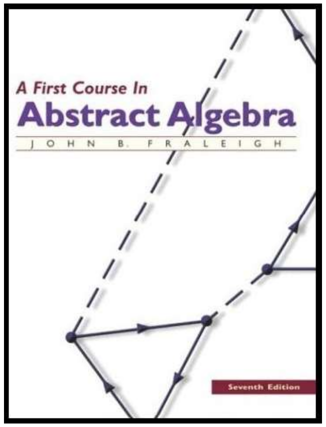
Introduction to Modern Algebra

Part III. Homomorphisms and Factor Groups

III.15. Factor-Group Computations and Simple Groups



Lemma

Lemma. If G is a finite group and N is a subgroup of G where $|N| = |G|/2$, then N is a normal subgroup of G.

Proof. Since all cosets of N must be the same size and the cosets partition G, then there are only two cosets of N, namely N and aN where $a \in G \setminus N$. Now for any $g \in G$, (1) if $g \in N$ then $gN = Ng = N$, and (2) if $g \in G \setminus N$ then $gN = Ng$ since this is the only coset of N other than N itself. So $gN = Ng$ for all $g \in G$, and N is a normal subgroup. □

Example 15.6

Example 15.6. Falsity of the Converse of the Theorem of Lagrange. We have claimed in the past that the alternating group A_4 (of order $4!/2 = 12$) does not have a subgroup of order 6. Recall that Lagrange's Theorem states that the order of a subgroup divides the order of its group. This example shows that there may be divisors of the order of a group which may not be the order of a subgroup.

Proof. Suppose, to the contrary, that H is a subgroup of A_4 of order 6. By Lemma, H must be a normal subgroup of G. Then A_4/H has only two elements, H and σH where $\sigma \in A_n \setminus H$. Since A_4/H is a group of order 2, then it is isomorphic to $\mathbb{Z}_2$ and the square of each element (coset) is the identity (H). So $H \cdot H = H$ and $(\sigma H) \cdot (\sigma H) = \sigma^2 H = H$. So if $\alpha \in H$ then $\alpha^2 \in H$ and if $\beta \notin H$ (then $\beta \in \sigma H$) then $\beta^2 \in H$. So, the square of every element of A_4 is in H.

Example 15.6 (continued)

Example 15.6. Falsity of the Converse of the Theorem of Lagrange. We have claimed in the past that the alternating group A_4 (of order $4!/2 = 12$) does not have a subgroup of order 6. Recall that Lagrange's Theorem states that the order of a subgroup divides the order of its group. This example shows that there may be divisors of the order of a group which may not be the order of a subgroup.

Proof (continued). But in A_4 we have

$$(1,2,3) = (1,3,2)^2 \text{ and } (1,3,2) = (1,2,3)^2$$

$$(1,2,4) = (1,4,2)^2 \text{ and } (1,4,2) = (1,2,4)^2$$

$$(1,3,4) = (1,4,3)^2 \text{ and } (1,4,3) = (1,3,4)^2$$

$$(2,3,4) = (2,4,3)^2 \text{ and } (2,4,3) = (2,3,4)^2.$$

So all 8 of the above (distinct) permutations are in H. This is a contradiction, since we assumed $|H| = 6$. Therefore no such H exists. □

Exercise 15.6

Exercise 15.6. Classify $\mathbb{Z} \times \mathbb{Z}/\langle(0,1)\rangle$ according to the Fundamental Theorem of Finitely Generated Abelian Groups.

Solution. Notice $\langle(0,1)\rangle = \{0\} \times \mathbb{Z} = H$ and the cosets are $(x,y) + \{0\} \times \mathbb{Z} = \{x\} \times (\mathbb{Z} + y) = \{x\} \times \mathbb{Z}$ for all $(x,y) \in \mathbb{Z} \times \mathbb{Z}$. Now $\{x\} \times \mathbb{Z}$ is isomorphic to $\mathbb{Z}$ (define $\varphi(\{x\} \times \mathbb{Z}) = x$ and φ is an isomorphism). So $\mathbb{Z} \times \mathbb{Z}/\langle(0,1)\rangle$ is isomorphic to $\mathbb{Z}$. □

Theorem 15.8

Theorem 15.8. Let $G = H \times K$ be the direct product of groups H and K. Then $H = \{(h,e) \mid h \in H\}$ is a normal subgroup of G. Also, $G/\widetilde{H}$ is isomorphic to K. Similarly $G/\widetilde{G}$ is isomorphic to H where $\widetilde{K} = \{(e,k) \mid k \in K\}$.

