s_p | p-1$ and $p | s_p - 1$. The former implies that $s_p \leq p-1$. The only non-negative integer in the arithmetic progression $pk+1$ is 1. Therefore, $s_p = 1$. Because G has a unique Sylow p-subgroup P, it is a normal subgroup.

3.4.2 Groups of order $p(p+1)$

Prove that a group of order $p(p+1)$ has a normal subgroup of order either p or $p+1$.

Suppose G does not have a normal subgroup of order p. Hence it has more than one Sylow p-subgroup; this means $s_p > 1$. By Sylow's third theorem, $s_p \equiv 1 \pmod{p}$. Because $s_p > 1$, we obtain that $s_p \geq p+1$. By Sylow's second theorem, $s_p = [G : N_G(P)]$ where P is a Sylow p-subgroup. Therefore, s_p divides $[G : P]$, which implies that $s_p | p+1$. Because $s_p \geq p+1$ and $s_p | p+1$, we obtain that $s_p = p+1$. This implies that $[G : N_G(P)] = p+1 = [G : P]$; and so $N_G(P) = P$. Suppose $\mathrm{Syl}_p(G) = \{P_1, \ldots, P_{p+1}\}$. Because P_i's are cyclic groups of prime order, $P_i \setminus \{1\}$ are disjoint. Thus $|\bigcup_{i=1}^{p+1} P_i \setminus \{1\}| = (p+1)(p-1) = p^2 - 1$. Let

$$H := G \setminus (\bigcup_{i=1}^{p+1} P_i \setminus \{1\}).$$

Then $|H| = p(p+1) - (p^2-1) = p+1$. Notice that if $g \in P_i \setminus \{1\}$, then $o(g) = p$, and conversely if $g \in G$ is of order p, then $\langle g \rangle$ is a Sylow p-subgroup of G. Hence

$$H = \{g \in G \mid o(g) \neq p\}.$$

Since $o(g) = o(xgx^{-1})$ for every $x \in G$, H is a normal subset of G; that means $xHx^{-1} = H$ for all $x \in G$.

Claim 1. *If $h \in H \setminus \{1\}$, then $C_G(h) \cap P = \{1\}$.*

Proof of Claim 1. Suppose to the contrary that there exists $g \in (C_G(h) \cap P) \setminus \{1\}$. Because P is a cyclic group of order p, $\langle g \rangle = P$. Since h commutes with g, $h \in N_G(\langle g \rangle) = N_G(P)$. Earlier we showed that $N_G(P) = P$. Hence, $h \in P$, which is a contradiction. □

Claim 2. *If $h \in H \setminus \{1\}$, then $H \setminus \{1\} = \mathrm{Cl}(h)$, where $\mathrm{Cl}(h)$ is the conjugacy class of h.*

Proof of Claim 2. Suppose $P = \langle g \rangle$. By Claim 1, $g^i \notin C_G(h)$ if $g^i \neq 1$. Hence $h, ghg^{-1}, \ldots, g^{p-1}hg^{-p+1}$ are pairwise distinct conjugates of h; notice that if $g^i h g^{-i} = g^j h g^{-j}$, then $g^{i-j} \in C_G(h)$. Therefore $\mathrm{Cl}(h)$ has at least p elements. As $h \in H$ and H is a normal subset, $\mathrm{Cl}(h)$ is a subset of $H \setminus \{1\}$. Because

$$|H \setminus \{1\}| = p,\ \mathrm{Cl}(h) \subseteq H \setminus \{1\}, \quad \text{and} \quad p \leq |\mathrm{Cl}(h)|,$$

we obtain that $\mathrm{Cl}(h) = H \setminus \{1\}$. □

By Claim 2 and the fact that $|\mathrm{Cl}(h)| = [G : C_G(h)]$, we obtain $[G : C_G(h)] = p$. Therefore $|C_G(h)| = p + 1$. Since $p \nmid |C_G(h)|$, none of the elements of $C_G(h)$ are of order p. Hence $C_G(h) \subseteq H$. Because $|C_G(h)| = |H| = p + 1$, we conclude that $H = C_G(h)$; in particular H is a subgroup. This implies that H is a normal subgroup of order $p + 1$.

In fact, we have proved much more. We showed that if there is no normal subgroup of order p, then there is a normal subgroup H of order $p+1$ such that for all $h \in H \setminus \{1\}$, $\mathrm{Cl}(h) = H \setminus \{1\}$. In your HW assignment, you use this to show that in this case p is a Mersenne prime; that means $p = 2^n - 1$ for some positive integer n. You can show that in this case, $H \simeq (\mathbb{Z}/2\mathbb{Z})^n$ for some positive integer n. Moreover, there is an element g of order $p = 2^n - 1$ in $\mathrm{GL}_n(\mathbb{Z}/2\mathbb{Z})$ which gives us the action of G/H on H.

Chapter 4

Exact sequences

Using Sylow theorems, we often find a non-trivial normal subgroup N. Then we try to repeat this process for the group G/N. Considering $|N|$ and $|G/N|$ are smaller than $|G|$, presumably we have a better chance of understanding their group structures. Next, we try to see if we can *glue* the information on N and G/N together and understand the group structure of G. This takes us to the definition of exact sequences.

Definition 35. *A family of groups G_i and group homomorphisms $\phi_i : G_i \to G_{i+1}$, often written as*

$$G_1 \xrightarrow{\phi_1} G_2 \xrightarrow{\phi_2} \cdots \xrightarrow{\phi_n} G_{n+1},$$

is called an exact sequence *if $\mathrm{Im}(\phi_i) = \ker \phi_{i+1}$ for all i.*

An exact sequence of the form $1 \to G_1 \to G_2 \to G_3 \to 1$ is called a Short Exact Sequence*; we use the abbreviation SES.*

We say an SES $1 \to G_1 \xrightarrow{\phi_1} G_2 \xrightarrow{\phi_2} G_3 \to 1$ splits *if there exists a group homomorphism $\psi : G_3 \to G_2$ such that $\phi_2 \circ \psi = \mathrm{id}_{G_3}$. This is often represented by a diagram of the following form:*

$$1 \longrightarrow G_1 \xrightarrow{\phi_1} G_2 \underset{\psi}{\overset{\phi_2}{\rightleftarrows}} G_3 \longrightarrow 1$$

A homomorphism of between two SES

$$1 \to G_1 \xrightarrow{\alpha_1} G_2 \xrightarrow{\alpha_2} G_3 \to 1 \quad \textit{and} \quad 1 \to H_1 \xrightarrow{\beta_1} H_2 \xrightarrow{\beta_2} H_3 \to 1$$

is a triple $(\theta_1, \theta_2, \theta_3)$ of group homomorphisms, $\theta_i : G_i \to H_i$ such that the fol-

lowing is a commutative diagram.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G_1 & \xrightarrow{\alpha_1} & G_2 & \xrightarrow{\alpha_2} & G_3 & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \theta_1} & & \downarrow{\scriptstyle \theta_2} & & \downarrow{\scriptstyle \theta_3} & & \\ 1 & \longrightarrow & H_1 & \xrightarrow{\beta_1} & H_2 & \xrightarrow{\beta_2} & H_3 & \longrightarrow & 1 \end{array}$$

An isomorphism of SESs is a SES homomorphism which consists of group isomorphisms.

Notice that if N is a normal subgroup of a group G, then the following is a SES: $1 \to N \to G \to G/N \to 1$. We refer to such a SES as a *standard SES*.

4.1 Lecture 10.

4.1.1 Short exact sequences

Let's start by two observations.

Lemma 36 (Injectivity and surjectivity in terms of exact sequences)**.** *1. The sequence $1 \to G_1 \xrightarrow{\phi} G_2$ is an exact sequence if and only if ϕ is injective.*

2. The sequence $G_1 \xrightarrow{\phi} G_2 \to 1$ is an exact sequence if and only if ϕ is surjective.

Proof. (1) The sequence $1 \to G_1 \xrightarrow{\phi} G_2$ is an exact sequence if and only if the image of the embedding of the trivial group in G_1 is the same as the kernel of ϕ. This means the given sequence is an exact sequence precisely when $\ker \phi = \{1\}$. But a group homomorphism has a trivial kernel if and only if it is injective.

(2) The sequence $G_1 \xrightarrow{\phi} G_2 \to 1$ is an exact sequence if and only if the image of ϕ is the same as the kernel of group homomorphism which sends every element of G_2 to 1. This means the given sequence is exact precisely when the image of ϕ is G_2. □

Next we show that every SES is isomorphic to a standard SES.

