Topics in Algebra solution

Sung Jong Lee, lovekrand.github.io

November 12, 2020

Problems in Section 2.13.

1. If A and B are groups, prove that $A \times B$ is isomorphic to $B \times A$.

Proof. Let us define a mapping $\phi : A \times B \to B \times A$ by $\phi((a, b)) = (b, a)$ for any $a \in A, b \in B$. We claim that ϕ is indeed a bijective homomorphism. From

$$\begin{aligned} \phi((a_1, b_1) \cdot (a_2, b_2)) &= \phi((a_1 a_2, b_1 b_2)) = (b_1 b_2, a_1 a_2) \\ &= (b_1, a_1) \cdot (b_2, a_2) = \phi((a_1, b_1)) \cdot \phi((a_2, b_2)) \end{aligned}$$

we can conclude that ϕ is a homomorphism. It is also injective since $\phi(e_a, e_b) = (e_b, e_a)$(e_a and e_b are identity elements of A and B respectively). Also from the definition of ϕ, it is clearly surjective. Hence, $A \times B \simeq B \times A$. □

2. If G_1, G_2, G_3 are groups, prove that $(G_1 \times G_2) \times G_3$ is isomorphic to $G_1 \times G_2 \times G_3$. Care to generalize?

Proof. Define a mapping $\phi : (G_1 \times G_2) \times G_3 \to G_1 \times G_2 \times G_3$ by

$$\phi(((g_1, g_2), g_3)) = (g_1, g_2, g_3), \quad \text{where } g_1 \in G_1,\ g_2 \in G_2,\ g_3 \in G_3.$$

ϕ is clearly a bijective homomorphism. Thus, $(G_1 \times G_2) \times G_3 \simeq G_1 \times G_2 \times G_3$. □

3. If $T = G_1 \times G_2 \times \cdots \times G_n$ prove that for each $i = 1, 2, \cdots, n$ there is a homomorphism ϕ_i of T onto G_i. Find the kernel of ϕ_i.

Proof. For each $i = 1, 2, \cdots, n$, define $\phi_i : T \to G_i$ by

$$\phi_i((g_1, g_2, \cdots, g_i, \cdots, g_n)) = g_i \in G_i$$

Then clearly ϕ_i is a homomorphism. Let K_i be the kernel of ϕ_i. Then

$$K_i = \{(g_1, g_2, \cdots, g_n) \in T : g_i = e_i\} = G_1 \times G_2 \times \cdots G_{i-1} \times (e_i) \times G_{i+1} \times \cdots \times G_n.$$

□

4. Let G be a group and let $T = G \times G$.
a) Show that $D = \{(g,g) \in G \times G : g \in G\}$ is a group isomorphic to G.

Proof. Define a mapping $\phi : D \to G$ by $\phi((g,g)) = g$. Then ϕ is a homomorphism. Moreover, ϕ has trivial kernel. Hence injective. Also from the definition itself, ϕ is surjective. Hence, $D \simeq G$. ☐

b) Prove that D is normal in T if and only if G is abelian.

Proof. Suppose D is normal. Then

$$(g,e)(d,d)(g^{-1},e) = (gdg^{-1},d) \in D \implies gd = dg$$

for all $g, d \in G$. Hence, G is abelian. Conversely, if G is abelian, for any $(d,d) \in D$, $(g,h) \in G \times G$, $(g,h)(d,d)(g^{-1},h^{-1}) = (d,d) \in D$ implying D is normal in T. Hence proved. ☐

