23. Quotient groups II

23.1. **Proof of the fundamental theorem of homomorphisms (FTH).**

We start by recalling the statement of FTH introduced last time.

Theorem (FTH). *Let G, Q be groups and $\varphi : G \to Q$ a homomorphism. Then*

$$G/\operatorname{Ker}\varphi \cong \varphi(G). \qquad (***)$$

Proof. Let $K = \operatorname{Ker}\varphi$ and define the map $\Phi : G/K \to \varphi(G)$ by

$$\Phi(gK) = \varphi(g) \text{ for } g \in G.$$

We claim that Φ is a well defined mapping and that Φ is an isomorphism. Thus we need to check the following four conditions:

(i) Φ is well defined
(ii) Φ is injective
(iii) Φ is surjective
(iv) Φ is a homomorphism

For (i) we need to prove the implication "$g_1K = g_2K \Rightarrow \Phi(g_1K) = \Phi(g_2K)$."

So, assume that $g_1K = g_2K$ for some $g_1, g_2 \in G$. Then $g_1^{-1}g_2 \in K$ by Theorem 19.2, so $\varphi(g_1^{-1}g_2) = e_Q$ (recall that $K = \operatorname{Ker}\varphi$). Since $\varphi(g_1^{-1}g_2) = \varphi(g_1)^{-1}\varphi(g_2)$, we get $\varphi(g_1)^{-1}\varphi(g_2) = e_Q$. Thus, $\varphi(g_1) = \varphi(g_2)$, and so $\Phi(g_1K) = \Phi(g_2K)$, as desired.

For (ii) we need to prove that "$\Phi(g_1K) = \Phi(g_2K) \Rightarrow g_1K = g_2K$." This is done by taking the argument in the proof of (i) and reversing all the implication arrows.

(iii) First note that by construction Codomain(Φ) $= \varphi(G)$. Thus, for surjectivity of Φ we need to show that Range(Φ) $= \Phi(G/K)$ is equal to $\varphi(G)$. This is clear since

$$\Phi(G/K) = \{\Phi(gK) : g \in G\} = \{\varphi(g) : g \in G\} = \varphi(G).$$

(iv) Finally, for any $g_1, g_2 \in G$ we have

$$\Phi(g_1K \cdot g_2K) = \Phi(g_1g_2K) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \Phi(g_1K)\Phi(g_2K)$$

where the first equality holds by the definition of product in quotient groups. Thus, Φ is a homomorphism.

So, we constructed an isomorphism $\Phi : G/\mathrm{Ker}\,\varphi \to \varphi(G)$, and thus $G/\mathrm{Ker}\,\varphi$ is isomorphic to $\varphi(G)$. $\square$

23.2. **Applications of FTH.** In most applications one uses a special case of FTH stated last time as Corollary 22.5:

If $\varphi : G \to Q$ is a surjective homomorphism, then $G/\mathrm{Ker}\,\varphi \cong Q$. (***)

Typically this result is being applied as follows. We are given a group G, a normal subgroup K and another group Q (unrelated to G), and we are asked to prove that $G/K \cong Q$. By (***) **to prove that $G/K \cong Q$ it suffices to find a surjective homomorphism $\varphi : G \to Q$ such that** $\mathrm{Ker}\,\varphi = K$.

Example 1: Let $n \geq 2$ be an integer. Prove that

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n.$$

We already established this isomorphism in Lecture 22 (see Corollary 22.3), so the point of this example is mostly to illustrate how FTH works.

In this example $G = \mathbb{Z}$, $Q = \mathbb{Z}_n$ and $K = n\mathbb{Z}$. Define the map $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ by $\varphi(x) = [x]_n$. It is straightforward to check that φ is a surjective homomorphism (anyway, this was verified in Lecture 15). We have

$$\mathrm{Ker}\,\varphi = \{x \in \mathbb{Z} : [x]_n = [0]_n\} = \{x \in \mathbb{Z} : x = nk \text{ for some } k \in \mathbb{Z}\} = n\mathbb{Z} = K.$$

Thus, by FTH (or, more precisely, by (***)) we have $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

Example 2: Let U be the group of rotations of the unit circle in $\mathbb{R}^2$. Prove that

$$U \cong \mathbb{R}/\mathbb{Z}.$$

Remark: As usual, by $\mathbb{R}$ we denote the group of reals (with addition) and $\mathbb{Z}$ is thought of as a subgroup of $\mathbb{R}$.