Lemma 37. *Suppose $1 \to G_1 \xrightarrow{\phi_1} G_2 \xrightarrow{\phi_2} G_3 \to 1$ is a SES. Then it is isomorphic to the standard SES $1 \to \ker \phi_2 \to G_2 \to G_2/\ker \phi_2 \to 1$.*

Proof. Let's recall that by the first isomorphism theorem

$$\overline{\phi}_2 : G_2/\ker\phi_2 \to \mathrm{Im}(\phi_2), \quad \overline{\phi}_2(x\ker\phi_2) := \phi_2(x)$$

is a well-defined group isomorphism. Notice that $\mathrm{Im}(\phi_2) = G_3$, and let θ_3 be the inverse of $\overline{\phi}_2$; and so θ_3 is an isomorphism from G_3 to $G_2/\ker\phi_2$. Let $\theta_2 := \mathrm{Id}_{G_2}$ and

$$\theta_1 : G_1 \to \mathrm{Im}(\phi_1), \quad \theta_1(x) := \phi_1(x);$$

notice that since $\mathrm{Im}(\phi_1) = \ker\phi_2$, the codomain of θ_1 is $\ker\phi_2$. Let's also point out that because ϕ_1 is injective, so is θ_1. Furthermore the codomain of θ_1 is precisely its image, and so θ_1 is an isomorphism. Hence, $(\theta_1, \theta_2, \theta_3)$ is a triple of group isomorphisms. Next we argue why this is an isomorphism of SESs. Consider the first square in the following diagram.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G_1 & \xrightarrow{\phi_1} & G_2 & \xrightarrow{\phi_2} & G_3 & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle\theta_1} & & \downarrow{\scriptstyle\theta_2} & & \downarrow{\scriptstyle\theta_3} & & \\ 1 & \longrightarrow & \ker\phi_2 & \xrightarrow{\iota} & G_2 & \xrightarrow{\pi} & G_2/\ker\phi_2 & \longrightarrow & 1 \end{array}$$

For every $x \in G_1$, we have

$$\theta_2(\phi_1(x)) = \phi_1(x) = \theta_1(x) = \iota(\theta_1(x)),$$

which means this part of the diagram is commutative. Next consider the second square. For every $x \in G_2$, $\overline{\phi}_2(x\ker\phi_2) = \phi_2(x)$, and so $\theta_3(\phi_2(x)) = x\ker\phi_2$. Thus

$$\theta_3(\phi_2(x)) = x\ker\phi_2 = \pi(x) = \pi(\theta_2(x)).$$

Altogether, we have that this is commutative diagram, and so $(\theta_1, \theta_2, \theta_3)$ is an isomorphism of SESs. □

4.1.2 Splitting short exact sequences

Our next task is to investigate splitting SESs. Considering every SES is isomorphic to a standard SES, we find a necessary and sufficient for a standard SES splits.

Lemma 38 (Splitting criterion)**.** *Suppose N is a normal subgroup of G. Then the standard SES $1 \to N \to G \to G/N \to 1$ splits if and only if there exists a*

subgroup H of G such that $HN = G$ and $H \cap N = \{1\}$. Moreover for a finite group G, the condition $HN = G$ can be replaced with $|H| = |G/N|$.

Proof. ($\Rightarrow$) Because the given standard SES splits, there exists a group homomorphism $\psi : G/N \to G$ such that for all $x \in G$,

$$\psi(xN)N = xN. \tag{4.1}$$

Let $H := \mathrm{Im}(\psi)$. We claim that H satisfies the desired conditions. For all $x \in G$, (4.1) implies that $x = \psi(xN)n$ for some n. Hence, $x \in HN$, which means $G = HN$.

Suppose $x \in H \cap N$. Then $x = \psi(yN)$ for some $y \in G$, and so by (4.1), $yN = xN = N$. Therefore $x = \psi(N) = 1$. Thus $H \cap N = \{1\}$.

For a finite group G, $G = HN$ implies that $|G| = \frac{|H||N|}{|H \cap N|}$. Because $H \cap N = \{1\}$, we obtain that $|G| = |H||N|$, and so $|H| = |G/N|$.

($\Leftarrow$) As in the proof of Lemma 33, we have that

$$f : H/(H \cap N) \to HN/N, \quad f(h(H \cap N)) := hN$$

is a bijection. Since $H \cap N = \{1\}$ and $G = HN$, we can view f as a bijection from H to G/N. Because N is a normal subgroup, G/N is a group and f is a group homomorphism. Altogether, we obtain the $f : H \to G/N, f(h) := hN$ is a group isomorphism. Let $\psi : G/N \to G, \psi(gN) := f^{-1}(gN)$. Then ψ is a group homomorphism. For $g \in G$, suppose $h = \psi(gN)$. Then $f(h) = gN$, which means $hN = gN$. Therefore, for all $g \in G$, $\psi(gN)N = gN$. This means the given standard SES splits.

For a finite group G, if $|H| = |G/N|$, then

$$|HN| = \frac{|H||N|}{|H \cap N|} = |H||N| = |G/N||N| = |G|.$$

Because $HN \subseteq G$ and these sets have the same cardinality, we obtain that $G = HN$. Therefore $G = HN$ can be replaced with $|H| = |G/N|$. □

The conditions on the subgroup H can be thought of as finding a subgroup in the *transverse direction* of N. Having this in mind, we are going to use elements of H and N as a *coordinate system* for G.

Lemma 39. *Suppose $G = HN$ and $H \cap N = \{1\}$. Then the following is a bijection*

$$f : N \times H \to G, \quad g(n, h) := nh.$$

Proof. Since $G = HN$, $G = NH$; and so f is surjective. Suppose $f(n_1, h_1) = f(n_2, h_2)$. Then $n_1 h_1 = n_2 h_2$, and so

$$n_2^{-1} n_1 = h_2 h_1^{-1} \in N \cap H = \{1\}.$$

Thus $n_2^{-1} n_1 = h_2 h_1^{-1} = 1$, which implies that $(n_1, h_1) = (n_2, h_2)$. □

In the next lecture, write product of two elements of G using coordinates given by N and H.

4.2 Lecture 11.

4.2.1 Semidirect product

In the previous lecture, we showed that a standard

$$1 \to N \to G \to G/N \to 1$$

splits if and only if there exists a subgroup H of G such that $H \cap N = \{1\}$ and $HN = G$. Having such a subgroup, we showed that

$$f : N \times H \to G, f(n, h) := nh$$

is a bijection. For all $n_1, n_2 \in N$ and $h_1, h_2 \in H$, we have

$$f(n_1, h_1) f(n_2, h_2) = n_1 h_1 n_2 h_2 = n_1 (h_1 n_2 h_1^{-1}) h_1 h_2 = f(n_1 (h_1 n_2 h_1^{-1}), h_1 h_2).$$

Hence, to capture the group structure of G only in terms of N and H, we need to understand how to *conjugate* elements of N by elements of H. Notice that conjugation of elements of N by elements of H gives us a group homomorphism from H to $\mathrm{Aut}(N)$. This takes us to the definition of a semidirect product of two groups.

Lemma 40. *Suppose N and H are two groups and $f : H \to \mathrm{Aut}(N)$ is a group homomorphism. Consider the following operation on $N \times H$. For all $n_1, n_2 \in N$ and $h_1, h_2 \in H$, let*

$$(n_1, h_1) \cdot (n_2, h_2) := (n_1 f(h_1)(n_2), h_1 h_2).$$

Then this operation gives us a group, which is denoted by $N \rtimes_f H$ (or simply $N \rtimes H$ if f is clear from the context). This group is called a semidirect product *of N and H.*

We leave the proof of this lemma as an exercise, and only make a few computations.