Proof. Define $\pi_2 : H \times K \to K$ where $\pi_2(h,k) = k$. Then π_2 is a projection map (see Example 13.8) and so is a homomorphism. Now, $\text{Ker}(\pi_2) = \widetilde{H}$ and so $\widetilde{H}$ is a normal subgroup of $H \times K$ by Theorem 13.15. Since π_2 is onto K then by Theorem 14.11, $(H \times K)/\widetilde{H} \cong K$ (here, $H \times K$ plays the role of G, and K plays the role of $\varphi[G]$ is Theorem 14.11). □

Theorem 15.9

Theorem 15.9. A factor group of a cyclic group is cyclic.

Proof. Let G be cyclic where $\langle a\rangle = G$. Let N be a normal subgroups of G. Next, G/N consists of all cosets of N. Let $gN \in G/N$ where $g \in G$. Since a generates G, $g = a^n$ for some $n \in \mathbb{Z}$, and $gN = (aN)^n = a^n N$. Therefore $G/N = \langle aN\rangle$ and G/N is cyclic, as claimed. □

Exercise 15.4

Exercise 15.4. Classify $(\mathbb{Z}_4 \times \mathbb{Z}_8)/\langle(1,2)\rangle$.

Solution. Notice $\langle(1,2)\rangle = \{(1,2),(2,4),(3,6),(0,0)\} = H$ and so $|\mathbb{Z}_4 \times \mathbb{Z}_8/\langle(1,2)\rangle| = 4 \times 8/4 = 8$. All groups are abelian, including the factor group. The abelian groups of order 8 are $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, and $\mathbb{Z}_8$ (we don't distinguish between $\mathbb{Z}_2 \times \mathbb{Z}_4$ and $\mathbb{Z}_4 \times \mathbb{Z}_2$). We try to determine which of these three choices is correct by considering orders of elements of the factor group. Consider the coset $(0,1) + H$. The order of this coset is 8 since:

$$\underbrace{((0,1)+H) + ((0,1)+H) + \cdots + ((0,1)+H)}_{k \text{ times}} = (0,k) + H$$

and the smallest value of k for which this yields the identity is $k = 8$. Since the only choice from the three groups which has elements of order 8 is $\mathbb{Z}_8$, then the factor group must be isomorphic to $\mathbb{Z}_8$. □

Theorem 15.18

Theorem 15.18. M is a maximal normal subgroup of G if and only if G/M is simple.

Proof. Let M be a maximal normal subgroup of G. Define $\gamma : G \to G/M$ as $\gamma(g) = gM$. Then by Theorem 14.9, γ is a homomorphism with $\text{Ker}(\gamma) = M$. ASSUME G/M is *not* simple and that N' is a proper nontrivial normal subgroup of G/M. Then by Theorem 15.16, $\gamma^{-1}[N']$ is a normal subgroup of G. Since N' is nontrivial then $N' \neq \{e\} = \{M\}$ (remember M is the identity in G/M). Also, we have $\text{Ker}(\gamma) = M$, so $\text{Ker}(\gamma) \neq N'$ and $\varphi^{-1}[N'] \neq M$. But $\{e\} = \{M\} \subsetneq N'$ and so $M \subsetneq \varphi^{-1}[N']$. So $\varphi^{-1}[N']$ properly contains M. Since N' is a proper subgroup of G/M, then it contains some but not all of the cosets of M. Since the cosets of M partition G (Section II.10), then $\varphi^{-1}[N']$ contains some but not all elements of G. That is, $\varphi^{-1}[N']$ is a proper subgroup of G. Therefore, $\varphi^{-1}[N']$ is a nontrivial proper normal subgroup of G which properly contains M. But this CONTRADICTS the maximality M. So no such N' exists and G/M is simple, as claimed.