In this example $G = \mathbb{R}$, $Q = U$ and $K = \mathbb{Z}$. By definition, $U = \{r_\alpha : \alpha \in \mathbb{R}\}$, where r_α is the counterclockwise rotation by α radians. Clearly, the group operation on U is given by $r_\alpha r_\beta = r_{\alpha+\beta}$ for all $\alpha, \beta \in \mathbb{R}$.

Define the map $\varphi : \mathbb{R} \to U$ by

$$\varphi(x) = r_{2\pi x} \text{ for all } x \in \mathbb{R}.$$

Then φ is a homomorphism since

$$\varphi(x)\varphi(y) = r_{2\pi x} r_{2\pi y} = r_{2\pi(x+y)} = \varphi(x+y),$$

and φ is surjective, since any element of U is equal to r_α for some $\alpha \in \mathbb{R}$, and any $\alpha \in \mathbb{R}$ can be written as $2\pi x$ for some $x \in \mathbb{R}$ (namely $x = \alpha/2\pi$).

Finally, $\operatorname{Ker}\varphi$ consists of all $x \in \mathbb{R}$ such that $r_{2\pi x}$ is the trivial rotation. But a rotation by the angle of α radians is trivial if and only if α is an integer multiple of 2π. Thus,

$$x \in \operatorname{Ker}\varphi \iff 2\pi x = 2\pi k \text{ for some } k \in \mathbb{Z} \iff x \in \mathbb{Z}.$$

Thus, $\operatorname{Ker}\varphi = \mathbb{Z} = K$, as desired, and again by FTH we conclude that

$$\mathbb{R}/\mathbb{Z} \cong U.$$

Note that in this example we managed to determine the isomorphism class of the quotient group $\mathbb{R}/\mathbb{Z}$ without having to "visualize" it. We will return to the latter problem later in this lecture.

Example 3: Prove that the alternating group A_n (the subgroup of even permutations in S_n) has index 2 in S_n.

This can be proved in a number of different ways; using FTH is just one of them. To prove that $[S_n : A_n] = 2$ we will construct a surjective homomorphism $\varphi : S_n \to \mathbb{Z}_2$ with $\operatorname{Ker}\varphi = A_n$. If this is achieved, it would follow that $S_n/A_n \cong \mathbb{Z}_2$, so $|S_n/A_n| = |\mathbb{Z}_2| = 2$, and therefore $[S_n : A_n] = |S_n/A_n| = 2$, as desired.

Define $\varphi : S_n \to \mathbb{Z}_2$ by

$$\varphi(f) = \begin{cases} [0] & \text{if } f \text{ is even} \\ [1] & \text{if } f \text{ is odd.} \end{cases}$$

By construction φ is surjective. To prove that φ is a homomorphism we need to show that

$$\varphi(f) + \varphi(g) = \varphi(fg) \text{ for all } f, g \in S_n \qquad (***)$$

Recall (Proposition A.3 in the notes on even/odd permutations) that

if f and g are both even or both odd, then fg is even

if f is even and g is odd, or if f is odd and g is even, then fg is odd.

Let us consider 4 cases.

1. f and g are both even. Then fg is also even. So, $\varphi(f) = \varphi(g) = \varphi(fg) = [0]$. Since $[0] + [0] = [0]$, (***) holds.
2. f is even, and g is odd. Then fg is odd. So, $\varphi(f) + \varphi(g) = [0] + [1] = [1] = \varphi(fg)$.
3. f is odd, and g is even. This case is analogous to Case 2.
4. f and g are both odd. Then fg is even, so $\varphi(f) + \varphi(g) = [1] + [1] = [0] = \varphi(fg)$.

Thus, we verified that φ is a homomorphism. Finally, $\operatorname{Ker}\varphi = \{f \in S_n : \varphi(f) = [0]_2\}$ is the set of all even permutations, so $\operatorname{Ker}\varphi = A_n$ (by definition of A_n).

