Topics in Algebra solution

Sung Jong Lee, lovekrand.github.io

November 6, 2020

Problems in the Section 2.8.

1. Let G be a group; consider the mappings of G into itself, λ_g, defined for $g \in G$ by $x\lambda_g = gx$ for all $x \in G$. Prove that λ_g is one-to-one and onto, and that $\lambda_{gh} = \lambda_h\lambda_g$.

Proof. Suppose $x\lambda_g = y\lambda_g$. Then $gx = gy \iff x = y$. Thus, λ_g is one-to-one. Also, $(g^{-1}x)\lambda_g = g(g^{-1}x) = x$ implying λ_g is onto. Moreover, $x\lambda_{gh} = gh(x) = g(hx) = g(x\lambda_h) = (x\lambda_h)\lambda_g = x\lambda_h\lambda_g$. Hence, $\lambda_{gh} = \lambda_h\lambda_g$. ☐

2. Let λ_g be defined as in Problem 1, τ_g as in the proof of Theorem 2.9.1. Prove that for any $g, h \in G$, the mappings λ_g, τ_h satisfy $\lambda_g\tau_h = \tau_h\lambda_g$.

Proof. Let $x \in G$. Observe that

$$x\lambda_g\tau_h = (gx)\tau_h = gxh = g(xh) = g(x\tau_h) = (x\tau_h)\lambda_g = x\tau_h\lambda_g.$$

Hence proved. ☐

3. If θ is a one-to-one mapping of G onto itself such that $\lambda_g\theta = \theta\lambda_g$ for all $g \in G$, prove that $\theta = \tau_h$ for some $h \in G$.

Proof. Note that $x\lambda_g\theta = x\theta\lambda_g \iff \theta(gx) = g\theta(x)$ for all $x \in G$. Since this holds for every $g \in G$, $\theta(x^{-1} \cdot x) = x^{-1}\theta(x) \iff \theta(x) = x\theta(e)$. Let $h = \theta(e)$. Consequently, $\theta = \tau_h$. ☐

4. a) If H is a subgroup of G show that for every $g \in G$, gHg^{-1} is a subgroup of G.

Proof. Refer to the Problem 4 of section 2.5. ☐

b) Prove that $W =$ intersection of all gHg^{-1} is a normal subgroup of G.

Proof. Refer to the Problem 18 of section 2.5. ☐

5. Using Lemma 2.9.1 prove that a group of order p^2, where p is a prime number, must have a normal subgroup of order p.

Proof. Suppose G is a group of order p^2. If G is cyclic and $G = (a)$, we have (a^p) the normal subgroup of G of order p. So, we now assume that G is not cyclic. Choose $a \in G$. Then the order of a is either 1 or p. If $a \neq e$, then the order of a is p. Thus, (a) is now the subgroup of order p. We show that (a) is normal in G. Note that $p^2 \nmid p!$. This implies that there exists a non-trivial normal subgroup contained in (a). Since $o(a) = p$, (a) is the non-trivial normal subgroup. Hence, we have shown that every group of order p^2 must have a normal subgroup of order p. □

6. Show that in a group G of order p^2 any normal group of order p must lie in the center of G.

Proof. Let H be the normal group of order p. Since H is cyclic, $H = (h)$. Using the normality of H, for all $g \in G$,

$$ghg^{-1} = h^k$$

for some $0 < k < p$. Note that $gh^n h^{-1} = h^{nk}$ and $g^n h g^{-n} = h^{k^n}$ for any natural n. Since $g^{p^2} = e$, $g^{p^2} h g^{-p^2} = h = h^{k^{p^2}}$ implying $k^{p^2} \equiv 1 \pmod{p}$. Now by Fermat's little theorem, $1 \equiv k^{p^2} \equiv k^p \equiv k \pmod{p}$ implying $k = 1$. Therefore, $ghg^{-1} = h$ for all $g \in G$. Thus, H lies in $Z(G)$. □

7. Using the result of Problem 6, prove that any group of order p^2 is abelian.

Proof. Let G be the group of order p^2. If G is cyclic then it is trivial. Otherwise, by Problem 5, we have a subgroup (a) of G of order p. Now consider $b \in G - (a)$. Then b must have order p. Now we have a subgroup (b) with order p. Applying the same procedure in Problem 5, since $p^2 \nmid p!$, (b) must be normal in G. Note that by Problem 6, $(a) \subset Z(G)$ and $b \notin (a)$ and $b \in Z(G)$, $o(Z(G)) > p$. Now by Lagranges theorem, $o(Z(G)) = p^2$ and hence $Z(G) = G$. Thus, G is abelian. □

8. If p is a prime number, prove that any group of G of order $2p$ must have a subgroup of order p, and that this subgroup is normal in G.

Proof. If G is cyclic, say, $G = (a)$ for some $a \in G$, then the subgroup (a^2) generated by a^2 is of order p. Normality is clear since G is cyclic. Suppose, G is not cyclic. If there is an element a of order p, then (a) is a subgroup of order p and since $[G : (a)] = 2$, (a) is normal in G. Now suppose we assume that there is no element of order p. Consequently, every elements in G is of self-inverses. Now we have G is abelian. But applying the Cauchy's theorem for abelian case, G must have an element of order p since $p \mid 2p$. This contradicts our hypothesis. Therefore, we can conclude that for any group G of order $2p$, it must have a subgroup of order p and this subgroup is normal in G. □

9. If $o(G)$ is pq where p and q are distinct prime numbers and if G has a normal subgroup of order p and normal subgroup of order q, prove that G is cyclic.

