MTH101: Symmetry

Lecture 15

Recall

Let G be a group and let $K \lhd G$. Let $\psi : G \to G/K$ be the quotient homomorphism.

We have seen the following:

- Given a subgroup H of G, $\psi(H)$ is a subgroup of G/K, and $\psi^{-1}(\psi(H))$ is to equal $HK = \{hk | h \in H, k \in K\}$. (This is also the subgroup of G generated by H and K.)
- By the first isomorphism theorem applied to the restriction of ψ to H, we get $H/H \cap K \cong \psi(H)$.
- Again, by the first isomorphism theorem applied to the restriction of ψ to HK, we get $HK/K \cong \psi(H)$.
- This gives us the second isomorphism theorem: $H/H \cap K \cong HK/K$.

We also saw that we have a $1-1$ correspondence

$$\{\text{Subgroups of } G \text{ containing } K\} \leftrightarrow \{\text{Subgroups of } G/K\}.$$

Under this correspondence, given a subgroup of G containing K, the corresponding subgroup of G/K is $\psi(H)$.

Given a subgroup L of G/K, the corresponding subgroup of G is $\psi^{-1}(L)$. It contains $K = \psi^{-1}(1_{G/K})$.

An application

We saw separate proofs for the following two statements:

(A) Every subgroup of $\mathbb{Z}$ is cyclic.

(B) Every subgroup of $\mathbb{Z}/m\mathbb{Z}$ is cyclic where m is a positive integer.

However, we will now see how (B) can be deduced from (A).

Let $\psi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ be the quotient homomorphism. Let L be a subgroup of $\mathbb{Z}/m\mathbb{Z}$. We want to show that L is cyclic.

The group $\psi^{-1}(L)$ is a subgroup of $\mathbb{Z}$ and is hence cyclic. Thus, there exists an integer d such that $\psi^{-1}(L) = \langle d \rangle$.

Note that $\psi(d)$ is just the coset $d + m\mathbb{Z}$, which we write as $\overline{d}$. We will show that $L = \langle \overline{d} \rangle$.

Let $x \in L$. As ψ is onto, there exists some integer $y \in \mathbb{Z}$ such that $\psi(y) = x$.

As $x \in L$, $y \in \psi^{-1}(L)$. Thus $y = rd$ for some integer r.

So, $x = \psi(y) = \psi(rd) = r\psi(d) = r \cdot \overline{d}$. Thus. $x \in \langle \overline{d} \rangle$.

As x was an arbitrary element of L, we see that $L = \langle \overline{d} \rangle$.

Thus, we have proved (B).

Problem 1

Let $\phi : G \to H$ be a group homomorphism. Let S be a subset of G. Prove that $\phi(\langle S \rangle) = \langle \phi(S) \rangle$.

Solution 1: The main idea is to use the following statement repeatedly:

> *For any subset A in a group G, if a subgroup M contains the subset A, then $\langle A \rangle \subset M$.*

As $S \subset \langle S \rangle$, we see that $\phi(S) \subset \phi(\langle S \rangle)$. Note that $\phi(\langle S \rangle)$ is a subgroup of H. Thus, since it contains $\phi(S)$, we see that $\langle \phi(S) \rangle \subset \phi(\langle S \rangle)$.

On the other hand, as $\phi(S) \subset \langle \phi(S) \rangle$, we see that $\phi^{-1}(\phi(S)) \subset \phi^{-1}(\langle \phi(S) \rangle)$.

But $S \subset \phi^{-1}(S)$. Thus, we see that $S \subset \phi^{-1}(\langle \phi(S) \rangle)$. As $\phi^{-1}(\langle \phi(S) \rangle)$ is a subgroup of G, we see that $\langle S \rangle \subset \phi^{-1}(\langle \phi(S) \rangle$.

Hence $\phi(\langle S \rangle) \subset \phi(\phi^{-1}(\langle \phi(S) \rangle)) = \langle \phi(S) \rangle$. (For any subset T of H, it is easy to see that $\phi(\phi^{-1}(T)) = T$. We are applying this to $T = \langle \phi(S) \rangle$.)

Thus, we conclude that $\phi(\langle S \rangle) = \langle \phi(S) \rangle$.

Solution 2:

$\langle S \rangle$ is the set of all elements of G which can be written in the form $s_1^{n_1} \ldots s_r^{n_r}$ for some positive integer r, some elements $s_1, \ldots, s_r \in S$ and some integers $n_1, \ldots, n_r$.

Similarly, $\langle \phi(S) \rangle$ is the set of all elements of H which can be written in the form $\phi(s_1)^{n_1} \ldots \phi(s_r)^{n_r}$ for some positive integer r, some elements $s_1, \ldots, s_r \in S$ and some integers $n_1, \ldots, n_r$. Such an element is equal to $\phi(s_1^{n_1} \ldots s_r^{n_r})$, and $s_1^{n_1} \ldots s_r^{n_r}$ is an element of $\langle S \rangle$. Thus, $\langle \phi(S) \rangle \subset \phi(\langle S \rangle)$.

On the other hand, if we take a general element of $\langle S \rangle$, it is of the form $s_1^{n_1} \ldots s_r^{n_r}$. Its image $\phi(s_1^{n_1} \ldots s_r^{n_r})$ is equal to $\phi(s_1)^{n_1} \ldots \phi(s_r)^{n_r}$, which is an element of $\langle \phi(S) \rangle$.

Thus, $\phi(\langle S \rangle) = \langle \phi(S) \rangle$.

Remark

Here, the first solution does not require the explicit description of the subgroup generated by a set S. It uses a property that characterizes the subgroup generated by a set S, namely that it is the intersection of all subgroups containing S.

