THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 3030 Abstract Algebra 2023-24
Homework 3 Answer

Compulsory Part

1. Let N be a normal subgroup of a group G, and let $m = [G : N]$. Show that $a^m \in N$ for every $a \in G$.

   Proof. Let N be a normal subgroup of a group G and let $m = [G : N]$, the index of N in G. The group G/N has order m, so by Lagrange's theorem, the order of any element in G/N divides m.

   Consider an arbitrary element $a \in G$. The order of the left coset aN in G/N divides m. Then $(aN)^m = N$, so $a^m N = N$. Therefore $a^m \in N$. □

2. Prove that the **torsion subgroup** T (i.e. the set of all elements having finite orders) of an abelian group G is a normal subgroup of G, and that G/T is **torsion free** (meaning that the identity is the only element of finite order).

   Proof. First, $e \in T$ because $\operatorname{ord}(e) = 1$. For any $a, b \in T$, let $m = \operatorname{ord}(a)$ and $n = \operatorname{ord}(b)$, then $m, n \in \mathbb{Z}_{>0}$. Then $(ab^{-1})^{mn} = a^{mn}b^{-mn} = e$. Therefore, $\operatorname{ord}(ab^{-1}) < \infty$. Therefore, $ab^{-1} \in T$, and so $T < G$.

   Since G is abelian, any subgroup of G is normal, thus $T \lhd G$.

   Let $g \in G$. Suppose $gT \in G/T$ has finite order. Then $(gT)^k = eT$ for some $k \in \mathbb{Z}_{>0}$. Then $g^k \in T$, so (g^k) has finite order. Therefore, g also has finite order, so $g \in T$. Therefore, $gT = eT$. It follows that G/T is torsion-free.

   □

3. Let G and G' be groups, and let N and N' be normal subgroups of G and G' respectively. Let ϕ be a homomorphism of G into G'. Show that ϕ induces a natural homomorphism $\phi_* : G/N \to G'/N'$ if $\phi(N) \subseteq N'$. (This fact is used constantly in algebraic topology.)

   Proof. Let $\pi : G \to G/N$ and $\pi' : G' \to G'/N'$ be the projection maps. Consider $f = \pi' \circ \phi$. We claim that f vanishes on N. Let $h \in N$. Then $f(h) = \pi'(\phi(h)) = e$ since $\phi[N] \subseteq N'$ and $\pi'[N'] = \{e\}$. It follows that there is a unique homomorphism $\phi_* : (G/N) \to (G'/N')$ such that $\phi_* \circ \pi = \pi' \circ \phi$. □

4. Let H and K be groups and let $G = H \times K$. Recall that both H and K appear as subgroups of G in a natural way. Show that these subgroups H (actually $H \times \{e\}$) and K (actually $\{e\} \times K$) have the following properties.

   (a) Every element of G is of the form hk for some $h \in H$ and $k \in K$.

   (b) $hk = kh$ for all $h \in H$ and $k \in K$.

   (c) $H \cap K = \{e\}$.

Proof. We identify $h \in H$ with $(h, e) \in H \times K$, and identify $k \in K$ with $(e, k) \in H \times K$.

(a) For any $g \in G = H \times K$, $g = (h, k)$ for some $h \in H, k \in K$. Then $g = (h, e)(e, k) = hk$.

(b) For any $h \in H, k \in K$, $hk = (h, e)(e, k) = (h, k) = (e, k)(h, e) = kh$.

(c) For any $g = (h, k) \in G$, $g \in H \cap K$ if and only if $k = e, h = e$. Therefore, $H \cap K = \{e\}$.

□

5. Let H and K be subgroups of a group G satisfying the three properties listed in the preceding exercise. Show that for each $g \in G$, the expression $g = hk$ for $h \in H$ and $k \in K$ is unique. Then let each g be renamed (h, k). Show that, under this renaming, G becomes structurally identical (isomorphic) to $H \times K$.

Proof. Define $\phi : H \times K \to G$ by $\phi(h, k) = hk$.

Condition (a) says that for any $g \in G$, $g = hk = \phi(h, k)$ for some $h \in H, k \in K$. Therefore, ϕ is surjective.

For any $h_1, h_2 \in H, k_1, k_2 \in K$, $\phi(h_1, k_1)\phi(h_2, k_2) = h_1k_1h_2k_2 = h_1h_2k_1k_2 = \phi(h_1h_2, k_1k_2)$ by condition (b). Therefore, ϕ is a group homomorphism.

For $(h, k) \in H \times K$, if $\phi(h, k) = e$, then $hk = e$. Then $h = k^{-1} \in H \cap K = \{e\}$. Then $h = k = e$ by condition (c). Therefore, $\ker(\phi) = \{(e, e)\}$, and so ϕ is injective.