Lemma 41. *Suppose $G := N \rtimes_\theta H$ is a semidirect product of N and H. Then $\iota_N : N \to G$, $\iota_N(n) := (n, 1)$, $\iota_H : H \to G$, $\iota_H(h) := (1, h)$, and $\pi : G \to H$, $\pi(n, h) := h$ are group homomorphisms. The group homomorphisms ι_N and ι_H are injective, and the group homomorphism π is surjective. For all $h \in H$ and $n \in N$,*

$$\iota_H(h)\iota_N(n)\iota_H(h)^{-1} = \iota_N(\theta(h)(n)).$$

Proof. For all $n_1, n_2 \in N$, we have

$$\iota_N(n_1)\iota(n_2) = (n_1, 1)(n_2, 1) = (n_1\theta(1)(n_2), 1) = (n_1 n_2, 1) = \iota_N(n_1 n_2).$$

For all $h_1, h_2 \in H$, we have

$$\iota_H(h_1)\iota_H(h_2) = (1, h_1)(1, h_2) = (1, \theta(h_1)(1), h_1 h_2) = (1, h_1 h_2) = \iota_H(h_1 h_2).$$

For all $n_1, n_2 \in N$ and $h_1, h_2 \in H$, we have

$$\pi((n_1, h_1)(n_2, h_2)) = \pi((n_1\theta(h_1)(n_2)), h_1 h_2) = h_1 h_2 = \pi(n_1, h_1)\pi(n_2, h_2).$$

For all $n \in N$ and $h \in H$, we have

$$\begin{aligned}\iota_H(h)\iota_N(n)\iota_H(h)^{-1} =& (1, h)(n, 1)(1, h^{-1}) = (1\theta(h)(n), hh^{-1}) \\ =& (\theta(h)(n), 1) = \iota_N(\theta(h)(n)).\end{aligned}$$

□

By Lemma 41, if θ is the trivial group homomorphism, then $N \rtimes_\theta H = N \times H$. If θ is a non-trivial group homomorphism, then there exist $n \in N$ and $h \in H$ such that

$$(1,h)(1,n) \neq (1,n)(1,h);$$

in particular, $N \rtimes_\theta H$ is not abelian and it is not isomorphic to $N \times H$.

Lemma 42. *Suppose N and H are two groups and $\theta : H \to \mathrm{Aut}(N)$ is a group homomorphism. Then the following is a splitting SES*

$$1 \to N \xrightarrow{\iota_N} N \rtimes_\theta H \xrightarrow{\pi} H \to 1.$$

Proof. Clearly ι_N is injective. By definition $\ker \pi = \mathrm{Im}(\iota_N)$ and π is surjective. Therefore the given sequence is a SES. Notice that $\pi \circ \iota_H = \mathrm{id}_H$, and so it is a splitting SES. □

Lemma 43. *Suppose $1 \to N \to G \to H \to 1$ is a splitting SES. Then there exist a group homomorphism $\theta : H \to \mathrm{Aut}(N)$ and an isomorphism $\phi : G \to N \rtimes_\theta H$ such that $(\mathrm{id}_N, \phi, \mathrm{id}_H)$ is an isomorphism of SES such that*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \longrightarrow & G & \longrightarrow & H & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{id}_N} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \mathrm{id}_H} & & \\ 1 & \longrightarrow & N & \xrightarrow{\iota_N} & N \rtimes_\theta H & \xrightarrow{\pi} & H & \longrightarrow & 1 \end{array}$$

Proof. Since every SES is isomorphic to a standard SES, without loss of generality we can and will assume that the given SES $1 \to N \to G \to H \to 1$ is a standard SES. Then by the Splitting Criterion, there exists a subgroup $\overline{H}$ of G such that $N\overline{H} = G$ and $N \cap \overline{H} = \{1\}$. Notice that the natural quotient map induces an isomorphism from $\overline{H}$ to H. Let $\theta : \overline{H} \to \mathrm{Aut}(N)$ be the group homomorphism given by conjugating elements of N by elements of $\overline{H}$. Then it is easy to see that $(n, \overline{h}) \mapsto n\overline{h}$ is a group isomorphism from $N \rtimes_\theta \overline{H}$ to G. The rest of the proof is left as an exercise. □

4.2.2 Groups of order pq, revisited.

Suppose G is a group of order pq where $p < q$ are primes. Let's recall that we have proved that G has a normal subgroup Q of order q and a subgroup P of order p. Then $P \cap Q = \{1\}$ and $|P| = |G/Q|$. Therefore the SES

$$1 \to Q \to G \to G/Q \to 1$$

splits. Hence, G is a semidirect product of Q and P. This means there exists a group homomorphism $\theta : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ such that $G \simeq \mathbb{Z}/p\mathbb{Z} \rtimes_\theta \mathbb{Z}/q\mathbb{Z}$. Because $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \simeq (\mathbb{Z}/q\mathbb{Z})^\times$ has $q-1$ elements, there is no non-trivial group homomorphism if $p \nmid q-1$. Hence, if $p \nmid q-1$, then $G \simeq \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$; and so by the Chinese Remainder Theorem, $G \simeq \mathbb{Z}/pq\mathbb{Z}$ if $p \nmid q-1$.

If $p|q-1$, then $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ has an element of order p. Hence there is non-trivial group homomorphism $\theta : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$. This implies that

$$(\mathbb{Z}/q\mathbb{Z}) \rtimes_\theta (\mathbb{Z}/p\mathbb{Z})$$

is a non-abelian group of order pq.

4.2.3 Schur-Zassenhaus theorem

The next theorem is a strong tool to understand structure of many finite groups.

Theorem 44. *Suppose N and H are two finite groups and $\gcd(|N|, |H|) = 1$. Then every SES of the form*

$$1 \to N \to G \to H \to 1$$

splits.

To Prove Theorem 44, we make a few reductions and show that it is enough to prove the case where N is abelian. The abelian case can be handled using basics of cohomology theory, and it is left as a HW assignment.

Lemma 45. *To prove Theorem 44, it is enough to show that the following holds. Suppose G is a finite group and N is a normal subgroup such that*

$$\gcd(|N|, |G/N|) = 1. \tag{4.2}$$

Then there exists a subgroup H of G such that $|H| = |G/N|$.

Proof. Since every SES is isomorphic to a standard SES, without loss of generality we can and will assume that

$$1 \to N \to G \to H \to 1$$

is a standard SES. Then $\gcd(|N|, |H|) = 1$ implies that N is a normal subgroup of G which satisfies (4.2). Hence by the assumption, G has a subgroup $\overline{H}$ such that $|\overline{H}| = |G/N|$. Since $\gcd(|N|, |G/N|) = 1$, we obtain that $\gcd(|N|, |\overline{H}|) = 1$. Therefore, $N \cap \overline{H} = \{1\}$. Thus by the Splitting Criterion,

$$1 \to N \to G \to G/N \to 1$$

splits. □

Theorem 46 (Schur-Zassenhaus: 2nd version)**.** *Suppose G is a finite group and N is a normal subgroup of G such that $\gcd(|N|, |G/N|) = 1$. Then there exists a subgroup H of G such that $|H| = |G/N|$.*

Proof. We proceed by strong induction on $|G|$.

Step 1. *it is enough to prove the case where N is a minimal normal subgroup.*

If N is not a minimal normal subgroup, then there exists a non-trivial normal subgroup N_0 of G such that N_0 is a proper subgroup of N.

Let $\overline{G} := G/N_0$ and $\overline{N} := N/N_0$. Then

$$|\overline{G}/\overline{N}| = \left|\frac{G/N_0}{N/N_0}\right| = |G/N|, \quad \text{and so} \quad \gcd(|\overline{N}|, |\overline{G}/\overline{N}|) = 1 \quad \text{as} \quad |\overline{N}||N|. \tag{4.3}$$

Therefore by the strong induction hypothesis, there exists a subgroup $\overline{H}$ of $\overline{G}$ such that

$$|\overline{H}| = |\overline{G}/\overline{N}| = |G/N|. \tag{4.4}$$

By the correspondence theorem, there exists a subgroup $\widetilde{H}$ of G which contains N_0 as a normal subgroup such that $\overline{H} = \widetilde{H}/N_0$. Then

$$|\widetilde{H}/N_0| = |\overline{H}| = |G/N| \quad \text{and} \quad |N_0||N|; \quad \text{and so} \quad \gcd(|N_0|, |\widetilde{H}/N_0|) = 1.$$

Thus by the strong induction hypothesis, there exists a subgroup H of $\widetilde{H}$ such that $|H| = |\widetilde{H}/N_0| = |G/N|$. This gives us the desired subgroup. Hence, without loss of generality, we can and will assume that N is a *minimal* normal subgroup. □

4.3 Lecture 12

Proof of Theorem 44; continue. **Step 2.** *it is enough to prove the case where N is a minimal normal subgroup and p-group.*

Proof of Step 2. Suppose p is a prime factor of N, and P is a Sylow p-subgroup of N. By Frattini's argument, $G = N_G(P)N$. (Frattini's argument was part of your HW assignment. Here is an overview of its proof. For all $g \in G$, gPg^{-1} is a Sylow p-subgroup of N. Hence there exists $n \in N$ such that $gPg^{-1} = nPn^{-1}$. This implies that $n^{-1}g \in N_G(P)$.) Suppose N is not a p-group. Then P is a proper subgroup of N. Because N is a minimal normal subgroup of G and P is a proper subgroup of N, P is not a normal subgroup of G. This means $N_G(P)$ is a proper subgroup of G. Because $G = N_G(P)N$, we have

$$\frac{G}{N} = \frac{N_G(P)N}{N} \simeq \frac{N_G(P)}{N_G(P) \cap N}. \tag{4.5}$$

