MATH 3030 ALGEBRA I

Lecture 3

Isomorphism Theorems

Recall the 1st Isomorphism Theorem:

Thm Let $\varphi : G \to G'$ be a homomorphism. Let $N = \mathrm{Ker}(\varphi)$.
Then the map $\overline{\varphi} : G/N \longrightarrow \varphi(G)$ defined by

$$\overline{\varphi}(aN) = \varphi(a)$$

is an isomorphism such that $\varphi = \overline{\varphi} \circ \pi_N$,
where

$$\pi_N : G \longrightarrow G/N, \quad a \longmapsto aN$$

is the canonical map.

$$\begin{tikzcd} G \arrow[r, "\pi"] \arrow[dr, "\varphi"'] & G/N \arrow[d, dashed, "\overline{\varphi}"] \\ & G' \end{tikzcd}$$

As an application, we have

Lemma ① Let $N \triangleleft G$. Then the map

$$\Pi : \left\{ L \;\middle|\; \begin{array}{c} L \triangleleft G \\ L > N \end{array} \right\} \longrightarrow \left\{ K \;\middle|\; K \triangleleft G/N \right\}$$

$$L \longmapsto \pi_N(L)$$

is a bijection.

To prove this, let us recall the following lemma:

Lemma ② Let $\phi : G \to G'$ be a homomorphism.

1. $N \triangleleft G \Rightarrow \phi(N) \triangleleft \phi(G)$ (NOT $\phi(N) \triangleleft G'$!!)
2. $N' \triangleleft G' \Rightarrow \phi^{-1}(N') \triangleleft G$

Pf of Lemma ①: First of all, $L \lhd G \Rightarrow \pi_N(L) \lhd \pi_N(G) = G/N$ by Lemma ②.

Also, since $L > N$, $\pi_N^{-1}(\pi_N(L)) = L$, so Π is 1-1.

Next, if $K \lhd G/N$, then $L := \pi_N^{-1}(K) \lhd G$ by (Lemma ②) and $L > N$.

As $K \subset \mathrm{Im}\,\pi_N$, we have $\pi_N(\pi_N^{-1}(K)) = K$, this shows that Π is onto. #

Def A group G is called simple if $G \neq \{e\}$ & it has no proper nontrivial normal subgroups.

e.g. • Any simple abelian group must be cyclic and of prime order.

• A_n is simple for $n \geq 5$. (Do §15, Ex 39 to prove it!)

Def A normal subgroup $M \ntrianglelefteq G$ is called maximal if $\nexists\, N \trianglelefteq G$ such that $M \subsetneqq N \subsetneqq G$.

Prop $M \trianglelefteq G$ is maximal iff G/M is simple.

Pf: ($\Longrightarrow$): If $K \trianglelefteq G/M$ is nontrivial proper, then by Lemma ②, we have

$$\pi_M^{-1}(K) \trianglelefteq G \text{ and } M \subsetneqq \pi_M^{-1}(K) \subsetneqq G \text{ where } \pi_M : G \to G/M$$

is the canonical map. So M is not maximal.

($\Longleftarrow$): Conversely, if $\exists\, N \trianglelefteq G$ s.t. $M \subsetneqq N \subsetneqq G$, then by Lemma ② again, $\pi_M(N) \trianglelefteq \pi_M(G) = G/M$; and it is nontrivial and proper by Lemma ①. So G/M is not simple. #

Rmk: Simple groups are the "basic building blocks" of groups.

Let H, N be subgroups of G.

Def The join $H \vee N$ of H and N is the subgroup of G generated by

$$HN := \{hn \mid h \in H \text{ and } n \in N\}$$

Lemma If $N \triangleleft G$, then $H \vee N = HN = NH$ for any $H < G$.

If furthermore $H \triangleleft G$, then $HN \triangleleft G$

Pf : Since $N \triangleleft G$, $HN = NH$. So it suffices to show $HN < G$.

