THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 3030 Abstract Algebra 2023-24
Homework 4 Answer

Compulsory Part

1. Show that the center of a direct product is the direct product of the centers, i.e.

$$Z(G_1 \times G_2 \times \cdots \times G_n) = Z(G_1) \times Z(G_2) \times \cdots \times Z(G_n).$$

Deduce that a direct product of groups is abelian if and only if each of the factors is abelian.

Proof. By induction, we only need to prove it for $n = 2$. Let $(z_1, z_2) \in Z(G_1 \times G_2)$, we have $(z_1, z_2)(g_1, g_2) = (g_1, g_2)(z_1, z_2) \Leftrightarrow (z_1g_1, z_2g_2) = (g_1z_1, g_2z_2) \Leftrightarrow z_1g_1 = g_1z_1,\ z_2g_2 = g_2z_2,\ \forall g_1, g_2 \in G_2, G_2$ respectively. which means that $Z(G_1 \times G_2) \simeq Z(G_1) \times Z(G_2)$.

For the last part, let $G = G_1 \times ... \times G_n$. Then G is abelian $\iff G = Z(G) \iff G_i = Z(G_i)$ for each $i \iff$ each G_i is abelian. ☐

2. Show that if G is nonabelian, then the quotient group $G/Z(G)$ is not cyclic.

[*Hint:* Show the equivalent contrapositive, namely, that if $G/Z(G)$ is cyclic then G is abelian (and hence $Z(G) = G$).]

Proof. Suppose that $G/Z(G) = \langle \overline{h} \rangle$ for some $h \in G$, where $\overline{h} = hZ(G)$. Then for any $g \in G$, $\overline{g} = \overline{h^i}$ for some $i \in \mathbb{Z}$. Then $g = h^i c$ for some $c \in Z(G)$. Then for any $g' \in G$, $g' = h^j c'$ for some $j \in \mathbb{Z}, c' \in Z(G)$. Then $gg' = h^i c h^j c' = h^{i+j} cc' = h^j c' h^i c = g'g$ because $c, c' \in Z(G)$. Since g, g' were two arbitrary elements in G, it follows that G is abelian. Therefore, nonabelian G can not have $G/Z(G)$ cyclic. ☐

3. Using the preceding question, show that a nonabelian group G of order pq where p and q are primes has a trivial center.

Proof. Let G be a nonabelian group of order pq, where p and q are primes (p, q may or may not be distinct). Since G is not abelian, $Z(G) \neq G$. Then $|G/Z(G)| > 1$. Since $|G/Z(G)|$ divides $|G| = pq$, $|G/Z(G)| = p, q$ or pq. By question 8, $G/Z(G)$ is not cyclic, hence not of prime order. Then $|G/Z(G)| = pq$, and so $|Z(G)| = 1$. It follows that the center $Z(G)$ is trivial. ☐

4. Let N be a normal subgroup of G and let H be any subgroup of G. Let $HN = \{hn \mid h \in H, n \in N\}$. Show that HN is a subgroup of G, and is the smallest subgroup containing both N and H.

Proof. Let N be a normal subgroup of G and let H be any subgroup of G. Then $e \in N$ and $e \in H$. Therefore, $e = ee \in HN$. Take $hn, h'n' \in HN$, where $h, h' \in H$, and $n, n' \in N$. Then $hn(h'n')^{-1} = hnn'^{-1}h'^{-1}$. Since $N \lhd G$, $h'nn'^{-1}h'^{-1} \in N$. Therefore, $h'nn'^{-1}h'^{-1} = n''$ for some $n'' \in N$. Then $nn'^{-1}h'^{-1} = h'^{-1}n''$, and $hn(h'n')^{-1} = hn(n')^{-1}(h')^{-1} = hh'^{-1}n'' \in HN$. It follows that HN is a subgroup of G.