Theorem 15.18 (continued)

Proof (continued). Now let G/M be simple. ASSUME that M is *not* a maximal normal subgroup and that there is a proper normal subgroup N of G properly containing M (i.e., $M \subsetneq N \subsetneq G$). Then by Theorem 15.16, $\gamma[N]$ is a normal subgroup of $\gamma[G] = G/M$ where γ is as defined above. Now $\text{Ker}(\gamma) = \{M\}$ (remember that M is the identity in G/M). Hence $\gamma[N]$ is a nontrivial normal subgroup of G/M. Now we show that $\gamma[N]$ is a proper subgroup of G/M. Recall that γ maps elements of G to cosets of M. So the only way that $\gamma[N] = G/M$ is if N contains an element of each coset of M. But we assumed $M \subsetneq N$, and so if N contains an element of each coset of M, then (since N is a group and so is closed under the binary operation) N must contain all cosets of M—that is, $M = G$. But this CONTRADICTS the choice of N as a proper subgroup of G. Hence N does not contain an element from each coset of M and $\gamma[N] \neq G/M$. That is, $\gamma[N] \subsetneq G/M$. Therefore, $\gamma[N]$ is a proper nontrivial subgroup of G/M. But this contradicts the fact that G/M is simple. Therefore, no such N exists and M is a maximal normal subgroup of G, as claimed. □

Theorem 15.20

Theorem 15.20. Let G be a group. Then the set $C = \left\{aba^{-1}b^{-1} \mid a, b \in G\right\}$ is a subgroup of G. Additionally, C is a normal subgroup of G then G/N is abelian if and only if $C \leq N$.

Proof. Since C is a subset of G, associativity of the binary operation is inherited from G and G_1 holds. Taking $a = e$, we see that $aba^{-1}be \in C$, we see that $aba^{-1}b^{-1} = e \in C$ and G_2 holds. If $x \in C$, then $x = aba^{-1}b^{-1}$ and $x^{-1} = bab^{-1}a^{-1} \in C$ and G_3 holds. Hence C is a group, as claimed.

For normality, let $x \in C$ and $g \in G$. Then $x = cdc^{-1}d^{-1}$ for some $c, d \in G$. Hence

$$\begin{aligned} g^{-1}xg &= g^{-1}\left(cdc^{-1}d^{-1}\right)g = g^{-1}\left(cdc^{-1}ed^{-1}\right)g \\ &= g^{-1}cdc^{-1}\left(gd^{1}dg^{-1}\right)d^{-1}g \text{ since } e = gd^{-1}dg^{-1} \\ &= \left[\left(g^{-1}c\right)d\left(g^{-1}c\right)^{-1}d^{-1}\right]\left[dg^{-1}d^{-1}g\right]\ldots \end{aligned}$$

Theorem 15.20 (continued).

Proof (continued). ...

$$\begin{aligned} g^{-1}xg &= \left[\left(g^{-1}c\right)d\left(g^{-1}c\right)^{-1}d^{-1}\right]\left[dg^{-1}d^{-1}g\right] \in C \\ & \quad \text{since } \left(g^{-1}c\right)d\left(g^{-1}c\right)^{-1}d^{-1}, \end{aligned}$$

so that $dg^{-1}d^{-1}g \in C$. So $g^{-1}xg \in C$ and C is a normal subgroup of G by Theorem 14.13, as claimed.

Now let N be a normal subgroup of G $(N \triangleleft G)$. Suppose G/n is abelian. Then for all $a, b \in G$ $\left(a^{-1}b^{-1}\right)N = \left(a^{-1}N\right)\left(b^{-1}N\right) = \left(b^{-1}N\right)\left(a^{-1}N\right) = b^{-1}a^{-1}N$ or $\left(aba^{-1}b^{-1}\right)N = N$ and so $aba^{-1}b^{-1} \in N$ and $C \leq N$.

Let N be a normal subgroup of G. Suppose $C \leq N$. Then for all $a, b \in G$ $(aN)(bN) = (ab)N = ab\left(b^{-1}a^{-1}ba\right)N$, since $b^{-1}a^{-1}ba \in C \subseteq N = baN = (bN)(aN)$, and so G/N is abelian, as claimed. □