Let $h_1 n_1, h_2 n_2 \in HN$. As $N \triangleleft G$, $\exists\, n_0 \in N$ s.t. $(n_1 n_2^{-1}) h_2^{-1} = h_2^{-1} n_0$

$\Rightarrow (h_1 n_1)(h_2 n_2)^{-1} = h_1 (n_1 n_2^{-1}) h_2^{-1} = h_1 h_2^{-1} n_0 \in HN$. Hence $HN < G$.

If in addition $H \triangleleft G$, then $\forall g \in G$,

$g(HN)g^{-1} = (gHg^{-1})(gNg^{-1}) = HN$. Hence $HN \triangleleft G$. #

Thm (2nd Isomorphism Theorem)

For $H < G$ and $N \triangleleft G$, we have $(HN)/N \simeq H/(H \cap N)$.

Pf: Consider the canonical map $\pi_N : G \longrightarrow G/N$, and its restriction

$$\pi_N|_H : H \longrightarrow \pi_N(H).$$

$Ker(\pi_N|_H) = \{h \in H \mid hN = N\} = \{h \in H \mid h \in N\} = H \cap N$ (so $H \cap N \triangleleft H$).

By the 1st Isom Thm, $\pi_N|_H$ induces an isom $H/(H \cap N) \cong \pi_N(H)$

On the other hand, restriction of π_N to HN gives a map

$$\pi_N|_{HN} : HN \longrightarrow \pi_N(HN) = \pi_N(H)$$

and $Ker(\pi_N|_{HN}) = \{hn \in HN \mid hnN = N\} = \{hn \in HN \mid h \in N\} = N$

Applying 1st Isom Thm again gives $(HN)/N \cong \pi_N(H)$. #

<u>Another (simpler) pf</u> :

Consider the map $\pi : H \longrightarrow HN/N$ defined by $\pi(h) = hN$.

Since $hnN = hN$ for any $h \in H$ and $n \in N$, π is surjective.

Next, $\pi(h_1 h_2) = (h_1 h_2)N = (h_1 N)(h_2 N) = \pi(h_1)\,\pi(h_2)$,

so π is a homomorphism.

Finally, $\mathrm{Ker}(\pi) = \{h \in H \mid hN = N\} = H \cap N$.

Hence the result follows from the 1st Isom. Thm. #

<u>Rmk</u> π is nothing but the restriction of π_N to H.

e.g. Let $m, n \in \mathbb{Z}$. Then in the group $\mathbb{Z}$, we have

$$\begin{cases} m\mathbb{Z} + n\mathbb{Z} = \langle m, n \rangle = \langle \gcd(m,n) \rangle = \gcd(m,n) \cdot \mathbb{Z} \\ m\mathbb{Z} \cap n\mathbb{Z} = \langle \operatorname{lcm}(m,n) \rangle = \operatorname{lcm}(m,n) \cdot \mathbb{Z} \end{cases}$$

So the 2nd Isom. Thm says that

$$\frac{\gcd(m,n) \cdot \mathbb{Z}}{n\mathbb{Z}} = \frac{m\mathbb{Z} + n\mathbb{Z}}{n\mathbb{Z}} \cong \frac{m\mathbb{Z}}{m\mathbb{Z} \cap n\mathbb{Z}} = \frac{m\mathbb{Z}}{\operatorname{lcm}(m,n) \cdot \mathbb{Z}}$$

which implies the fact that

$$\gcd(m,n) \cdot \operatorname{lcm}(m,n) = m \cdot n.$$

Thm (3rd Isomorphism Theorem)
Let $H, K \trianglelefteq G$ w/ $K < H$. Then $G/H \simeq (G/K)/(H/K)$

Pf: Define $\phi : G/K \longrightarrow G/H$ by $\phi(aK) = aH$.

If $aK = bK$, then $a^{-1}b \in K$. But $K < H$ so $a^{-1}b \in H \Rightarrow aH = bH$.