Therefore, $\phi : H \times K \to G$ is a group isomorphism. In particular, each $g \in G$ can be written in the form $hk = \phi(h, k)$, where $h \in H, k \in K$ in a unique way, and $\phi^{-1} : G \to H \times K$ defined by $\phi^{-1}(g) = (h, k)$ when $g = hk$ is an isomorphism. □

6. Let G, H, and K be finitely generated abelian groups. Show that if $G \times K$ is isomorphic to $H \times K$, then $G \simeq H$.

Proof. Let G, H, and K be finitely generated abelian groups. Suppose that $G \times K$ is isomorphic to $H \times K$. By the fundamental theorem of finitely generated abelian groups,

$G \simeq \mathbb{Z}^{r_1} \times \mathbb{Z}/q_1\mathbb{Z} \times ... \times \mathbb{Z}/q_{s_1}\mathbb{Z}$, $H \simeq \mathbb{Z}^{r_2} \times \mathbb{Z}/q'_1\mathbb{Z} \times ... \times \mathbb{Z}/q'_{s_2}\mathbb{Z}$, $K \simeq \mathbb{Z}^{r_3} \times \mathbb{Z}/q''_1\mathbb{Z} \times ... \times \mathbb{Z}/q''_{s_3}\mathbb{Z}$, where $r_1, r_2, r_3, s_1, s_2, s_3 \in \mathbb{Z}_{\geq 0}$, and each q_i, q'_i, q''_i are prime powers.

Since $G \times K \simeq H \times K$, $\mathbb{Z}^{r_1+r_3} \times \mathbb{Z}/q_1\mathbb{Z} \times ... \times \mathbb{Z}/q_{s_1}\mathbb{Z} \times \mathbb{Z}/q''_1\mathbb{Z} \times ... \times \mathbb{Z}/q''_{s_3}\mathbb{Z} \simeq \mathbb{Z}^{r_2+r_3} \times \mathbb{Z}/q'_1\mathbb{Z} \times ... \times \mathbb{Z}/q'_{s_2}\mathbb{Z} \times \mathbb{Z}/q''_1\mathbb{Z} \times ... \times \mathbb{Z}/q''_{s_3}\mathbb{Z}$.

By the uniqueness part of the above theorem, $r_1 + r_3 = r_2 + r_3$, $s_1 + s_3 = s_2 + s_3$, and $(q_1, ..., q_{s_1}, q''_1, ..., q''_{s_3})$ is the same as $(q'_1, ..., q'_{s_2}, q''_1, ..., q''_{s_3})$ up to reordering. Then $r_1 = r_2, s_1 = s_2$ and $(q_1, ..., q_{s_1})$ is the same as $q_1, ..., q_{s_1}$ up to reordering. Therefore, $G \simeq H$.

□

7. Suppose that H and K are normal subgroups of a group G with $H \cap K = \{e\}$. Show that $hk = kh$ for all $h \in H$ and $k \in K$.

Proof. Let $h \in H, k \in K$ be arbitrary. Then $h^{-1} \in H$ and $k^{-1} \in K$,

Since $H \lhd G$, $kh^{-1}k^{-1} \in H$ so $hkh^{-1}k^{-1} = h(kh^{-1}k^{-1}) \in H$.

Since $K \lhd G$, $hkh^{-1} \in K$, so $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} \in K$.

Therefore, $hkh^{-1}k^{-1} \in H \cap K = \{e\}$. Thus, $hk = kh$. □

Remark. Under condition 4(a), the condition 4(b) implies that 4(b'): H and K are both normal subgroups of G. Under condition 4(c), 4(b') implies 4(b) by question 7. Therefore the condition 4(b) may be replaced by condition 4(b'). This is what Artin did in chapter 2.11.

Optional Part

1. Given any subset S of a group G, show that it makes sense to speak of the smallest normal subgroup that contains S.

   Proof. Let $\{N_\alpha\}$ be the set of normal subgroups of G containing S. Then this set is nonempty as G is such a subgroup. By Exercise 6 in Compulsory part in HW2, $\bigcap N_\alpha \lhd G$. It is the smallest normal subgroup of G containing S. □

2. Prove that if a finite abelian group has order a power of a prime p, then the order of every element in the group is a power of p. Can the hypothesis of commutativity be dropped? Why, or why not?

   Proof. Let G be an abelian group of order p^n for some prime p and $n \geq 1$. Let $g \in G$. By Lagrange's theorem, the order of g, denoted $|g|$, divides the order of G, i.e. $|g|$ divides p^n. Since p is a prime number, any divisor of p^n must be a power of p. Hence, the order of every element in the group is a power of p.