Notice that $|N_G(P) \cap N|$ divides $|N|$ and $\gcd(|N|, |G/N|) = 1$, by (4.5) we obtain that $\gcd(|N_G(P) \cap N|, |N_G(P)/N_G(P) \cap N|) = 1$. Therefore, by the strong induction hypothesis, we deduce that there exists a subgroup H of $N_G(P)$ such that $|H| = |N_G(P)/(N_G(P) \cap N)|$; and so by (4.5), we obtain that H is a subgroup of G which has order G/N. So if N is a minimal normal subgroup which is not a p-group, then we obtain the desired subgroup H. □

Step 3. *A minimal normal subgroup N which is a p-group is abelian.*

Proof of Step 3. Since N is a p-group, $Z(N)$ is a non-trivial subgroup. Because N is a normal subgroup of G and $Z(N)$ is a characteristic subgroup of N, $Z(N)$ is a normal subgroup of G. (This statement was part of your HW assignment. Here we give an overview of this argument. For every automorphism θ of N, $x \in Z(N)$, and $y \in N$, we have

$$y\theta(x)y^{-1} = \theta(\theta^{-1}(y)x\theta^{-1}(y)^{-1}) = \theta(x).$$

Therefore $\theta(Z(N)) = Z(N)$. For all $g \in G$, let $c_g : N \to N, c_g(n) := gng^{-1}$. Then $c_g \in \mathrm{Aut}(N)$; and so $c_g(Z(N)) = Z(N)$, which implies that $Z(N)$ is a normal subgroup of G.) Since $Z(N)$ is a non-trivial normal subgroup of G, $Z(N)$ is a subgroup of N, and N is a minimal normal subgroup of G, we obtain that $Z(N) = N$. This means N is abelian. □

By Step 2 and Step 3, we can and will assume that N is abelian. The abelian case of Schur-Zassenhaus theorem can be proved using cohomological techniques, and it is part of your HW assignment. □

The converse of Schur-Zassenhaus theorem is correct as well. This means if $\gcd(m,n) \neq 1$, then there exist groups H and N and a non-splitting SES

$$1 \to N \to G \to H \to 1,$$

and $|N| = n$ and $|H| = m$. Suppose p is a prime factor which divides $\gcd(m,n)$. Then

$$0 \to \frac{\mathbb{Z}}{p\mathbb{Z}} \oplus \frac{\mathbb{Z}}{(n/p)\mathbb{Z}} \to \frac{\mathbb{Z}}{p^2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{(n/p)\mathbb{Z}} \oplus \frac{\mathbb{Z}}{(m/p)\mathbb{Z}} \to \frac{\mathbb{Z}}{p\mathbb{Z}} \oplus \frac{\mathbb{Z}}{(m/p)\mathbb{Z}} \to 0$$

is a non-splitting SES. To understand this example better, it is easier to think about only the following SES

$$0 \to \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \to 0.$$

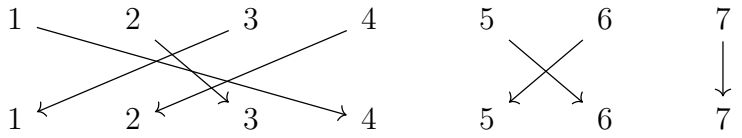
Chapter 5

Symmetric groups

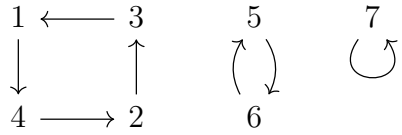
Given a permutation $\sigma \in S_n$, we can visualize it in different ways. For instance, we can use a directed bipartite graph where the vertices of each part are labelled by integers $1, \ldots, n$ and we connect i to $\sigma(i)$ for all i. The other method is to use a directed graph with vertices labelled by integers $1, \ldots, n$ and connecting i to $\sigma(i)$ for all i. For instance the graphs attached to the permutation

$$\sigma(1) = 4,\ \sigma(2) = 3,\ \sigma(3) = 1,\ \sigma(4) = 2,\ \sigma(5) = 6,\ \sigma(6) = 5,\ \sigma(7) = 7$$

are



and



In the second method, the outward degree of every vertex is 1 and the inward degree of every vertex is 1. Hence it consists of finitely many closed directed closed cycles. One can think about this graph as a flow where powers of σ takes us. Therefore the vertices of a connected component of this graph is an orbit of $\langle\sigma\rangle$. So the number of connected components of this graph is the number of orbits of the action of $\langle\sigma\rangle$ on $[1..n]$. For a permutation σ, let

$$\mathrm{Fix}(\sigma) := \{i \in [1..n] \mid \sigma(i) = i\},$$

and

$$\mathrm{Supp}(\sigma) := [1..n] \setminus \mathrm{Fix}(\sigma).$$

We call $\mathrm{Supp}(\sigma)$ the *support* of σ. Notice that if σ fixes $n-1$ points in $[1..n]$, then it should be the identity function. This means $\mathrm{Supp}(\sigma)$ can never have only one point.

Two permutations σ_1 and σ_2 are called *disjoint* if $\mathrm{Supp}(\sigma_1) \cap \mathrm{Supp}(\sigma_2) = \varnothing$. Thinking about a permutation as a *card shuffler*, two permutations are disjoint if the *shufflers* are handling two separate parts of deck of cards. So it is clear that these shufflers can do their jobs in a parallel fashion. This means these permutations commute.

Lemma 47. *Suppose $\sigma_1, \sigma_2 \in S_n$ are disjoint permutations. Then the following statements hold.*

1. $\sigma_1\sigma_2 = \sigma_2\sigma_1$.
2. $\mathrm{Supp}(\sigma_1\sigma_2) = \mathrm{supp}(\sigma_1) \cup \mathrm{Supp}(\sigma_2)$.

Proof. For all $i \notin \mathrm{Supp}(\sigma_1) \cup \mathrm{Supp}(\sigma_2)$, i is fixed by both σ_1 and σ_2. Hence $\sigma_1(\sigma_2(i)) = i$ and $\sigma_2(\sigma_1(i)) = i$. In particular,

$$\mathrm{Fix}(\sigma_1) \cap \mathrm{Fix}(\sigma_2) \subseteq \mathrm{Fix}(\sigma_1\sigma_2); \quad \text{and so} \quad \mathrm{Supp}(\sigma_1\sigma_2) \subseteq \mathrm{supp}(\sigma_1) \cup \mathrm{Supp}(\sigma_2).$$

For all $i \in \mathrm{Supp}(\sigma_1)$, $i \in \mathrm{Fix}(\sigma_2)$ as σ_1 and σ_2 are disjoint. Therefore $\sigma_1(i)$ is also in the support of σ_1, and so it is fixed by σ_2. Thus,

$$\sigma_1(\sigma_2(i)) = \sigma_1(i) \neq i \quad \text{and} \quad \sigma_2(\sigma_1(i)) = \sigma_1(i) \neq i.$$

By a similar argument, for all i in the support of $\mathrm{Supp}(\sigma_2)$, we have

$$\sigma_1(\sigma_2(i)) = \sigma_2(\sigma_1(i)) \neq i.$$

Altogether we have $\sigma_1\sigma_2 = \sigma_2\sigma_1$ and $\mathrm{supp}(\sigma_1) \cup \mathrm{Supp}(\sigma_2) \supseteq \mathrm{Supp}(\sigma_1\sigma_2)$. □

By induction we obtain the following corollary.