This completes the proof of the equality $[S_n : A_n] = 2$. The homomorphism $\varphi : S_n \to \mathbb{Z}_2$ constructed in the above proof has many other applications. We illustrate this by using φ to give an alternative solution to Problem 6(c) in HW#10, in fact, a stronger version of it:

Claim 23.1. *Let $f \in S_n$, and suppose $f = f_1 \ldots f_r$ where f_i's are cycles (not necessarily disjoint!) Let a be the number of cycles in the sequence $f_1, f_2, \ldots, f_r$ which have even length. Then f is even if and only if a is even.*

Proof. Applying φ to both sides of the equality $f = f_1 \ldots f_r$, we get

$$\varphi(f) = \varphi(f_1) + \ldots + \varphi(f_r). \qquad (***)$$

If f_i has odd length, then f_i is an even permutation, so $\varphi(f_i) = [0]$ by definition of φ. Likewise if f_i has even length, then f_i is an odd permutation, so $\varphi(f_i) = [1]$. Thus, each cycle of even length contributes [1] to the right-hand side of (***), and cycles of odd length contribute [0]. Hence $\varphi(f) = \underbrace{[1] + \ldots + [1]}_{a \text{ times}} = [a]$. Therefore, f is even $\iff \varphi(f) = [0] \iff [a] = [0] \iff a$ is even. □

23.3. **Transversals.**

Definition. Let G be a group and H a subgroup of G. A subset T of G is called a <u>transversal of H in G</u> if T contains PRECISELY one element from each left coset with respect to H.

Example: Let $G = \mathbb{Z}$ and $H = 3\mathbb{Z}$. Then H has 3 left cosets: $0+H, 1+H$ and $2+H$, so the set $T = \{0, 1, 2\}$ is a transversal. Another transversal is $\{2, 7, 9\}$. In general, in this example, a set T will be a transversal $\iff$ $|T| = 3$ and T contains one integer divisible by 3, one integer congruent to 1 mod 3 and one integer congruent to 2 mod 3.

If T is a transversal of H in G, then by definition $|T| = |G/H|$, that is, T has the same size as the quotient set G/H. In fact, there is a natural bijective mapping $T \to G/H$ given by $t \mapsto tH$.

Assume now that H is normal, so that G/H is a group. Then we can define a binary operation $*$ on T so that $(T, *)$ is a group which is isomorphic to G/H. This can be done as follows: for each $g \in G$ denote by $\bar{g}$ the unique element of T which lies in the coset gH. Note that $\bar{g} = g \iff g \in T$. Now define a binary operation $*$ on T by setting

$$t_1 * t_2 = \overline{t_1 t_2} \text{ for all } t_1, t_2 \in T \qquad (!!!)$$

The following proposition is left as an exercise:

Proposition 23.2. *$(T, *)$ is a group, which is isomorphic to G/H via the map $\iota : T \to G/H$ given by $\iota(t) = tH$.*

We can now use Proposition 23.2 to give a new "interpretation" of the cylcic groups $\mathbb{Z}_n$ and also better visualize the quotient group $\mathbb{R}/\mathbb{Z}$.

Example A: Let $n \geq 2$ be an integer. We already proved that the quotient group $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$.

Let $G = \mathbb{Z}$, $H = n\mathbb{Z}$ and $T = \{0, 1, \ldots, n-1\}$. Then T is clearly a transversal of H in G, and in the above notations for any $x \in \mathbb{Z}$ we have

$$\overline{x} = \text{ the remainder of dividing } x \text{ by } n.$$

Thus, by Proposition 23.2, $G/H = \mathbb{Z}/n\mathbb{Z}$ is isomorphic to the following group which we denote by $\mathbb{Z}'_n$:

As a set $\mathbb{Z}'_n = \{0, 1, \ldots, n-1\}$, the set of integers from 0 to $n-1$. The group operation $+'$ on $\mathbb{Z}'_n$ is defined by

$$x +' y = \text{ the remainder of dividing } x + y \text{ by } n.$$

From this description you can see that $\mathbb{Z}'_n$ is essentially the same group as $\mathbb{Z}_n$ except for minor notational differences. In fact, if we defined $\mathbb{Z}_n$ as we did in Lecture 2 (at the very beginning of the course), then the group $(\mathbb{Z}_n, +)$ would be precisely $\mathbb{Z}'_n$ as defined above.