5. Let G be a finite abelian group. Prove that G is isomorphic to the direct product of its Sylow subgroups.

Proof. Let $o(G) = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ where p_i are distinct primes. Let P_i denote the p_i-Sylow subgroups of G respectively. Since G is abelian, P_i's are normal in G. Hence, arbitrary product of P_i's form a subgroup in G. Also, from the fact that each p_i Sylow subgroups are p_i groups, $P_i \cap \prod_{k \neq i} P_k = (e)$. Thus, $o(G) = o(P_1)o(P_2)\cdots o(P_k) = o(P_1 P_2 \cdots P_k)$ and hence $G = P_1 P_2 \cdots P_k$. Now suppose $g = p_1 p_2 \cdots p_k$, $p_i \in P_i$ is not unique in its representation. So, we assume that there is $q_i \in P_i$, not every $p_i = q_i$, $q_1 q_2 \cdot q_k = p_1 p_2 \cdots p_k$. But since G is abelian and for each i,

$$q_i^{-1} p_i = (q_1^{-1} p_1)(q_2^{-1} p_2) \cdots (q_{i-1}^{-1} p_{i-1})(q_{i+1}^{-1} p_{i+1}) \cdots (q_k^{-1} p_k) \in P_i \cap \prod_{k \neq i} P_k = (e)$$

so that $p_i = q_i$. Hence, we conclude that G is (internal) direct product of its Sylow subgroups. ☐

6. Let A, B be cyclic groups of order m and n, respectively. Prove that $A \times B$ is cyclic if and only if m and n are relatively prime.

Proof. Let $G = A \times B$. Clearly, $o(G) = mn$. Suppose given G is cyclic but $\gcd(m,n) > 1$. Choose any $(a,b) \in G$. Let $k = \mathrm{lcm}(m,n)$. Then,

$$(a,b)^k = (a^k, b^k) = (e,e)$$

for all $(a,b) \in G$. Since $\gcd(m,n) > 1$, $k = \mathrm{lcm}(m,n) < mn$. Thus, G does not admit a generator, which is clearly a contradiction. Conversely, assume that $\gcd(m,n) = 1$. Let a and b be the generators of A and B respectively. Set d be the order of (a,b). We know that $(a,b)^k = (e,e)$ so that $d \mid k$. Also, from the fact that $a^d = e, b^d = e$, $m \mid d$ and $n \mid d$ so that $k \mid d$. This shows that $d = k = \mathrm{lcm}(m,n) = mn$, and hence G admits a generator. ☐

7. Use the result of Problem 6 to prove the Chinese Remainder Theorem; namely, if m and n are relatively prime integers and u, v any two integers, then we can find an integer x such that $x \equiv u \pmod{m}$ and $x \equiv v \pmod{n}$.

Proof. Let a and b be the generators of A and B respectively, where A and B are cyclic groups of order m and n. Note that (a, b) is a generator for the cyclic group $A \times B$. Choose $a^u \in A, b^v \in B$. Then there will be an integer x such that

$$(a, b)^x = (a^x, b^x) = (a^u, b^v) \iff x \equiv u \pmod{m}, \quad x \equiv v \pmod{n},$$

thereby proving the theorem. □

8. Give an example of a group G and normal subgroups $N_1, N_2, \cdots, N_n$ such that $G = N_1 N_2 \cdots N_n$ and $N_i \cap N_j = (e)$ for $i \neq j$ and yet G is not the internal direct product of $N_1, \cdots, N_n$.

Solution. Take a Klein-4 group $G = \{e, a, b, ab\}$. Consider the normal subgroups $N_1 = \{e, a\}$, $N_2 = \{e, b\}$, $N_3 = \{e, ab\}$. Then clearly $G = N_1 N_2 N_3$ and $N_i \cap N_j = (e)$ for all $i \neq j$. But $ab = a \cdot b \cdot e = e \cdot e \cdot ab$ which shows that representation of $ab \in G$ is not unique in such decomposition. Hence, G is not the internal direct product of N_1, N_2 and N_3. □

9. Prove that G is the internal direct product of the normal subgroups $N_1 \cdots, N_n$ if and only if
1) $G = N_1 \cdots N_n$.
2) $N_i \cap (N_1 N_2 \cdots N_{i-1} N_{i+1} \cdots N_n) = (e)$ for $i = 1, \cdots, n$.