So ϕ is well-defined, and is clearly surjective.

For $aK, bK \in G/K$,

$$\phi((aK)(bK)) = \phi((ab)K) = (ab)H = (aH)(bH) = \phi(aK)\phi(bK)$$

so ϕ is a homomorphism.

Finally,
$$\begin{aligned} \operatorname{Ker}(\phi) &= \{aK \in G/K \mid aH = H\} \\ &= \{aK \in G/K \mid a \in H\} = H/K \end{aligned}$$

The result follows from the 1st Isom Thm. #

Series of groups

Let G be a group.

Def A subnormal series of G is a finite chain of subgroups

$$\{e\} = H_0 < H_1 < \cdots < H_n = G$$

s.t. $H_i \triangleleft H_{i+1}$ $\forall i$; and it is called a normal series if $H_i \triangleleft G$ $\forall i$.

n is called the length of the series.

The quotient groups H_{i+1}/H_i are called the quotient (or factor) groups of the series.

e.g.

- $\{0\} < 8\mathbb{Z} < 4\mathbb{Z} < \mathbb{Z}$
- $\{id\} < \langle (1\,2)(3\,4) \rangle < V = \left\{ \begin{matrix} id, (1\,2)(3\,4), \\ (1\,3)(2\,4), (1\,4)(2\,3) \end{matrix} \right\} < D_4$

Def Given two subnormal (normal) series $\{H_i\}$ and $\{K_j\}$ of a group G. We say $\{K_j\}$ is a refinement of $\{H_i\}$ if $\{H_i\} \subseteq \{K_j\}$.

Def A subnormal (resp. normal) series $\{H_i\}$ is a composition (resp. principal) series if it has no proper refinement, or equivalenty, if all its quotient groups H_{i+1}/H_i (now called composition factors) are simple.

- Clearly, every finite group has a composition series.
- Given a composition series

$$\{e\} = H_0 < H_1 < \cdots < H_n = G$$

we obtain a sequence of short exact sequences (or extensions):

$$1 \to H_1 \to H_2 \to H_2/H_1 \to 1$$

$$1 \to H_2 \to H_3 \to H_3/H_2 \to 1$$

$$\vdots$$

$$1 \to H_i \to H_{i+1} \to H_{i+1}/H_i \to 1$$

$$\vdots$$

$$1 \to H_{n-1} \to H_n = G \to H_n/H_{n-1} \to 1$$

finite simple groups

Here, 1 denotes the trivial gp. Given groups G, H & Q, a sequence of maps

$$1 \longrightarrow H \xrightarrow{\iota} G \xrightarrow{\pi} Q \longrightarrow 1$$

is called <u>short exact</u> if (i) ι is 1-1, (ii) π is onto & (iii) $\ker \pi = \operatorname{Im} \iota$.

In this case, we also say G is an <u>extension</u> of Q by H.

Hölder program : every finite group is built from finite simple groups

① Classify all finite simple groups ← completed around 2004

② Classify all possible ways of building a group from given finite simple groups ← largely unknown

Examples

- $\{id\} < A_3 < S_3$

  $\{id\} < \langle (13)(24) \rangle < V < A_4 < S_4$

  are composition series for S_3 and S_4 resp.

- Since A_n is simple for $n \geq 5$, $\{id\} < A_n < S_n$ is a composition series for $n \geq 5$.

Thm (Jordan-Hölder) Let G be a finite group. If

$$\{e\} = H_0 < H_1 < \cdots < H_n = G$$

$$\{e\} = K_0 < K_1 < \cdots < K_m = G$$

are two composition series for G, then $m=n$ and $\exists\, \sigma \in S_n$

s.t. $\quad H_{i+1}/H_i \simeq K_{\sigma(i)+1}/K_{\sigma(i)}$

Pf: We use induction on $|G|$.