Corollary 48. *Suppose $\sigma_1, \ldots, \sigma_k \in S_n$ are pairwise disjoint permutations. Then σ_i's commute and*

$$\mathrm{Supp}(\sigma_1 \cdots \sigma_k) = \bigcup_{i=1}^{k} \mathrm{Supp}(\sigma_i).$$

Lemma 49. *Suppose $\sigma_1, \ldots, \sigma_k \in S_n$ are pairwise disjoint permutations. Then for every i*

$$(\sigma_1 \cdots \sigma_k)|_{\mathrm{Supp}(\sigma_i)} = \sigma_i|_{\mathrm{Supp}(\sigma_i)}.$$

Proof. For every $x \in \mathrm{Supp}(\sigma_i)$, x is fixed by σ_j's for all $j \neq i$. Then

$$(\sigma_1 \cdots \sigma_k)(x) = \sigma_i((\sigma_1 \cdots \sigma_{i-1}\sigma_{i+1} \cdots \sigma_k)(x)) = \sigma_i(x).$$

□

Corollary 50. *Suppose $\sigma_1, \ldots, \sigma_k \in S_n$ are pairwise disjoint permutations and X is a subset of $[1..n]$ that has at least two elements. Then X is an orbit of $\langle \sigma_1 \cdots \sigma_k \rangle$ if and only if X is an orbit of $\langle \sigma_i \rangle$ for some i.*

Proof. ($\Rightarrow$) Suppose $x \in X$. Since $|X| \geq 2$ and X is an orbit of $\langle \sigma_1 \cdots \sigma_k \rangle$, x is in the support of $\sigma_1 \cdots \sigma_k$. Hence x is in the support of σ_i for some i. Since

$$\sigma_1 \cdots \sigma_k|_{\mathrm{Supp}(\sigma_i)} = \sigma_i|_{\mathrm{Supp}(\sigma_i)},$$

and $\mathrm{Supp}(\sigma_i)$ is invariant under $\sigma_1 \cdot \sigma_k$ and σ_i, we deduce that $X \subseteq \mathrm{Supp}(\sigma_i)$. ($\Leftarrow$) Suppose $x \in X$. Since $|X| \geq 2$ and X is an orbit of $\langle \sigma_i \rangle$, x is in the support of σ_i. The rest of the argument is similar to the previous case. □

5.1 Lecture 13

A permutation σ is called a cycle if

$$\sigma(i_1) = i_2,\ \sigma(i_2) = i_3, \ldots, \sigma(i_k) = i_1$$

for some i_j's and $\mathrm{Supp}(\sigma) = \{i_1, \ldots, i_k\}$; in particular, $k \geq 2$. Such a cycle is called a k-cycle and we say its length is k. This cycle is denoted by

$$(i_1\ i_2\ \cdots\ i_k).$$

For $\sigma \in S_n$ and an orbit $\mathscr{O}$ of $\langle \sigma \rangle$, we have that

$$\mathscr{O} = \{i, \sigma(i), \ldots, \sigma^{k-1}(i)\}$$

and so $\sigma|_{\mathscr{O}} = \tau_{\mathscr{O}}$ where

$$\tau_{\mathscr{O}} = (i\ \sigma(i)\ \cdots\ \sigma^{k-1}(i)).$$

If $|\mathscr{O}| = 1$, we let $\tau_{\mathscr{O}} = \mathrm{id}$. Let

$$\langle\sigma\rangle\backslash^{[1..n]} = \{\mathscr{O}_1, \ldots, \mathscr{O}_k\}.$$

Then $\tau_{\mathscr{O}_i}$'s are disjoint cycles. Using Corollary 50, it is easy to see that

$$\sigma = \tau_{\mathscr{O}_1} \cdots \tau_{\mathscr{O}_k}.$$

We refer to such a decomposition as a *cycle decomposition*. In the converse direction, if $\sigma = \tau_1 \cdots \tau_k$ and τ_i's are disjoint cycles, then $\mathrm{Supp}(\tau_i)$ is an orbit of $\langle\tau_i\rangle$. Hence by Corollary 50, $\mathrm{Supp}(\tau_i)$ is an orbit $\mathscr{O}_i$ of σ. By Lemma 49, $\tau_i = \tau_{\mathscr{O}_i}$. This shows that a cycle decomposition is unique up to reordering the terms. Altogether, we have proved the following theorem.

Theorem 51. *Every permutation can be written as a product of disjoint cycles, and this decomposition is unique up to reordering the terms.*

The cycle type of a permutation $\sigma \in S_n$ is the cardinality of the orbits of $\langle\sigma\rangle$. Since these orbits form a partition of $[1..n]$, the cycle type of σ is a partition of n; that means the cycle type of σ is a decreasing sequence $a_1 \geq a_2 \geq \cdots \geq a_l$ of positive integers such that

$$a_1 + \cdots + a_l = n.$$

Next we show that there exists a bijection between partitions of n and conjugacy classes of S_n. To this end, we compute the conjugate of a cycle by σ.

Lemma 52. *Suppose $\sigma \in S_n$ and $(i_1 \ \cdots \ i_k)$ is a k-cycle. Then*

$$\sigma(i_1 \ \cdots \ i_k)\sigma^{-1} = (\sigma(i_1) \ \cdots \ \sigma(i_k)).$$

Proof. Let $\tau := (i_1 \ \cdots \ i_k)$. Then

$$\mathrm{Fix}(\sigma\tau\sigma^{-1}) = \sigma(\mathrm{Fix}(\tau)) = [1..n] \setminus \{\sigma(i_1), \ldots, \sigma(i_k)\}.$$

So it is enough to understand the restriction of $\sigma\tau\sigma^{-1}$ on $\{\sigma(i_1), \ldots, \sigma(i_k)\}$. Notice that

$$\sigma\tau\sigma^{-1}(\sigma(i_j)) = \sigma\tau(i_j) = \sigma(i_{j+1})$$

for $j < k$ and $\sigma\tau\sigma^{-1}(\sigma(i_k)) = \sigma(i_1)$. □

Suppose $\sigma = \tau_1 \cdots \tau_k$ is a cycle decomposition of σ. Then for every $\gamma \in S_n$ we have

$$\gamma\sigma\gamma^{-1} = (\gamma\tau_1\gamma^{-1}) \cdots (\gamma\tau_k\gamma^{-1}),$$

and by the previous lemma, $\gamma\tau_j\gamma^{-1}$ is a cycle and

$$\mathrm{Supp}(\gamma\tau_j\gamma^{-1}) = \gamma(\mathrm{Supp}(\tau_j)).$$

We also notice that if $\mathscr{O}$ is an orbit of $\langle\sigma\rangle$, then $\gamma(\mathscr{O})$ is an $\langle\gamma\sigma\gamma^{-1}\rangle$-orbit. Because $|\mathscr{O}| = |\gamma(\mathscr{O})|$ for every $\langle\sigma\rangle$-orbit $\mathscr{O}$, we deduce that σ and $\gamma\sigma\gamma^{-1}$ have the same cycle types.

Conversely suppose σ_1 and σ_2 have the same cycle type $j_1, \ldots, j_k$. Then there are two reordering

$$a_{11}, \ldots, a_{1j_1}, a_{21}, \ldots, a_{2j_2}, \ldots, a_{k1}, \ldots, a_{kj_k}$$

and

$$b_{11}, \ldots, b_{1j_1}, b_{21}, \ldots, b_{2j_2}, \ldots, b_{k1}, \ldots, b_{kj_k}$$

of the numbers $1, \cdots, n$, such that

$$\sigma_1 = (a_{11} \ \ldots \ a_{1j_1})(a_{21} \ \ldots \ a_{2j_2}) \cdots (a_{k1} \ \ldots \ a_{kj_k})$$

and

$$\sigma_2 = (b_{11} \ \ldots \ b_{1j_1})(b_{21} \ \ldots \ b_{2j_2}) \cdots (b_{k1} \ \ldots \ b_{kj_k}).$$

Then $\gamma : [1..n] \to [1..n], \gamma(a_{ij}) := b_{ij}$ is a well-defined permutation and

$$\sigma_2 = \gamma\sigma_1\gamma^{-1}.$$

Altogether we have proved the following result.

Theorem 53. *Two elements of S_n are conjugate if and only if they have the same cycle type.*

5.2 Lecture 14

An important relation between elements of S_n is given by the following lemma.

Lemma 54 (Linking relation)**.** *For every distinct numbers* $a_1, \ldots, a_{l+k}$ *in* $[1..n]$*, where* l, k *are integers more than* 1*, we have*

$$(a_1 \cdots a_k)(a_k \cdots a_{k+l}) = (a_1 \cdots a_{k+l}).$$

Proof. Let σ_1 be the k-cycle $(a_1 \cdots a_k)$ and σ_2 be the l-cycle $(a_{k+1} \cdots a_{k+l})$. Then

$$\mathrm{Supp}(\sigma_1\sigma_2) \subseteq \mathrm{Supp}(\sigma_1) \cup \mathrm{Supp}(\sigma_2) = \{a_1, \ldots, a_{k+l}\}.$$

So to determine $\sigma_1\sigma_2$, we can focus only on a_j's. For every j in $[1..(k-1)]$, a_j is fixed by σ_2, which implies that

$$\sigma_1\sigma_2(a_j) = \sigma_1(a_j) = a_{j+1}.$$

For j in $[k..(k+l-1)]$, $\sigma_2(a_j) = a_{j+1}$ and a_{j+1} is fixed by σ_1. Altogether, we obtain that

$$\sigma_1\sigma_2(a_j) = \sigma_1(a_j) = a_{j+1},$$

for every j in $[1..(k+l-1)]$. Finally, we notice that

$$\sigma_1\sigma_2(a_{k+l}) = \sigma_1(a_k) = a_1.$$

The claim follows. □

We can visualize the linking relation as *bursting a bubble*! Using Lemma 54, we obtain that for every distinct $a_1, \ldots, a_k \in [1..n]$

$$(a_1\ a_2)(a_2\ a_3)\cdots(a_{k-1}\ a_k) = (a_1 \cdots a_k). \tag{5.1}$$

Since every permutation can be written as a product of cycles, by (5.1) we obtain that every permutation can be written as a product of transpositions. Notice a permutation can be written as a product of transpositions in various forms. For instance,

$$(1\ 2)(2\ 3)(1\ 2) = (1\ 3).$$

Nevertheless, next we show that the parity of the number of transpositions stays the same for all the decompositions of a permutation as a product of transpositions.