Note that $H \subseteq HN$ and $N \subseteq HN$. Clearly, any subgroup containing both N and H will also contain HN. Therefore, HN is the smallest subgroup containing both N and H. $\square$

5. Show directly from the definition of a normal subgroup that if H and N are subgroups of a group G, and N is normal in G, then $H \cap N$ is normal in H.

Proof. (In the following $<$ means be a subgroup of, we do not distinguish $<$ and $\leq$.)

Let $H < G, N \lhd G$. Then $H \cap N$ is a subgroup of G contained in H, so $H \cap N < H$. For any $h \in H$, $n \in H \cap N$, $hnh^{-1} \in N$ because $N \lhd G$. Also, $h, n \in H$ implies that $hnh^{-1} \in H$. Therefore, $hnh^{-1} \in H \cap N$, and so $H \cap N \lhd H$. $\square$

6. Let H, K, and L be normal subgroups of G with $H < K < L$. Let $A = G/H, B = K/H$, and $C = L/H$.

   (a) Show that B and C are normal subgroups of A, and $B < C$.

   (b) To what quotient group of G is $(A/B)/(C/B)$ isomorphic?

Proof. (a) Let H, K, and L be normal subgroups of G with $H < K < L$. Let $\phi : G \to G/H$ be the natural projection: $\phi(g) = gH$ for any $g \in G$. Then $A = \phi(G), B = \phi(K), C = \phi(L)$. Since ϕ is surjective, it preserves normal groups, therefore, $B \lhd G$, and $C \lhd G$. Since $K < L$, $B = \phi(K) \subseteq \phi(L) = C$. Since B, C are both subgroups of A, $B < C$.

(b) By the third isomorphism theorem, $(A/B)/(C/B) \simeq A/C = (G/H)/(L/H) \simeq G/L$. $\square$

Optional Part

1. Let F be a field, and $n \in \mathbb{Z}_{>0}$.

   (a) Show that $SL_n(F)$ is a normal subgroup in $GL_n(F)$.

   (b) When F is a finite field, show that $[GL_n(F) : SL_n(F)] = |F| - 1$.

   Proof. (a) Note that $\mathrm{SL}_n(F)$ is the kernel of the determinant map $\det : \mathrm{GL}_n(F) \to F^\times$. Therefore, $\mathrm{SL}_n(F)$ is a normal subgroup in $\mathrm{GL}_n(F)$.

   (b) The map $\det$ in (a) is surjective: For any $\lambda \in F^\times$, $\det(\text{diag}(\lambda, 1, 1, ..., 1)) = \lambda$. Therefore, by the first isomorphism theorem, $\mathrm{GL}_n(F)/\mathrm{SL}_n(F) \simeq F^\times$. Therefore, $[\mathrm{GL}_n(F) : \mathrm{SL}_n(F)] = |F| - 1$.

   $\square$

2. Let $F = F^A$ be the free group on two generators $A = \{a, b\}$. Show that the normal subgroup generated by the single commutator $aba^{-1}b^{-1}$ is the commutator of F.

3. Show that the converse to the Theorem of Lagrange holds for an abelian group, namely, if G is a finite abelian group and $d \mid |G|$, then there exists a subgroup of G of order d.

   Proof. Let G be a finite abelian group and $d \mid |G|$. We may assume that $|G| \geq 2$. Then $G \simeq \mathbb{Z}_{d_1} \oplus ...\mathbb{Z}_{d_k}$, where $k \geq 1$, $d_1|d_2|...|d_k$, and $d_1 \geq 2$. We do induction on k.

   When $k = 1$, G is cyclic, and G has a subgroup of order d for each $d \mid |G|$.