The second proof is more direct, but it relies on the explicit description of $\langle S \rangle$.

The fact that these two descriptions are equivalent was proved in Lecture 10.

Problem 2

Find the order of the group $\langle 36, 24, 16 \rangle$ of $\mathbb{Z}/50\mathbb{Z}$.

Solution: Let $\phi : \mathbb{Z} \to \mathbb{Z}/50\mathbb{Z}$ denote the quotient homomorphism. Let L denote the subgroup $\langle \overline{3}6, \overline{2}4, \overline{1}6 \rangle$ of $\mathbb{Z}/50\mathbb{Z}$. Let H denote the subgroup $\langle 36, 24, 16 \rangle$ of $\mathbb{Z}$. Then, we see (from the previous problem) that $\phi(H) = L$.

As H is a subgroup of $\mathbb{Z}$, it is cyclic. Let d be a generator of H. Then its image in $\mathbb{Z}/50\mathbb{Z}$ will be a generator of L. So we first have to find d.

We know that d can be taken to be the gcd of 36, 24 and 16. Thus, $d = 4$.

The image of 4 in $\mathbb{Z}/50\mathbb{Z}$ is the coset $4 + 50\mathbb{Z}$, which we write as $\overline{4}$.

The order of $\overline{4} = 4 \cdot \overline{1}$ is equal to $\frac{ord(\overline{1})}{gcd(4, ord(\overline{1}))}$. As $ord(\overline{1}) = 50$, we see that $ord(\overline{4}) = 50/2 = 25$. Thus, $|L| = ord(\overline{4}) = 25$.

Remark

We have proved in earlier lectures that if m_1, m_2 are generators, then $\langle m_1, m_2 \rangle$ is generated by $gcd(m_1, m_2)$. This statement generalizes to any finite collection of integers. Let us see how to prove this.

Given any finite collection of integers $m_1, \ldots, m_r$, if $d = gcd(m_1, \ldots, m_r)$, then clearly d divides every integer of the form $x_1 m_1 + x_2 m_2 + \cdots + x_r m_r$, where $x_1, \ldots, x_r \in \mathbb{Z}$.

Thus, d divides every element of $\langle m_1, \ldots, m_r \rangle$. Thus, it is clear that $\langle m_1, \ldots, m_r \rangle \subset \langle d \rangle$.

We want to prove that $\langle d \rangle \subset \langle m_1, \ldots, m_r \rangle$.

Observe that the subgroup $\langle m_1, \ldots, m_r \rangle$ is cyclic (as it is a subgroup of $\mathbb{Z}$). Thus, there exists some integer g such that $\langle m_1, \ldots, m_r \rangle = \langle g \rangle$.

Then, for $1 \leqslant i \leqslant r$, we see that $m_i \in \langle m_1, \ldots, m_r \rangle = \langle g \rangle$ and so $g | m_i$. Thus, $g | gcd(m_1, \ldots, m_r) = d$.

Thus, $d \in \langle g \rangle = \langle m_1, \ldots, m_r \rangle$. This completes our proof.

Conjugation

Let G be a group. For any element g, we can define a function $\phi_g : G \to G$ by $\phi_g(x) = gxg^{-1}$. Then, we can show that ϕ_g is an isomorphism from G to itself. (See problem 3 in Problem Set 1.)

A group isomorphism from G to itself is called an automorphism of G. The automorphisms of the type ϕ_g are called the inner automorphisms of G.

We had defined a subgroup H of G to be normal if $gHg^{-1} \subset H$ for every $g \in G$. However, we showed that in this case, we actually have $gHg^{-1} = H$ for every $g \in G$. Thus, we can say that a subgroup H is normal in G if every inner automorphism maps H onto itself, i.e. $\phi_g(H) = H$ for every $g \in G$.

Problem 3

Let G be a group. Let H be the subgroup of G generated by all elements of the form $xyx^{-1}y^{-1}$, where x, y are arbitrary elements of G. Prove that H is a normal subgroup of G.

Solution: For any $g \in G$, let $\phi_g : G \to G$ denote the inner automorphism $\phi_g(x) = gxg^{-1}$. We want to show that $\rho_g(H) = H$ for every $g \in G$.

Let S be the set of all elements of the form $xyx^{-1}y^{-1}$ where $x, y \in G$. Let us fix an element $g \in G$.

Observe that for any $g \in G$, $\phi_g(xyx^{-1}y^{-1}) = \phi_g(x)\phi_g(y)\phi_g(x)^{-1}\phi_g(y)^{-1}$, which is also an element of S. Thus, $\phi_g(S) \subset S$.

On the other hand, let $u = \phi_g^{-1}(x)$ and $v = \phi_g^{-1}(y)$. Then $\phi_g(uvu^{-1}v^{-1} = xyx^{-1}y^{-1}$. Thus, we see that every element of S is contained in $\phi_g(S)$. Thus, $\phi_g(S) = S$.

By Problem 1, $\phi_g(\langle S \rangle) = \langle \phi_g(S) \rangle = \langle S \rangle$. Thus, we see that $H = \langle S \rangle$ is a normal subgroup of G.

Remark

The elements of the form $xyx^{-1}y^{-1}$ are called the commutators of G. The subgroup generated by all these elements is called the commutator subgroup of G. It is sometimes written as $[G, G]$ or G'.

The quotient $G/[G, G]$ is an abelian group. (Exercise: Prove this!) In fact, it can be proved that $[G, G]$ is the smallest normal subgroup of G such that the quotient group of G with respect to this subgroup is abelian. In other words, if N is a normal subgroup of G such that G/N is abelian, then $[G, G] \leqslant N$.

$G/[G, G]$ is called the abelianization of G.