Let $\Delta(x_1, \ldots, x_n) := \prod_{1 \le i < j \le n}(x_i - x_j)$ and for every permutation σ, define

$$\Delta_\sigma(x_1, \ldots, x_n) := \Delta(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

Notice that

$$\Delta(x_1,\dots,x_n)^2 = (1)^{n(n-1)/2}\prod_{i\neq j}(x_i - x_j).$$

This implies that

$$\begin{aligned}\Delta_\sigma(x_1,\dots,x_n)^2 =&\Delta(x_{\sigma(1)},\dots,x_{\sigma(n)})^2\\ =&(-1)^{n(n-1)/2}\prod_{\sigma(i)\neq\sigma(j)}(x_{\sigma(i)} - x_{\sigma(j)})\\ =&(-1)^{n(n-1)/2}\prod_{i\neq j}(x_i - x_j)\\ =&\Delta(x_1,\dots,x_n)^2.\end{aligned}$$

This implies that for every $\sigma \in S_n$, there exists $\operatorname{sign}(\sigma) \in \{-1,1\}$ such that

$$\Delta_\sigma = \operatorname{sign}(\sigma)\Delta.$$

The function sign : $S_n \to \{-1,1\}$ is called the *sign function*. We sometimes denote the sign function by ε. Show that

$$\prod_{i\neq j}(x_i - x_j) = (-1)^{n(n-1)/2}\Delta^2 = (-1)^{n(n-1)/2}\Delta_\sigma^2.$$

Proposition 55. *The sign function $\varepsilon : S_n \to \{-1,1\}$ is a group homomorphism.*

Proof. For every $\sigma,\tau \in S_n$, let $y_i = x_{\sigma(i)}$ for all i. Then

$$\begin{aligned}\Delta_\tau(y_1,\dots,y_n) =&\Delta(y_{\tau(1)},\dots,y_{\tau(n)})\\ =&\Delta(x_{\sigma(\tau(1))},\dots,x_{\sigma(\tau(n))})\\ =&\Delta_{\sigma\tau}(x_1,\dots,x_n)\\ =&\varepsilon(\sigma\tau)\Delta(x_1,\dots,x_n).\end{aligned} \tag{5.2}$$

We also have

$$\begin{aligned}\Delta_\tau(y_1,\dots,y_n) =&\varepsilon(\tau)\Delta(y_1,\dots,y_n)\\ =&\varepsilon(\tau)\Delta(x_{\sigma(1)},\dots,x_{\sigma(n)})\\ =&\varepsilon(\tau)\Delta_\sigma(x_1,\dots,x_n)\\ =&\varepsilon(\tau)\varepsilon(\sigma)\Delta(x_1,\dots,x_n).\end{aligned} \tag{5.3}$$

By (5.2) and (5.3), we obtain that

$$\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau).$$

□

For every permutation σ, we have

$$\Delta_\sigma(x_1, \ldots, x_n) = \Delta(y_1, \ldots, y_n) = \prod_{i<j}(y_i - y_j),$$

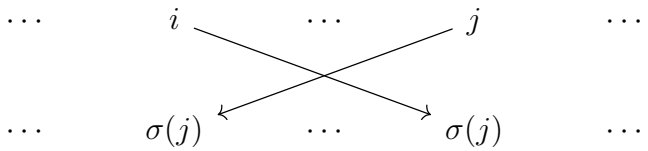
where $y_i := x_{\sigma(i)}$ for all i. Moreover

$$\prod_{i<j}(y_i - y_j) = \prod_{i<j}(x_{\sigma(i)} - x_{\sigma(j)}) = (-1)^{n_\sigma} \prod_{i<j}(x_i - x_j),$$

where

$$n_\sigma := |\{(i, j) \mid i < j, \sigma(i) > \sigma(j)\}|.$$

Notice that n_σ counts the number of crossing as we connect i to $\sigma(i)$ and create a planar bipartite graph.



That is why n_σ is called the *crossing number* of σ. By symmetry, we see that the crossing number of a transposition is odd. Hence

Corollary 56. *For every distinct $a, b \in [1..n]$, $\varepsilon(a\ b) = -1$.*

Corollary 57. *For every $\sigma \in S_n$, σ is in the kernel of the sign function if and only if σ can be written as a product of even number of transpositions.*

Proof. We have proved that every permutation can be written as a product of transpositions. Suppose $\sigma = \tau_1 \cdots \tau_k$ and τ_i's are transpositions. Then

$$\varepsilon(\sigma) = \prod_{i=1}^{k} \varepsilon(\tau_i) = (-1)^k.$$

Hence σ is in the kernel of the sign function if and only if k is even. □

A permutation is called an *even* permutation if it can be written as a product of even number of transpositions. By the previous corollary, a permutation is an even permutation if and only if it is in the kernel of the sign function. The kernel of the sign function is denoted by A_n and it is called the *alternating* group. Notice that for $n \geq 2$,

$$S_n/A_n \simeq \{\pm 1\},$$

and so A_n is a normal subgroup of index 2 in S_n for every integer $n \geq 2$.

5.2.1 Alternating group is simple

Our next task is to show that A_n is a simple group if $n \geq 5$.

Lemma 58. *For all positive integer n, A_n is generated by 3-cycles.*

Proof. Notice that every 3-cycle $(a_1\ a_2\ a_3)$ can be written as

$$(a_1\ a_2\ a_3) = (a_1\ a_2)(a_2\ a_3).$$

Hence it is an even permutation.

On the other hand, every even permutation is a product of even number of transpositions. So it is enough to prove that product of two transpositions is in the subgroup generated by 3-cycles.

We consider the following three cases:

$$|\mathrm{Supp}(\tau_1) \cap \mathrm{Supp}(\tau_2)| = 2,\ 1,\ \text{or } 0.$$

In the first case, $\tau_1 = \tau_2$, and $\tau_1\tau_2 = \mathrm{Id}$. In the second case, $\tau_1 = (a\ b)$ and $\tau_2 = (b\ c)$, and so

$$\tau_1\tau_2 = (a\ b)(b\ c) = (a\ b\ c)$$

is a 3-cycle. In the third case, $\tau_1 = (a\ b)$ and $\tau_2 = (c\ d)$,

$$\tau_1\tau_2 = (a\ b)(c\ d) = (a\ b)(b\ c)(b\ c)(c\ d) = (a\ b\ c)(b\ c\ d);$$

and so it is in the group generated by 3-cycles. (We are using the linking relation in all of these equations.) □

5.3 Lecture 15

Midterm.

5.4 Lecture 16

Lemma 59. *Suppose $n \geq 5$. If N is a normal subgroup of A_n and it contains a 3-cycle, then it $N = A_n$.*

Proof. Suppose N is a normal subgroup of A_n and $(a\,b\,c) \in N$ where a, b, c are distinct numbers. Suppose σ is another 3-cycle. Then σ and $(a\,b\,c)$ are conjugate of each other in S_n; that means there exists $\tau \in S_n$ such that

$$\sigma = \tau(a\,b\,c)\tau^{-1}.$$

Since $n \geq 5$, there exist distinct numbers $d, e \in [1..n] \setminus \{a, b, c\}$. Then

$$\sigma = \tau(d\,e)(a\,b\,c)(d\,e)\tau^{-1}.$$

Notice that either $\tau \in A_n$ or $\tau(d\,e)$. Hence σ is a conjugate of $(a\,b\,c)$ in A_n. Because N is a normal subgroup of A_n and $(a\,b\,c) \in N$, we obtain that $\sigma \in N$. This means every 3-cycle is in N. By Lemma 58, 3-cycles generate A_n. Hence $N = A_n$. □

Let's remark that the above argument shows that if $\sigma, \sigma' \in A_n$ are conjugate in S_n and $|\mathrm{Supp}(\sigma)| \leq n-2$, then σ and σ' are conjugate in A_n.

To continue, we need the following lemma.