   Suppose $k \geq 2$. Let $c = \gcd(d, d_k)$. Then $\gcd(\frac{d}{c}, \frac{d_k}{c}) = 1$. Since $d \mid |G|$, $\frac{d}{c} \mid \frac{|G|}{c} = \frac{|G|}{d_k} \cdot \frac{d_k}{c}$. Then $\frac{d}{c} \mid \frac{|G|}{d_k}$. By induction hypothesis, $c|d_k$ implies that $\mathbb{Z}_{d_k}$ has a subgroup H_2 of order c, and $\frac{d}{c} \mid \frac{|G|}{d_k}$ implies that $\mathbb{Z}_{d_1} \oplus ...\mathbb{Z}_{d_{k-1}}$ has a subgroup H_1 of order $\frac{d}{c}$. Therefore, $G \simeq \mathbb{Z}_{d_1} \oplus ...\mathbb{Z}_{d_{k-1}} \oplus \mathbb{Z}_{d_k}$ has a subgroup $H_1 \oplus H_2$ of degree d. $\square$

4. Prove that A_n is simple for $n \geq 5$, following the steps and hints given.

   (a) Show that A_n contains every 3-cycle if $n \geq 3$.

   (b) Show that A_n is generated by the 3-cycles for $n \geq 3$ [*Hint:* Note that $(a, b)(c, d) = (a, c, b)(a, c, d)$ and $(a, c)(a, b) = (a, b, c)$.]

   (c) Let r and s be fixed elements of $\{1, 2, \cdots, n\}$ for $n \geq 3$. Show that A_n is generated by the n "special" 3-cycles of the form (r, s, i) for $1 \leq i \leq n$. [*Hint:* Show every 3-cycle is the product of "special" 3-cycles by computing

   $$(r, s, i)^2,\ (r, s, j)(r, s, i)^2,\ (r, s, j)^2(r, s, i),$$

   and

   $$(r, s, i)^2(r, s, k)(r, s, j)^2(r, s, i).$$

   Observe that these products give all possible types of 3-cycles.]

(d) Let N be a normal subgroup of A_n for $n \geq 3$. Show that if N contains a 3-cycle, then $N = A_n$. [*Hint:* Show that $(r, s, i) \in N$ implies that $(r, s, j) \in N$ for $j = 1, 2, \cdots, n$ by computing

$$((r, s)(i, j))(r, s, i)^2((r, s)(i, j))^{-1}.]$$

(e) Let N be a nontrivial normal subgroup of A_n for $n \geq 5$. Show that one of the following cases must hold, and conclude in each case that $N = A_n$.

Case I N contains a 3-cycle.

Case II N contains a product of disjoint cycles, at least one of which has length greater than 3. [*Hint:* Suppose N contains the disjoint product $\sigma = \mu(a_1, a_2, \cdots, a_r)$. Show $\sigma^{-1}(a_1, a_2, a_3)\sigma(a_1, a_2, a_3)^{-1}$ is in N, and compute it.]

Case III N contains a disjoint product of the form $\sigma = \mu(a_4, a_5, a_6)(a_1, a_2, a_3)$. [*Hint:* Show $\sigma^{-1}(a_1, a_2, a_4)\sigma(a_1, a_2, a_4)^{-1}$ is in N, and compute it.]

Case IV N contains a disjoint product of the form $\sigma = \mu(a_1, a_2, a_3)$ where μ is a product of disjoint 2-cycles. [*Hint:* Show $\sigma^2 \in N$ and compute it.]

Case V N contains a disjoint product σ of the form $\sigma = \mu(a_3, a_4)(a_1, a_2)$, where μ is a product of an even number of disjoint 2-cycles.
[*Hint:* Show that $\sigma^{-1}(a_1, a_2, a_3)\sigma(a_1, a_2, a_3)^{-1}$ is in N, and compute it to deduce that $\alpha = (a_2, a_4)(a_1, a_3)$ is in N. Using $n \geq 5$ for the first time, find $i \neq a_1, a_2, a_3, a_4$ in $\{1, 2, \cdots, n\}$. Let $\beta = (a_1, a_3, i)$. Show that $\beta^{-1}\alpha\beta\alpha \in N$, and compute it.]

Proof. See p202 of Artin's Algebra. $\square$