Proof. Suppose G is the internal direct product of N_i's. Clearly 1) must hold. Also, if there are $m_i \in N_i$ such that

$$\begin{aligned} m_i &= m_1 m_2 \cdots m_{i-1} m_{i+1} \cdots m_n \in N_i \cap (N_1 N_2 \cdots N_{i-1} N_{i+1} \cdots N_n) \\ &\iff e \cdots e \cdot m_i \cdot e \cdots e = m_1 m_2 \cdots m_{i-1} \cdot e \cdot m_{i+1} \cdots m_n, \end{aligned}$$

then by the uniqueness of representation in internal products, $m_i = e$ for all $i = 1, \cdots, n$. Hence, 2) is also satisfied. Conversely, we assume that the conditions 1) and 2) are true. It is enough to show the uniqueness of representation of the elements in the product. Suppose not. That is, there are more than one representation of $g \in G$ as

$$g = m_1 m_2 \cdots m_n = k_1 k_2 \cdots k_n$$

where $m_i, k_i \in N_i$. Using that every N_i is normal in G, observe that

$$
\begin{aligned}
&m_1 m_2 \cdots m_n = k_1 k_2 \cdots k_n \\
&\iff (k_1)^{-1} m_1 = k_2 \cdots k_n \cdot m_n^{-1} m_{n-1}^{-1} \cdots m_2^{-1} \\
&\iff (k_1)^{-1} m_1 = k_2 (k_3 \cdots k_n m_n^{-1} \cdots m_3^{-1}) m_2^{-1} \\
&\iff (k_1)^{-1} m_1 = k_2 (k_3 \cdots k_n m_n^{-1} \cdots m_3^{-1}) m_2^{-1} \cdot (k_3 \cdots k_n m_n^{-1} \cdots m_3^{-1})^{-1} \cdot (k_3 \cdots k_n m_n^{-1} \cdots m_3^{-1}) \\
&\iff (k_1)^{-1} m_1 = k_2 m_2' \cdot (k_3 \cdots k_n m_n^{-1} \cdots m_3^{-1}) \quad \text{for some } m_2' \in N_2 \\
&\iff (k_1)^{-1} m_1 = (k_2 m_2')(k_3 m_3') \cdot (k_4 \cdots k_n m_n^{-1} \cdots m_4^{-1}) \quad \text{for some } m_3' \in N_3 \\
&\iff (k_1)^{-1} m_1 = (k_2 m_2')(k_3 m_3') \cdots (k_n m_n') \quad \text{for some } m_i' \in N_i \\
&\iff k_1 = m_1.
\end{aligned}
$$

Repeating the above process, we can conclude that $k_i = m_i$ for each $i = 1, \cdots, n$. Thus, G is the internal direct product of N_i's. □

10. Let G be a group, $K_1, \cdots, K_n$ normal subgroups of G. Suppose that $K_1 \cap K_2 \cap \cdots \cap K_n = (e)$. Let $V_i = G/K_i$. Prove that there is an isomorphism of G into $V_1 \times V_2 \times \cdots \times V_n$.

Proof. We define a mapping $\phi : G \to V_1 \times V_2 \times \cdots \times V_n$ by

$$\phi(g) = (gK_1, gK_2, \cdots, gK_n).$$

ϕ is clearly a homomorphism since

$$\phi(gh) = (ghK_1, ghK_2, \cdots, ghK_n) = (gK_1, gK_2, \cdots, gK_n) \cdot (hK_1, hK_2, \cdots, hK_n) = \phi(g)\phi(h).$$

Kernel K of ϕ is given by:

$$
\begin{aligned}
K &= \{g \in G : (gK_1, gK_2, \cdots, gK_n) = (K_1, K_2, \cdots, K_n)\} \\
&= \{g \in G : g \in K_1 \cap K_2 \cap \cdots \cap K_n\} = (e)
\end{aligned}
$$

hence ϕ is an injective homomorphism and our proof is done. □

11. Let G be a finite abelian group such that it contains a subgroup $H_0 \neq (e)$ which lies in every subgroup $H \neq (e)$. Prove that G must be cyclic. What can you say about $o(G)$?