Lemma 60. *Suppose the cycle type of σ is $(a_1, \ldots, a_k)$. Then*

$$o(\sigma) = \mathrm{lcm}(a_1, \ldots, a_k).$$

Proof. Permutation σ can be written as a product of disjoint cycles τ_i's of length a_i's. Notice that σ^l is identity if and only if the restriction of σ^l to the support of τ_i's is identity. The restriction of σ to the support of τ_i acts via τ_i. Hence σ^l is identity if and only if τ_i^l is identity for all i. Because τ_i^l is identity precisely when $a_i | l$, we obtain that $o(\sigma) = \mathrm{lcm}(a_1, \ldots, a_k)$. □

Lemma 61. *A_5 is a simple group.*

Proof. Suppose to the contrary that A_5 has a proper non-trivial normal subgroup N.

Case 1. $3||N|$.

In this case, N has an element σ of order 3. Suppose $(a_1, \ldots, a_k)$ is a cycle type of σ. Then $\sum_{i=1}^{k} a_i = 5$ and $\mathrm{lcm}(a_1, \ldots, a_k) = 3$. Therefore $a_1 = 3, a_2 = a_3 = 1$, which means that σ is a 3-cycle. Hence, by Lemma 59, $N = A_5$, which is a contradiction.

Case 2. $5||N|$, but $3 \nmid |N|$.

In this case, N has an element of order 5. Suppose $(a_1, \ldots, a_k)$ is a cycle type of σ. Then $\sum_i a_i = 5$ and $\text{lcm}(a_1, \ldots, a_k) = 5$. Therefore, $a_1 = 5$, which implies that σ is a 5-cycle. Notice that A_5 has 4! 5-cycles, and so A_5 has 6 Sylow 5-subgroups. Because N is a normal subgroup of A_5 and N contains a 5-cycle, all Sylow 5-subgroups are subset of N. Hence, $|N| \geq 25$. Because $|N|$ divides $|A_5|$ and $|N| \geq 25$, we obtain that $|N| = 30$. This implies that $3||N|$, which is a contradiction.

Case 3. $\gcd(|N|, 15) = 1$.

Because $|N|$ divides 60 and $\gcd(|N|, 15) = 1$, we obtain that $|N|$ divides 4. Hence N has an element σ of order 2. Therefore the cycle type of σ is either $(2, 2, 1)$ or $(2, 1, 1, 1)$. But the latter is not possible as σ is an even permutation. Hence, σ is a product of two disjoint transpositions. Without loss of generality, we can and will assume that

$$\sigma = (1\ 2)(3\ 4).$$

Then

$$(1\ 2\ 3)\sigma(1\ 2\ 3)^{-1} = (2\ 3)(1\ 4) \in N,$$

$$(1\ 3\ 2)\sigma(1\ 3\ 2)^{-1} = (3\ 1)(2\ 4) \in N,$$

and

$$(1\ 2\ 5)\sigma(1\ 2\ 5)^{-1} = (2\ 5)(3\ 4) \in N.$$

Hence $|N| \geq 5$, which is a contradiction. □

5.5 Lecture 17

Theorem 62. *For every integer $n \geq 5$, A_n is simple.*

Proof. We proceed by induction on n. The base of induction follows from Lemma 61. To prove the induction step, for every $i \in [1..n]$, let G_i be the stabilizer subgroup of A_n with respect to i. Then $G_i \simeq A_{n-1}$. Suppose N is a non-trivial normal subgroup of A_n. Then for all i, $N \cap G_i$ is a normal subgroup of G_i. By the induction hypothesis and the fact that $G_i \simeq A_{n-1}$, $N \cap G_i$ is either $\{\text{Id}\}$ or G_i. If $N \cap G_i$, then N has a 3-cycle. In this case, by Lemma 59, $N = A_n$. So without loss of generality, we can and will assume that $N \cap G_i = \{\text{Id}\}$ for all i. Therefore

for all distinct $\sigma_1, \sigma_2 \in N$ and i, $\sigma_1(i) \neq \sigma_2(i)$; otherwise $\sigma_1^{-1}\sigma_2(i) = i$, and so $\sigma_1^{-1}\sigma_2 \in N \cap G_i$, which is a contradiction.

In the rest of the argument, we conjugate an element of N and find two elements of N which send i to the same value for some i. Suppose σ is a non-trivial element of N, and its cycle type is $(a_1, \ldots, a_k)$.

Case 1. $a_1 \geq 3$.

Hence $\sigma = (a\, b\, c\, \cdots)\cdots(\cdots)$ for some distinct values a, b, c. Since $n \geq 5$, there are distinct values e, d in $[1..n] \setminus \{a, b, c\}$. Hence

$$\sigma' := (c\, d\, e)\sigma(c\, d\, e)^{-1} = (a\, b\, d\, \cdots)\cdots(\cdots) \in N.$$

This implies $\sigma(a) = \sigma'(a) = b$, which is a contradiction.

Case 2. $a_1 = 2$.

Since σ is an even permutation, $\sigma = (a\, b)(c\, d)\cdots(\cdots)$ for some distinct values a, b, c, d. Since $n \geq 5$, there exists e in $[1..n] \setminus \{a, b, c, d\}$. Then

$$\sigma' := (c\, d\, e)\sigma(c\, d\, e)^{-1} = (a\, b)(d\, e)\cdots(\cdots).$$

Hence $\sigma, \sigma' \in N$ and $\sigma(a) = \sigma'(a) = b$, which is a contradiction. □

Chapter 6

Composition series and solvable groups.

6.1 Lecture 17 (continue)

6.1.1 Composition series

In this section, we see how we can treat simple groups as building blocks for finite groups.

Definition 63. *Suppose G is a group. We say $\{G_i\}_{i=0}^k$ is a* composition series *of G if*

$$\{1\} =: G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_k := G$$

and G_{i+1}/G_i is a simple group for every i. For every i, G_{i+1}/G_i is called a composition factor *of G.*

We show that the composition factors of G are unique up to reordering and isomorphisms. For the sake of convenience, we say

$$(H_1, \ldots, H_k) \sim (H_1', \ldots, H_l')$$

if $k = l$ and $H_i \simeq H'_{\sigma(i)}$ for some permutation σ in the symmetric group S_k. Notice that $\sim$ is an equivalence relation.

Theorem 64. *Suppose G is a finite group. Then G has a composition series, and its composition factors are unique up to reordering and isomorphisms.*

Proof. Consider all the normal series of G, and suppose

$$\{1\} = G_0 \lhd \cdots \lhd G_k = G$$

has the maximum length among all such normal series.

Claim. For all i, G_{i+1}/G_i is a simple group.

Proof of Claim. Suppose to the contrary that G_{i+1}/G_i is not simple for some i. Then there exists a non-trivial proper normal subgroup $\overline{N} \trianglelefteq G_{i+1}/G_i$. By the correspondence theorem, there exists a normal subgroup N of G_{i+1} such that $G_i \lhd N$ and $\overline{N} = N/G_i$. Then

$$G_0 \lhd \cdots \lhd G_i \lhd N \lhd G_{i+1} \lhd \cdots \lhd G_k = G,$$

is a longer normal series which is a contradiction. □

Because all G_i/G_{i+1}'s are simple, $\{G_i\}_i$ is a composition series.

Next we use strong induction on $|G|$ to prove that the uniqueness of composition factors. Suppose

$$\{1\} = G_0 \lhd \cdots \lhd G_k = G \quad \text{and} \quad \{1\} = H_0 \lhd \cdots \lhd H_l = G$$

are two composition series.

Case 1. $G_{k-1} = H_{l-1}$.

Proof of Case 1. Notice that $\{G_i\}_{i=0}^{k-1}$ and $\{H_i\}_{i=0}^{l-1}$ are two composition series of G_{k-1} and H_{l-1}. Then by the induction hypothesis, $k-1 = l-1$ and

$$(G_1/G_0, \ldots, G_{k-1}/G_{k-2}) \sim (H_1/H_0, \ldots, H_{l-1}/H_{l-2}).$$

Hence $k = l$ and

$$(G_1/G_0, \ldots, G_{k-1}/G_{k-2}, G/N) \sim (H_1/H_0, \ldots, H_{l-1}/H_{l-2}, G/N),$$

where $N = G_{k-1} = H_{l-1}$. This means

$$(G_1/G_0, \ldots, G_{k-1}/G_{k-2}, G_k/G_{k-1}) \sim (H_1/H_0, \ldots, H_{l-1}/H_{l-2}, H_l/H_{l-1}).$$

□

Case 2. $G_{k-1} \neq H_{l-1}$.

