Section III.14. Factor Groups

Note. In the previous section we used a homomorphism φ to map the cosets of $H = \text{Ker}(\varphi)$ one to one and into group G' where $\varphi : G \to G'$. In fact, φ is one to one and onto $\varphi[G]$, which we know to be a group by Theorem 13.2 Part (3). So we should be able to make a group out of the cosets of $H = \text{Ker}(\varphi)$ and the group should be isomorphic to $\varphi[G]$. In this section, we make this clear and explicitly define the binary operation on the cosets. The group of cosets of $H = \text{Ker}(\varphi)$ is called a *factor group*.

Theorem 14.1. Let $\varphi : G \to G'$ be a group homomorphism with kernel $H = \text{Ker}(\varphi)$. Then the cosets of $H = \text{Ker}(\varphi)$ form a *factor group*, G/H, where $(aH) \cdot (bH) = (ab)H$. Also, the map $\mu : G/H \to \varphi[G]$ defined by $\mu(aH) = \varphi(a)$ is an isomorphism. Both coset multiplication and μ are well defined (i.e., independent of the choices of a and b from the cosets).

Example 14.2. Define $\gamma : \mathbb{Z} \to \mathbb{Z}_n$ as $\gamma(m) \equiv m \pmod{n}$. Then γ is a homomorphism by Example 13.10. $\text{Ker}(\gamma) = \{m \in \mathbb{Z} \mid m \equiv 0 (\text{mod } n)\} = n\mathbb{Z}$. The cosets of $\text{Ker}(\gamma) = n\mathbb{Z}$ are (remember, $\mathbb{Z}$ and $\mathbb{Z}_n$ are both additive groups):

$$\begin{aligned} n\mathbb{Z} = 0 + n\mathbb{Z} &= \{\ldots, -2n, -n, 0, n, 2n, \ldots\} \\ 1 + n\mathbb{Z} &= \{\ldots, -2n+1, -n+1, 1, n+1, 2n+1, \ldots\} \\ 2 + n\mathbb{Z} &= \{\ldots, -2n+2, -n+2, 2, n+2, 2n+2, \ldots\} \\ &\vdots \end{aligned}$$

$$(n-1)+n\mathbb{Z} \;=\; \{\ldots,-n-1,-1,n-1,2n-1,3n-1,\ldots\}.$$

These cosets are the *residue classes modulo n*. The mapping μ of Theorem 14.1 is $\mu : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}_n$ where $\mu(m+n\mathbb{Z}) = m$ for each $m+n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$. To illustrate how addition of the cosets is well-defined, notice that if we choose any elements of $3+n\mathbb{Z}$ and $(n-1)+n\mathbb{Z}$, say $5n+3$ and $-n-1$, then we have

$$\mu((3+n\mathbb{Z})+((n-1)+n\mathbb{Z})) = \gamma(5n+3)+\gamma(-n-1) = (5n+3)(\text{mod } n)+(-n-1)(\text{mod } n)$$

$$= 5n+3+(-n-1)(\text{mod } n) = (4n+2)(\text{mod } n) = 2.$$

Since we do addition modulo n, any representatives of the two cosets will also yield the same result, 2 here.

Note. The group G/H is at present only defined when H is the kernel of some homomorphism between group G and some other group G'. Next, we will define G/H for any H a normal subgroup of G (recall that H is a normal subgroup if the left and right cosets of H coincide—that is, $aH = Ha$ for all $a \in G$—and of course $\text{Ker}(\varphi)$ is a normal subgroup). A group G/H produced in this way is called a *factor group*, a *factor group G modulo H*, or a *quotient group*, and "G/H" is read as "G over H," "G modulo H," or "G mod H." Elements in the same cosets are said to be *congruent modulo H*.

Note. We have seen how coset multiplication is well-defined in Theorem 14.1 since left cosets coincide with right cosets for $H = \text{Ker}(\varphi)$ and φ a homomorphism

$G \to G'$. However, we can generate cosets of a group G using any subgroup H of G. As the next result shows, coset multiplication can be well-defined *only* when left and right cosets of H coincide and we know that this occurs for normal subgroups of G (this is the *definition* of H is a normal subgroup of G, $H \triangleleft G$).

Theorem 14.4. Let H be a subgroup of a group G. Then left coset multiplication is well-defined by the equation $(aH) \cdot (bH) = (ab)H$ if and only if H is a normal subgroup of G.

Note. We now just need to confirm that the binary operation of Theorem 14.4 actually produces a group of cosets of normal subgroup H of G.

Corollary 14.5. Let H be a normal subgroup of G. Then the cosets of H form a group G/H under the binary operation $(aH) \cdot (bH) = (ab)H$.