Case I: $H_{n-1} = K_{m-1}$. In this case, we have two composition series for this smaller group, so we can apply the induction hypothesis

Case II: $H_{n-1} \neq K_{m-1}$.

In this case, $H_{n-1} \lhd G$ & $K_{m-1} \lhd G \Rightarrow H_{n-1}K_{m-1} \lhd G$

But $H_{n-1}K_{m-1}$ properly contains both H_{n-1} & K_{m-1}, which are both maximal normal subgroups of G, so $G = H_{n-1}K_{m-1}$.
By the 2nd Isom. Thm, we have

$$G/H_{n-1} \simeq K_{m-1}/(H_{n-1} \cap K_{m-1}) \text{ and } G/K_{m-1} \simeq H_{n-1}/(H_{n-1} \cap K_{m-1})$$

Let $J := H_{n-1} \cap K_{m-1}$. Then J is a maximal normal subgroup in both H_{n-1} and K_{m-1}, and

$$G/H_{n-1} \simeq K_{m-1}/J \quad \text{and} \quad G/K_{m-1} \simeq H_{n-1}/J.$$

Choose a composition series

$$\{e\} = J_0 < J_1 < \cdots < J_{\ell-1} = J$$

Now we have

$$\mathrm{Quotients}(G > H_{n-1} > H_{n-2} > \cdots)$$

$$= \{ G/H_{n-1},\ H_{n-1}/H_{n-2},\ H_{n-2}/H_{n-3},\ \dots \}$$

equal up to permutations

$$\sim \{ \underset{\underset{K_{m-1}/J}{\wr}}{G/H_{n-1}},\ \underset{\underset{G/K_{m-1}}{\wr}}{H_{n-1}/J},\ J/J_{\ell-2},\ \dots \} \quad \left(\begin{array}{c}\text{by induction hypothesis}\\ \text{applied to } H_{n-1}\end{array}\right)$$

$$\sim \{ G/K_{m-1},\ K_{m-1}/J,\ J/J_{\ell-2},\ \dots \} \quad (\text{reordering})$$

$$\sim \{ G/K_{m-1},\ K_{m-1}/K_{m-2},\ K_{m-2}/K_{m-3},\ \dots \} \quad \left(\begin{array}{c}\text{by induction hypothesis}\\ \text{applied to } K_{m-1}\end{array}\right)$$

$$= \mathrm{Quotients}(G > K_{m-1} > K_{m-2} > \cdots). \qquad \#$$

<u>Rmk</u> Since a simple abelian group is of prime order (and hence cyclic), the above theorem applied to cyclic groups gives the uniqueness of prime factorization of positive integers.

Solvable groups

Def A group G is solvable if it has a subnormal series whose quotient groups are all abelian (called a solvable series).

Rmk If G is finite, then G is solvable iff it has a composition series whose composition factors are all cyclic of prime order.

In other words, a solvable group is a group built from (successive extensions of) abelian groups.

Examples
- All abelian groups are solvable
- S_3 and S_4 (and their subgroups) are solvable
- S_n is not solvable when $n \geq 5$.

- Consider $U = \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\} < B = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} < GL_2(F)$

Then $U \trianglelefteq B$, $B/U \simeq F^* \times F^*$ $\quad \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto (a, c)$

and $U \simeq (F, +)$

Hence B is solvable.

<u>Prop</u> (a) Every subgroup and quotient group of a solvable group is solvable.

(b) Let N be a normal subgroup of G. If N and G/N are both solvable, then G is solvable.

Pf: (a) Suppose that G is solvable w/ a solvable series

$$\{e\} = K_0 < K_1 < \cdots < K_n = G$$

Let $H < G$ be a subgroup.

Then the homomorphism $H \cap K_{i+1} \longrightarrow K_{i+1}/K_i$

$$a \longmapsto aK_i$$

has kernel $(H \cap K_{i+1}) \cap K_i = H \cap K_i$.