Proof. Let (a) and (b) be the normal subgroups of order p and q respectively. Since $\gcd(p,q)=1$, $(a)\cap(b)=(e)$. Moreover, since these are abelian normal subgroups, product group $(a)(b)$ is abelian. Note that

$$o((a)(b)) = \frac{o(a)\cdot o(b)}{o((a)\cap(b))} = \frac{pq}{1} = pq$$

so that $(a)(b)=G$. Now we have G is abelian. Since a,b are elements of order p,q respectively, applying the Problem 25 of section 2.5, there exists an elements of order $\mathrm{lcm}(p,q)=pq$. This shows that G is cyclic. □

10. Let $o(G)$ be pq, $p>q$ are primes, prove
a) G has a subgroup of order p and a subgroup of order q.

Proof. Suppose G is cyclic. Then we have $G=(a)$ for some $a\in G$. Consequently, (a^q) and (a^p) are the required subgroups of order p and q respectively. Now, we assume that G is not cyclic. If there is an element a of order p, this must be unique subgroup of order p (refer to the comments in pg 46 in the Herstein's book). Now choose $b\in G-(a)$. Then the only choice for the order of b is q. Hence, we established the subgroups of order p and q respectively. Now assume that there are only elements of order q. Then the number of non-identity elements is multiple of q and equal to $pq-1$. But this is weird. Hence, G must have an element of order p. □

b) If $q\nmid p-1$, then G is cyclic.

Proof. We introduce some useful lemmas:

Lemma. If G is a group and $G/Z(G)$ is cyclic, then G is abelian.
⇒ Suppose $G/Z(G)$ is cyclic, then we can write $G/Z(G)=(aZ)$ for some $a\in G$. Note that for any $x\in G$ lies in one of the coset a^kZ. Thus, we can represent x as $x=a^{k_1}z_1$, $y=a^{k_2}z_2$ for some $k_1,k_2\in\mathbb{Z}$ and $z_1,z_2\in Z(G)$. Consequently,

$$xy=(a^{k_1}z_1)(a^{k_2}z_2)=a^{k_1}(z_1a^{k_2})z_2=a^{k_1}a^{k_2}z_1z_2=a^{k_1+k+2}z_1z_2,$$

while

$$yx=(a^{k_2}z_2)(a^{k_1}z_1)=a^{k_2}(z_2a^{k_1})z_1=a^{k_2}a^{k_1}z_2z_1=a^{k_1+k_2}z_1z_2,$$

so that $xy=yx$. Hence, G is abelian.

Lemma. If G is a group and H is a normal subgroup of G. Let G acts on H by conjugation as automorphisms of H, then $G/C(H)\hookrightarrow \mathscr{A}(H)$. That is, $G/C(H)$ is isomorphic to a subgroup of $\mathscr{A}(G)$. Here $C(H)$ denotes the centralizer of subgroup H.
⇒ Let us define a mapping $\phi: G\to\mathscr{A}(G)$ by $\phi(g)=T_g$ where $T_g: H\to H$ is an

automorphism defined as $T_g(h) = ghg^{-1}$ where $h \in H$. Clearly, ϕ is a homomorphism, with the kernel $Ker(\phi) = \{g \in G : T_g = I \iff gh = hg, \forall h \in H\} = C(H)$. Now apply Isomorphism theorem to obtain $G/C(H) \hookrightarrow \mathscr{A}(H)$.

If G was abelian, then by a), we have elements of order p and q respectively. Applying Problem 24 of section 2.3 2.5, we can conclude that there is an element of order $\text{lcm}(p, q) = pq$ so that G is cyclic. Now we assume that $Z(G)$ is non-trivial but does not equal to G itself. Since the order of $G/Z(G)$ is either p or q, so that $G/Z(G)$ is cyclic and hence G is abelian. Thus, we are now left with the case of G having trivial center. That is, $Z(G) = (e)$. Note that the subgroup H of G with order p must be normal in G. Applying the lemma above, we have $G/C(H) \hookrightarrow \mathscr{A}(H)$. Moreover, from the fact that $Z(G) = (e)$, and $H \subset C(H)$, $C(H)$ is of order either p or pq. But if $C(H)$ has order of pq, then this contradicts the fact that $Z(G) = (e)$. Hence, $C(H) = H$. Therefore, $G/H \hookrightarrow \mathscr{A}(H)$. Note that $o(G/H) = q$ and $o(\mathscr{A}(H)) = \phi(p) = p - 1$. It follows that $q \mid p - 1$, contrary to our hypothesis that $q \nmid p - 1$. Hence, $Z(G) = (e)$ is not the case again. We conclude that G is abelian, and applying the assertion of Problem 9, G is cyclic. □

c) Given two primes $p, q, q \mid p - 1$, there exists a non-abelian group of order pq.

Proof. We shall continue using the notations introduced above. We build a non-abelian group of order pq with the method of construction used in Pg.69. From the assertions of b), if $q \mid p - 1$, $\mathscr{A}(H)$ admits a subgroup of order q, that is, there exists an automorphism $\phi \in \mathscr{A}(H)$ such that $\phi(h) = h^i$ for $i^q \equiv 1 \pmod{p}$. Let h and k be the generators of H and K(group of order q). Now let the action of k on P by conjugation be $x \mapsto x^j$ with $j \neq 1 \pmod{p}$. Thus,

$$G =< h, k : h^p = e, k^q = e, khk^{-1} = h^j >$$

In this way, G is non-abelian group. In an explicit way, G is isomorphic to

$$G \simeq \left\{ \begin{pmatrix} h & k \\ 0 & 1 \end{pmatrix} : h \in U_p, k \in Z_p, h^q = 1 \pmod{p} \right\}.$$

□

d) Any two non-abelian groups of order pq are isomorphic.

Proof. Note that choosing different j in above is exactly the same of choosing different generator for the group K. Thus, this gives that the obtained group is an isomorphism(isomorphic) to G. □