Proof. We introduce an useful lemma:

Lemma. Let p be a prime. A group G of order p^n is cyclic if and only if it is an abelian group having a unique subgroup of order p.
($\Rightarrow$) Suppose a p-group is cyclic, then it is trivially abelian and has a unique subgroup of order p. We now prove the converse. Suppose G is abelian and has an unique subgroup H of order p. Let $a \in G$ be the maximal order in G, that is, $a^{p^k} = e$ and consequently

$g^{p^k} = e$ for all $g \in G$. Now consider the subgroup (a). If (a) is proper in G, choose $x \notin (a)$. If $x^p \in (a)$, we take this. If $x^p \notin (a)$, let $x' = x^p$. If $x'^p = x^{p^2} \in (a)$, we take this x' as x. In fact, we are choosing $x \in G - (a)$ with $x^p \in (a)$ with minimal order. Hence, $x^p = a^q$ for some integer q. Note that $k = 1$ is clearly not the case, otherwise $x \in (a)$. So we assume $k > 1$. Consequently,

$$e = x^{p^k} = a^{qp^{k-1}}$$

and since a is of order p^k, $p \mid q$ so that $x^p = a^{mp}$ for some integer m. Hence, $x^{-p}a^{mp} = e \iff (x^{-1}a^m)^p = e \implies x^{-1}a^m \in H \subset (a)$, which is clearly a contradiction. Hence, $(a) = G$, and G is cyclic.

Now we head to our main problem. Note that every finite abelian group G is an internal direct product of its Sylow subgroups. By the conditions given, every Sylow subgroups must have non-trivial subgroup, which is clearly impossible. So the only case is that G itself is a p-group, and H_0 is a subgroup of order p. Now we apply the lemma. Hence we obtain that G is cyclic. □

12. Let G be a finite abelian group. Using Problem 11 show that G is isomorphic to a subgroup of a direct product of a finite number of finite cyclic groups.

Proof. Let G be the group of minimal counter-example. We know that G is an internal direct product of its Sylow sub-groups. That is, $G = P_1 P_2 \cdots P_n$, where P_i are p_i-Sylow subgroups. For each P_i, if P_i is cyclic, then we are done. If not, by the Problem 11, there are at least two normal subgroups A and B of P_i, each with order p_i. Let $P_i^{1,1} = P_i/A$, $P_i^{1,2} = P_i/B$. Since P_i is isomorphic to a subgroup of $P_i/A \times P_i/B$, if both $P_i^{1,1}$ and $P_i^{1,2}$ are cyclic, then we are done. If not, we can repeat the above procedure, at least within finite times, to obtain $P_i^{k,1}$ and $P_i^{k,2}$ which both are cyclic at the same time. Then P_i must be isomorphic to a subgroup of direct product of finite number of finite cyclic groups. Recall that G is internal direct product of Sylow subgroups, thereby isomorphic to a subgroup of finitely many number of finite cyclic groups. □

13. Give an example of a finite non-abelian group G which contains a subgroup $H_0 \neq (e)$ such that $H_0 \subset H$ for all subgroups $H \neq (e)$ of G.

Solution. Take the quaternion group G, $G = \{\pm 1, \pm i, \pm j, \pm k\}$. There are only four non-trivial proper subgroups, $\{1, -1\}$, $\{1, -1, i, -i\}$, $\{1, -1, j, -j\}$, $\{1, -1, k, -k\}$. Take $H_0 = \{1, -1\}$ to see that H_0 is contained in every 4 of above and nontrivial at the same time. □

14. Show that every group of order p^2, p a prime, is either cyclic or is isomorphic to the direct product of two cyclic groups each of order p.