Definition 14.6. The group G/H in Corollary 14.5 is the *factor group* (or *quotient group*) of G by H.

Example. Consider $\mathbb{R}$ under addition. This is an abelian group, so all subgroups are normal. Consider the subgroup $\langle 2\pi \rangle$. $\langle 2\pi \rangle$ contains all integer multiples of 2π. For each $x \in [0, 2\pi)$ we get the coset $x + \langle 2\pi \rangle$ (so this is an example of an uncountably infinite number of cosets). Coset $x + \langle 2\pi \rangle$ includes all values of angles coterminal with the angle of measure x. So the group $\mathbb{R}/\langle 2\pi \rangle$ involves addition "modulo 2π." For example,

$$(\pi + \langle 2\pi \rangle) + (3\pi/2 + \langle 2\pi \rangle) = \pi/2 + \langle 2\pi \rangle.$$

In fact, $\mathbb{R}/\langle 2\pi \rangle$ is isomorphic to the group U of all complex numbers of magnitude 1 under multiplication. The isomorphism is $\varphi(x + \langle 2\pi \rangle) = \cos x + i \sin x$.

Note. Initially, we defined the factor groups G/H using a homomorphism φ with $H = \text{Ker}(\varphi)$ (in Theorem 14.1). Then, in Corollary 14.5, we constructed G/H using any normal subgroup without an appeal to a homomorphism. The following result shows that the normal subgroup is the kernel of a certain homomorphism, so the approaches of Theorem 14.1 and Corollary 14.5 are closely related.

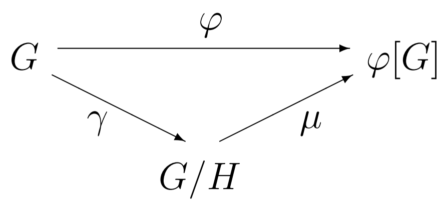
Theorem 14.9. Let H be a normal subgroup of G. Then $\gamma : G \to G/H$ given by $\gamma(x) = xH$ is a homomorphism with kernel H.

Theorem 14.11. The Fundamental Homomorphism Theorem.
Let $\varphi : G \to G'$ be a group homomorphism with kernel H, and let $\gamma : G \to G/H$ be the homomorphism given by $\gamma(g) = gH$ of Theorem 14.9. Then:

1. $\varphi[G]$ is a group,
2. $\mu : G/H \to \varphi[G]$ given by $\mu(gH) = \varphi(g)$ is an isomorphism, and
3. $\varphi(g) = \mu(\gamma(g)) = \mu \circ \gamma(g)$ for each $g \in G$.

μ is called the *canonical* (or *natural*) *isomorphism* between G/H and $\varphi[G]$. γ is similarly the *canonical* (or *natural*) *homomorphism* between G and G/H.

Note. We can map the relationship between φ, γ, and μ as:



This shows that any homomorphism $\varphi : G \to G'$ can be "factored" into a composition of the homomorphism $\gamma : G \to G/H$ of Theorem 14.9 and the isomorphism $\mu : G/H \to \varphi[G]$ of Theorem 14.1 (this is the real claim of The Fundamental Homomorphism Theorem).

Exercise 14.6. Find the order of $\mathbb{Z}_{12} \times \mathbb{Z}_{18}/\langle(4,3)\rangle$.

Theorem 14.13. Let G be a group and H a subgroup of G. The following are equivalent.

1. $gH = Hg$ for all $g \in G$ (that is, H is a normal subgroup).
2. $ghg^{-1} \in H$ for all $g \in G$ and for all $h \in H$.
3. $gHg^{-1} = H$ for all $g \in G$.

Definition 14.15a. An isomorphism $\varphi : G \to G$ of a group with itself is an *automorphism* of G.

Exercise 13.29. Let G be a group and let $g \in G$. Let $i_g : G \to G$ be defined by $i_g(x) = gxg^{-1}$ for $x \in G$. The i_g is an automorphism of G.

Definition 14.15b. Automorphism i_g of Exercise 13.29 is called the *inner automorphism of G by g*. Applying i_g to x is called *conjugation of x by g*.

Note. By Theorem 14.13, we see that H is a normal subgroup of G if and only if $i_g[H] = H$ for all $g \in G$ (this is (1) iff (3) in my statement of Theorem 14.13). In this case when $i_g[H] = H$, H is called an *invariant* of i_g. So the normal subgroups of G are precisely those which are invariant under inner automorphisms (for all $g \in G$, that is). In general, a subgroup K of G is called a *conjugate subgroup* of subgroup H if $K = i_g[H]$ for some $g \in G$. Exercise 14.27 shows that subgroup conjugacy forms an equivalence relation on the set of subgroups of a given group G.

Revised: 7/14/2023