Example B: Now let $G = \mathbb{R}$ (with addition) and $H = \mathbb{Z}$. Let

$$T = [0, 1) = \{x \in \mathbb{R} : 0 \leq x < 1\} \subset \mathbb{R}.$$

We claim that T is a transversal of H in G. Indeed, the cosets of H have the form $x + \mathbb{Z}$, with $x \in \mathbb{R}$, and it is easy to see that $x + \mathbb{Z}$ will contain precisely one element of T, namely the fractional part of x, denoted by $\{x\}$. For instance, let $x = 2.1$. Then

$$x + \mathbb{Z} = \{\ldots, -0.9, 0.1, 1.1, 2.1, 3.1, \ldots\},$$

and the unique number in $(x + \mathbb{Z}) \cap T$ is $0.1 = \{2.1\}$.

Thus, T is a transversal of $\mathbb{Z}$ in $\mathbb{R}$, and in the above notations for every $x \in \mathbb{R}$ we have $\overline{x} = \{x\}$. Applying Proposition 23.2, we get the following conclusion: introduce the group operation $+'$ on $T = [0, 1)$ by

$$x +' y = \{x + y\}.$$

Then $(T, +')$ is isomorphic to $\mathbb{R}/\mathbb{Z}$. Note that the operation $+'$ on T can be more explicitly described as follows: for every $x, y \in T$ we have

$$x +' y = \begin{cases} x + y & \text{if } x + y < 1 \\ x + y - 1 & \text{if } x + y \geq 1. \end{cases}$$

(we have only two case above because if $x, y \in T$, then $0 \le x, y < 1$, so $0 \le x + y < 2$).

Let us go back to the general case. Let G be a group, H a normal subgroup, and suppose that we found a transversal T which itself is a subgroup of G. Then for any $t_1, t_2 \in T$ we have $t_1 t_2 \in T$, so $\overline{t_1 t_2} = t_1 t_2$. Therefore, the formula (!!!) for the operation $*$ on T simplifies to $t_1 * t_2 = t_1 t_2$. In other words, in this case the newly defined operation $*$ on T coincides with the group operation on G restricted to T. Therefore, we obtain the following useful result as a consequence of Proposition 23.2.

Corollary 23.3. *Let G be a group and H a normal subgroup of G. Assume that there exists a transversal T of H in G such that T is also a subgroup. Then the quotient group G/H is isomorphic to T (considered as a subgroup of G).*

We finish with two examples – in the first one there will exist a transversal which is a subgroup, and in the second one there will be no such transversal.

Example 1: Let $G = \mathbb{Z}_6$ and $H = \langle [3] \rangle = \{[0], [3]\}$. Then H has three cosets: $H = \{[0], [3]\}$, $[1] + H = \{[1], [4]\}$ and $[2] + H = \{[2], [5]\}$. The simplest possible transversal $\{[0], [1], [2]\}$ is not a subgroup, but there is another one that works: $T = \{[0], [2], [4]\}$ is also a transversal, and it is clearly a subgroup (e.g. because it coincides with $\langle [2] \rangle$, the cyclic subgroup generated by $[2]$).

Example 2: Now let $G = \mathbb{Z}$ and $H = 3\mathbb{Z}$. We claim that no transversal can be a subgroup here. Indeed, in this example, as we saw earlier, every transversal has 3 elements. On the other hand, we know any subgroup of $\mathbb{Z}$ is equal to $n\mathbb{Z}$ for some n, and

$$|n\mathbb{Z}| = \begin{cases} \infty & \text{if } n \neq 0 \\ 1 & \text{if } n = 0 \end{cases}$$

In particular, $\mathbb{Z}$ has no subgroups of order 3, so none of them could be a transversal of $H = 3\mathbb{Z}$.

23.4. **Book references.** The general references for this lecture are [Pinter, Chapter 16] and [Gilbert, 4.6]. None of the books discusses transversals. In Pinter's terminology FTH (which he calls FHT) is a special case of what we called FTH dealing with surjective homomorphisms (our Corollary 22.5). Pinter proves FTH as a consequence of another result (Theorem 1 in Chapter 16) which is useful by itself.