Hence $H \cap K_i \trianglelefteq H \cap K_{i+1}$ and $(H \cap K_{i+1})/(H \cap K_i) \hookrightarrow K_{i+1}/K_i$ by 1st Isom Thm

In particular, the quotient is abelian, so

$$\{e\} = H \cap K_0 < H \cap K_1 < \cdots < H \cap K_n = H$$

is a solvable series for H.

On the other hand, let N be a normal subgroup of G.

Consider $N = K_0 N < K_1 N < \cdots < K_{n-1}N < K_n N = G$.

Quotient by N and letting $\overline{K}_i := (K_i N)/N$ (for $i = 0, 1, \ldots, n$) gives

$$\{N\} = \overline{K}_0 < \overline{K}_1 < \cdots < \overline{K}_{n-1} < \overline{K}_n = G/N.$$

To see that this is a solvable series, consider the composition

$$K_{i+1} \hookrightarrow K_{i+1}N \twoheadrightarrow (K_{i+1}N)/(K_i N)$$

This is a surjective homomorphism with kernel $\supset K_i$, so it induces (by 1st Isom. Thm) the surjective homomorphism

$$K_{i+1}/K_i \twoheadrightarrow (K_{i+1}N)/(K_i N)$$

But $\overline{K_{i+1}}/\overline{K_i} \cong (K_{i+1}N)/(K_i N)$ by the 3rd Isom Thm.

So $\overline{K_{i+1}}/\overline{K_i}$ is abelian $\forall i$.

(b) Let

$$\{N\} = \bar{K}_0 < \bar{K}_1 < \cdots < \bar{K}_n = \bar{G}, \text{ and}$$

$$\{e\} = H_0 < H_1 < \cdots < H_m = N$$

be solvable series of $\bar{G}$ and N respectively

Take $K_i = \pi_N^{-1}(\bar{K}_i)$ so that $N < K_i < G$ and $\bar{K}_i = \pi_N(K_i)$.

By the 3rd Isom Thm, $\bar{K}_{i+1}/\bar{K}_i \simeq K_{i+1}/K_i$

$$\Longrightarrow \{e\} = H_0 < H_1 < \cdots < H_m = N = K_0 < K_1 < \cdots < K_n = G$$

is a solvable series for G. #

<u>Rmk</u> Part (b) can be rephrased as: an extension of solvable groups is solvable.

Derived series

Recall that the commutator subgroup $[G,G] < G$ is the subgroup generated by commutators $[a,b] := aba^{-1}b^{-1}$.

$[G,G]$ is also called the 1st derived subgroup of G and denoted by $G' = G^{(1)}$

The 2nd derived subgroup of G is $G^{(2)} = (G')'$; the 3rd is $G^{(3)} = (G'')'$; and so on.

‖ Def The series $G > G^{(1)} > G^{(2)} > \cdots$ is called the derived series of G.

e.g. $S_n > A_n > A_n > A_n > \cdots$

‖ Prop A group G is solvable iff $G^{(k)} = \{e\}$ for some k.

Pf: $(\Leftarrow)$ is trivial.

($\Longrightarrow$) Conversely, suppose

$$\{e\} = H_0 < H_1 < \cdots < H_n = G$$

is a solvable series for G.

Since G/H_{n-1} is abelian, $G^{(1)} \subset H_{n-1}$

Now $G^{(1)}H_{n-2} < H_{n-1}$ and by the 2nd Isom Thm

$$G^{(1)}/(G^{(1)} \cap H_{n-2}) \simeq (G^{(1)}H_{n-2})/H_{n-2} \subset H_{n-1}/H_{n-2}$$

Since H_{n-1}/H_{n-2} is abelian, $G^{(2)} \subset G^{(1)} \cap H_{n-2} \subset H_{n-2}$.

Repeating this argument shows that $G^{(i)} \subset H_{n-i}$ $\forall i$.

Hence $G^{(k)} = \{e\}$ for some k. #