   Note that the proof only uses Lagrange's theorem, and equally applies when the hypothesis of commutativity is dropped. □

3. Let G be a finite abelian group and let p be a prime dividing $|G|$. Prove that G contains an element of order p.

   Proof. By the structure theorem of finite generated abelian group, $G = \bigoplus_{i=1}^{n} \mathbb{Z}_{p_i^{r_i}}$. Since p divides $|G|$, thus there exists some $p_i = p$. Then the element $(0, ..., 0, p_i^{r_i-1}, 0, ...0)$ has order p, where $p_i^{r_i-1}$ appears on the $\mathbb{Z}_{p_i}$'s factor. □

4. Show that a finite abelian group is not cyclic if and only if it contains a subgroup isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$ for some prime p.

   Proof. Let G be a finite abelian group. We may assume that $|G| \geq 2$. Then $G \simeq \mathbb{Z}_{d_1} \times ...\mathbb{Z}_{d_k}$, where $k \in \mathbb{Z}_{>0}$, $d_1 \mid d_2 \mid ... \mid d_k$, and $d_1 \geq 2$. If G is not cyclic, then $k \geq 2$, and $\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2}$ is a subgroup of G. Choose any prime p dividing d_1. Then $\frac{d_1}{p}\mathbb{Z}_{d_1} \times \frac{d_2}{p}\mathbb{Z}_{d_2}$ is a subgroup of G isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$.

   Conversely, if G contains a subgroup H isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$ for some prime p. Then for any $g \in G$, $(gH)^{|G|/|H|} = H$ in the group G/H. Then $g^{|G|/|H|} \in H$. But $h^p = e$ for any $h \in H$. Then $g^{p|G|/|H|} = e$ for any $g \in G$. That is, any $g \in G$ has order $\leq p|G|/|H| = |G|/p$. Then G is not cyclic. □

5. If a group N can be realized as a normal subgroup of two groups G_1 and G_2, and if $G_1/N \cong G_2/N$, does it imply that $G_1 \cong G_2$? Give a proof or a counterexample.

   Proof. Consider the two groups: $\mathbb{Z} \times \{0\}$ and $2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, they have the same normal subgroup $2\mathbb{Z} \times \{0\}$ and the quotient groups are both isomorphic to $\mathbb{Z}/2\mathbb{Z}$. But the later group has an order 2 element while the first one does not. □

6. Suppose N is a normal subgroup of a group G such that N and G/N are finitely generated. Show that G is also finitely generated.

   Proof. Let N be a normal subgroup of a group G such that both N and G/N are finitely generated. This means that there exists a finite set $S = \{n_1, n_2, \ldots, n_k\}$ that generates N and another finite set $T = \{g_1N, g_2N, \ldots, g_lN\}$ that generates G/N, where each g_iN is a coset of N in G.

   Consider the set $U = S \cup \{g_1, g_2, \ldots, g_l\}$, where each g_i is a representative element from the coset gN_i. We claim that U generates G.

   To see this, take an arbitrary element $g \in G$. Because G/N is generated by T, we can write gN as a product of elements from T, say $gN = g_{i_1}^{a_1}Ng_{i_2}^{a_2}N \ldots g_{i_m}^{a_m}N$ for some integers $a_1, a_2, \ldots, a_m$.

   This means that g is in the coset $g_{i_1}^{a_1}g_{i_2}^{a_2} \ldots g_{i_m}^{a_m}N$. But since N is generated by S, we can write each $n \in N$ as a product of elements from S, say $n = n_{j_1}^{b_1}n_{j_2}^{b_2} \ldots n_{j_n}^{b_n}$ for some integers $b_1, b_2, \ldots, b_n$.

   Therefore, we can write g as a product of elements from U, which means that U generates G. Furthermore, U is a finite set because it is the union of two finite sets. Hence, G is finitely generated. □

7. Suppose N is a normal subgroup of a group G which is cyclic. Show that every subgroup of N is normal in G.

   Proof. Let N be a normal cyclic subgroup of G. This means there exists an element $n \in G$ such that $N = \langle n \rangle = \{n^k | k \in \mathbb{Z}\}$.

   Now let H be any subgroup of N. Since N is cyclic, H is also cyclic. So, there exists an $m \in \mathbb{Z}$ such that $H = \langle n^m \rangle$.

   We need to show that for all $g \in G$ and $h \in H$, $ghg^{-1} \in H$. We know that $h = (n^m)^p = n^{mp}$ for some integer p.

   Since N is normal in G, we have $gn^kg^{-1} \in N$ for all $k \in \mathbb{Z}$ and all $g \in G$. Therefore,

   $$ghg^{-1} = g(n^{mp})g^{-1} = (gn^kg^{-1})^p \in N.$$

   But since $ghg^{-1} = (n^m)^p = n^{mp} \in H$ (because H is generated by n^m), we have $ghg^{-1} \in H$ as required. □

8. Show that the isomorphism class of a direct product is independent of the ordering of the factors, i.e. $G_1 \times G_2 \times \cdots \times G_n$ is isomorphic to $G_{\sigma(1)} \times G_{\sigma(2)} \times \cdots \times G_{\sigma(n)}$ for any permutation $\sigma \in S_n$.

   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. □