Proof. If G has a generator, then it is clearly cyclic. So we now investigate the case where G has no generator. In other words, every non-trivial elements of G has order p. Choose $a \neq e \in G$. Then (a) is a normal subgroup in G. Further, choose $b \in G - (a)$. Then again $b^p = e$, so that (b) is also a normal subgroup of G and $(a) \cap (b) = (e)$. Consequently, $(a)(b) = G$. Applying the result of Problem 9, G is the internal product of two cyclic groups each of order p. □

15. Let $G = A \times A$ where A is cyclic of order p, p a prime. How many automorphisms does G have?

Solution. $\mathbb{Z}_p \times \mathbb{Z}_p \simeq GL(2, \mathbb{Z}_p)$ so that $o(\mathscr{A}(G)) = (p^2 - 1)(p^2 - p)$. □

16. If $G = K_1 \times K_2 \times \cdots \times K_n$ describe the center of G in terms of those of the K_1.

Solution. Let $Z(G)$ denote the center of a group G. Choose $k_i \in K_i$ and $z_i \in K_i$ where $(k_1, k_2, \cdots, k_n) \in G$ and $(z_1, z_2, \cdots, z_n) \in Z(G)$. It follows that

$$(k_1, k_2, \cdots, k_n) \cdot (z_1, z_2, \cdots, z_n) = (z_1, z_2, \cdots, z_n) \cdot (k_1, k_2, \cdots, k_n) \iff k_i z_i = z_i k_i$$

so that for each $i = 1, 2, \cdots, n$, $z_i \in Z(K_i)$. Thus we can describe the centre of G as:

$$Z(G) = Z(K_1) \times Z(K_2) \times \cdots \times Z(K_n).$$

□

17. If $G = K_1 \times K_2 \times \cdots \times K_n$ and $g \in G$, describe

$$N(g) = \{x \in G : xg = gx\}.$$

Solution. Let $N_G(g)$ denote the normalizer of an $g \in G$, where G is a group. Choose $k_i \in K_i$. Let $g = (g_1, g_2, \cdots, g_n)$. It follows that

$$(k_1, k_2, \cdots, k_n)(g_1, g_2, \cdots, g_n) = (g_1, g_2, \cdots, g_n) \cdot (k_1, k_2, \cdots, k_n) \iff k_i g_i = g_i k_i$$

so that for each $i = 1, 2, \cdots, n$, $k_i \in N_{K_i}(g_i)$. Thus,

$$N_G(g) = N_{K_1}(g_1) \times N_{K_2}(g_2) \times \cdots \times N_{K_2}(g_2).$$

□

18. If G is a finite group and $N_1, N_2, \cdots N_n$ are normal subgroups of G such that $G = N_1 N_2 \cdots N_n$ and $o(G) = o(N_1)o(N_2) \cdots o(N_n)$, prove that G is the direct product of $N_1, N_2, \cdots, N_n$.

Proof. Recall that any product of two normal subgroups is a normal subgroup. So,

$$\begin{aligned} o((N_1N_2\cdots N_{n-1})N_n) &= \frac{o(N_1\cdots N_{n-1})o(N_n)}{o(N_1\cdots N_{n-1}\cap N_n)} \\ &= \frac{o(N_1\cdots N_{n-2})o(N_{n-1})o(N_n)}{o(N_1\cdots N_{n-2}\cap N_{n-1})o(N_1\cdots N_{n-1}\cap N_n)} \\ &\ \ \vdots \\ &= \frac{\prod_{i=1}^{n} o(N_i)}{\prod_{k=1}^{n-1} o((\prod_{j=1}^{n-k} N_j)\cap N_{n+1-k})}. \end{aligned}$$

But this implies $N_1\cdots N_{n-1}\cap N_n = (e)$. By changing N_n with any N_i, we can draw same conclusions. Hence, by Problem 9, G is the direct product of N_i's. □