Proof of Case 2. Since $G_{k-1} \neq H_{l-1}$, $G_{k-1}H_{l-1}/H_{l-1}$ is a non-trivial normal subgroup of H_l/H_{l-1}. Because H_l/H_{l-1} is a simple group, we obtain that

$$G_{k-1}H_{l-1} = H_l = G. \tag{6.1}$$

By (6.1), we deduce that

$$G/H_{l-1} = G_{k-1}H_{l-1}/H_{l-1} \simeq G_{k-1}/(G_{k-1} \cap H_{l-1}) \tag{6.2}$$

and

$$G/G_{k-1} = G_{k-1}H_{l-1}/G_{k-1} \simeq H_{l-1}/(G_{k-1} \cap H_{l-1}). \tag{6.3}$$

Let $K := G_{k-1} \cap H_{l-1}$. By the first part, we know that K has a composition series. Suppose

$$\{1\} = K_0 \lhd \cdots \lhd K_s := K$$

is a composition series of K. By (6.2), we obtain that

$$K_0 \lhd \cdots \lhd K_s \lhd G_{k-1}$$

is a composition series of G_{k-1} and similarly, by (6.3),

$$K_0 \lhd \cdots \lhd K_s \lhd H_{l-1}$$

is a composition series of H_{l-1}. Notice that $\{G_i\}_{i=0}^{k-1}$ is also a composition series of G_{k-1}. Hence by the induction hypothesis, we deduce that $s+1 = k-1$ and

$$(G_1/G_0, \ldots, G_{k-1}/G_{k-2}) \sim (K_1/K_0, \ldots, K_s/K_{s-1}, G_{k-1}/K_s). \tag{6.4}$$

Similarly, we have $s+1 = l-1$ and

$$(H_1/H_0, \ldots, H_{l-1}/H_{l-2}) \sim (K_1/K_0, \ldots, K_s/K_{s-1}, H_{k-1}/K_s). \tag{6.5}$$

Therefore $k = l$ and by (6.4) and (6.5), we obtain

$$(G_1/G_0, \ldots, G_k/G_{k-1}) \sim (K_1/K_0, \ldots, K_s/K_{s-1}, G_{k-1}/K_s, G/G_{k-1}), \tag{6.6}$$

and

$$(H_1/H_0, \ldots, H_l/H_{l-1}) \sim (K_1/K_0, \ldots, K_s/K_{s-1}, H_{l-1}/K_s, G/H_{l-1}). \tag{6.7}$$

Notice that by (6.2) and (6.3), we have

$$(G_{k-1}/K_s, G/G_{k-1}) \sim (H_{l-1}/K_s, G/H_{l-1}).$$

Therefore, by (6.6) and (6.7), we deduce that

$$(G_1/G_0, \ldots, G_k/G_{k-1}) \sim (H_1/H_0, \ldots, H_l/H_{l-1}).$$

□

□

6.2 Lecture 18

We start by investigating composition factors of a finite abelian group. Notice that if G is an abelian group, then all of its subgroups and quotients are abelian. Therefore all of its composition factors are abelian. Hence the next lemma shows that a composition factor of an abelian group is a cyclic group of prime order.

Lemma 65. *An abelian group is simple if and only if it is cyclic group of prime order.*

Proof. Every subgroup of an abelian group is normal. Hence an abelian group is simple if and only if it does not have any non-trivial proper subgroup. This means an abelian group G is simple precisely when every non-trivial element generates G. If G has an element of infinite order g, then g^2 cannot generate G. Hence every element of G is of finite order. If an element g of G has a composite order pq, then g^p is of smaller order. Therefore every non-trivial element of G if of prime order. The converse is clearly true. □

Corollary 66. *Suppose G is an abelian group of order $\prod_{i=1}^{k} p_i^{n_i}$ where p_i's are prime and n_i's are positive integers. Then the set of composition factors of G is $\{\mathbb{Z}/p_i\mathbb{Z}\}_{i=1}^{k}$ and $\mathbb{Z}/p_i\mathbb{Z}$ appears with multiplicity n_i.*

Proof. Suppose $G_0 \lhd \cdots \lhd G_s$ is a composition series of G. Then

$$|G| = \prod_{i=1}^{s} |G_i/G_{i-1}|$$

and G_i/G_{i-1}'s are the composition factors of G. By Lemma 65, G_i/G_{i-1} is a cyclic group of prime order. Hence $|G_i/G_{i-1}| = q_i$ is a prime number. Therefore

$$\prod_{i=1}^{k} p_i^{n_i} = \prod_{i=1}^{s} q_i.$$

By the uniqueness of prime factorization of integers, we deduce that $\mathbb{Z}/p_i\mathbb{Z}$ appears among the composition factors of G exactly n_i-times. □

In particular, we see that only the order of a finite abelian group determines all the composition factors. Next, we want to investigate what other finite groups have only cyclic groups of prime order as their composition factors.

6.2.1 Solvable groups

We say a group G is *solvable* if there is a chain of normal subgroups

$$\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_k = G$$

such that G_i/G_{i-1} is abelian for all i. For instance if G has a composition series and all of its composition factors are cyclic groups of prime order, then G is solvable.

The name *solvable* is coming from Galois theory. Galois proved that zeros of a polynomial in $\mathbb{Q}[x]$ can be expressed using addition, subtraction, multiplication, division, and radicals precisely when the group of symmetries of the polynomial is solvable.

To understand properties of solvable groups better, let's recall the definition of the commutator of two subgroups. Suppose G is a group and

6.3 11/7/2022

Theorem 67. *Suppose G is a group. Then $\gamma_{1+c}(G) = \{1\}$ if and only if $Z_c(G) = G$.*

Proof. ($\Rightarrow$) we proved in the previous lecture.

($\Leftarrow$) By induction on i, we prove that

$$\gamma_{1+i}(G) \subseteq Z_{c-i}(G).$$

□

Lemma 68. *Every nilpotent group is solvable.*

The converse is not true. The solvability length of a nilpotent group is logarithmic in terms of its nilpotency class.

Lemma 69. *Suppose G is nilpotent. Then every subgroup and every quotient of G is nilpotent.*

Lemma 70. *Every finite p-group is nilpotent.*

Proof. We proceed by strong induction on $|G|$. Use the fact that $Z(G) \neq \{1\}$ if G is a non-trivial finite p-group. □

Lemma 71. *Direct product of nilpotent groups is nilpotent.*

6.4 11/9/2022

Lemma 72. *Suppose G is a nilpotent group. If H is a proper subgroup of G, then H is a proper subgroup of $N_G(H)$.*

Proof. Since $Z_c(G) = G$ for some positive integer c and H is a proper subgroup, there exists an integer i such that

$$Z_i(G) \subseteq H \quad \text{and} \quad Z_{i+1}(G) \nsubseteq H.$$

Argue why $Z_{i+1}(G)$ is a subset of $N_G(H)$. □

Proposition 73. *Suppose G is a finite nilpotent group. Then Sylow subgroups of G are normal.*

Proof. Suppose P is a Sylow p-subgroup. Then $N_G(N_G(P)) = N_G(P)$. By the previous lemma, $N_G(P)$ cannot be a proper subgroup. Therefore $N_G(P) = G$, which means P is a normal subgroup of G. □

Theorem 74. *Suppose G is a finite group. Then the following statements are equivalent.*

1. *G is nilpotent.*
2. *All the Sylow subgroups of G are normal.*

3. $G \simeq \prod_{i=1}^{k} P_i$ *where* $|P_i|$ *is a power of a prime* p_i*.*

Proof. ($\Rightarrow$) Suppose $|G| = \prod_{i=1}^{k} p_i^{n_i}$. Let P_i be the unique Sylow p_i-subgroup. First we prove that, for every subset $I := \{i_1, \ldots, i_s\}$ of $[1..k]$,

$$|P_{i_1} \cdots P_{i_k}| = \prod_{j=1}^{k} |P_{i_j}|.$$

By one of your earlier homework assignments, we obtain the claim.

($\Leftarrow$) All P_i's are nilpotent groups. Suppose $\gamma_{1+c}(P_i) = \{1\}$ for all i. Then $\gamma_{1+c}(G) = \{1\}$. □

Theorem 75. *A finite group* G *is nilpotent if and only if all of its maximal subgroups are normal.*

Proof. ($\Rightarrow$) Suppose M is a maximal subgroup. Then M is a proper subgroup of $N_G(M)$ implies that $N_G(M) = G$.

($\Leftarrow$) Suppose $N_G(P)$ is a proper subgroup for some Sylow p-subgroup P. Let M be a maximal subgroup of G which contains $N_G(P)$. Then by the Frattini argument $N_G(P)M = G$, which is a contradiction. □

Proposition 76. *Suppose* G *is nilpotent and* N *is a non-trivial normal subgroup of* G*. Then* $Z(G) \cap N \neq \{1\}$*.*