MATH 6/71051
Homework #9
Selected Solutions

§5.2 #5: *If G is a finite abelian group of type $(n_1, n_2, \dots, n_t)$, then G contains an element of order m if and only if $m \mid n_1$. Moreover, the exponent of G is n_1.*

Proof. Let $G = Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_t}$, with Z_{n_i} a multiplicative cyclic group of order n_i for each i. If $g = (a_1, a_2, \dots, a_t) \in G$, then $|a_i|$ divides n_i. Since $n_i \mid n_{i-1}$, we have $n_i \mid n_1$, and so $|a_i|$ divides n_1 for each i. Hence

$$g^{n_1} = (a_1, a_2, \dots, a_t)^{n_1} = (a_1^{n_1}, a_2^{n_1} \dots, a_t^{n_1}) = (1, 1, \dots, 1) = 1_G.$$

Thus if $g \in G$ with $|g| = m$, then $g^{n_1} = 1$ and so $|g| = m \mid n_1$.

Conversely, if m is a positive divisor of n_1, then there is an element $a \in Z_{n_1}$ of order m since Z_{n_1} is cyclic. The order of $g = (a, 1, 1, \dots, 1) \in G$ is the least common multiple of the orders of the components of g, hence is m. Therefore, G contains an element of order m.

Finally, we have seen that if $g \in G$, then $g^{n_1} = 1_G$, so the exponent of G is at most n_1. Also, G contains an element of order n_1 by the previous paragraph, hence the exponent of G is equal to n_1. □

§5.4 #4: *The commutator subgroup of S_4 is A_4 and the commutator subgroup of A_4 is $V = \{1, (12)(34), (13)(24), (14)(23)\}$.*

Proof. Since A_4 is of index 2 in S_4, we have $A_4 \trianglelefteq S_4$ and $|S_4/A_4| = 2$. Hence S_4/A_4 is abelian and $S_4' \leqslant A_4$. Also, $(123) = (12)^{-1}(132)^{-1}(12)(132) \in S_4'$, and since $S_4' \trianglelefteq S_4$ and all 3-cycles are conjugate to (123) in S_4, we have that all eight 3-cycles are in S_4'. Hence $|S_4'|$ divides $|A_4| = 12$ and $|S_4| > 8$, and so $|S_4'| = 12$ and $S_4' = A_4$.

The subgroup $V = \{1, (12)(34), (13)(24), (14)(23)\}$ of A_4 contains 1 and all elements of S_4 with cycle type 2^2. Hence V is a union of conjugacy classes of S_4 and is therefore a normal subgroup of S_4, hence also of A_4. Since $|A_4/V| = 3$, we have that A_4/V is abelian and so $A_4' \leqslant V$.

Since A_4 is not abelian, we know that $A_4' \neq \langle 1 \rangle$. The only other proper subgroups of V are of order 2. Hence if $A_4' \neq V$, then A_4' is a normal subgroup of A_4 of order 2, and so A_4' is contained in the center of A_4. But it is easily checked that no nonidentity element of V is in the center of A_4, hence $A_4' = V$. □

§5.4 #9: *If p is an odd prime and P is a group of order p^3, then the p^{th} power map $x \mapsto x^p$ is a homomorphism of P into $Z(P)$. If P is not cyclic, then the kernel of the p^{th} power map has order p^2 or p^3.*

Proof. Let P be a group of order p^3 and denote the p^{th} power map by ρ. If P is abelian and $a, b \in P$, then a and b commute, hence $(ab)^p = a^p b^p$, and so ρ is a homomorphism. If P is a nonabelian group of order p^3, then by Problem #II on this homework, $P' = Z(P)$, and so §5.4 #8 applies to every pair of elements of P. Hence for $a, b \in P$, we have

$$(ab)^p = a^p b^p [b, a]^{\frac{p(p-1)}{2}} = a^p b^p \left([b, a]^p\right)^{(p-1)/2},$$

and since p is odd, $(p-1)/2$ is an integer. Again by Problem #II, $|P'| = p$, hence $[b, a]^p = 1$ and this implies $(ab)^p = a^p b^p$. Hence ρ is a homomorphism in any case.

[Continued next page →]

[§5.4 #9, continued:]

If P is not cyclic, then every element of P is of order 1, p, or p^2. Hence $a^{p^2} = 1$ for each $a \in P$. If $x \in \operatorname{Im}\rho$, then $x = \rho(a) = a^p$ for some $a \in P$. Therefore,

$$\rho(x) = x^p = (a^p)^p = a^{p^2} = 1,$$

and so $x \in \ker\rho$. Thus we have $\operatorname{Im}\rho \leqslant \ker\rho$. By the First Isomorphism Theorem,

$$|P|/|\ker\rho| = |\operatorname{Im}\rho|,$$

and so

$$p^3 = |P| = |\ker\rho| \cdot |\operatorname{Im}\rho| \geqslant |\operatorname{Im}\rho| \cdot |\operatorname{Im}\rho| = |\operatorname{Im}\rho|^2.$$

It follows that $|\operatorname{Im}\rho| = 1$ or $|\operatorname{Im}\rho| = p$, and so $|\ker\rho| = p^3/|\operatorname{Im}\rho|$ is either p^3 or p^2.

If P is abelian or if $|\operatorname{Im}\rho| = 1$, then clearly $\operatorname{Im}\rho \leqslant Z(G)$, so assume now that P is nonabelian and $|\operatorname{Im}\rho| = p$. If $g \in P$ and $x = \rho(a) = a^p \in \operatorname{Im}\rho$, then

$$gxg^{-1} = ga^pg^{-1} = (gag^{-1})^p = \rho(gag^{-1}) \in \operatorname{Im}\rho,$$

hence $\operatorname{Im}\rho \trianglelefteq P$. The group $P/\operatorname{Im}\rho$ is of order p^2, hence is abelian, and so $Z(P) = P' \leqslant \operatorname{Im}\rho$. As $|\operatorname{Im}\rho| = p = |Z(P)|$, we have $\operatorname{Im}\rho = Z(P)$, and so in any case ρ maps P into $Z(P)$. □

§5.4 #19(b): *If H and K are perfect subgroups of G, then $\langle H, K\rangle$ is a perfect group.*

Proof. In any case, $\langle H, K\rangle' \leqslant \langle H, K\rangle$, so it suffices to show that $\langle H, K\rangle \leqslant \langle H, K\rangle'$. Since $H' = H$ and $K' = K$, we will show $\langle H', K'\rangle \leqslant \langle H, K\rangle'$.

Now $\langle H', K'\rangle = \langle H' \cup K'\rangle$ and every element of $H' \cup K'$ is a product of commutators of elements of H or elements of K. Hence $\langle H', K'\rangle = \langle \mathcal{C}\rangle$, where

$$\mathcal{C} = \{[h_1, h_2] \mid h_1, h_2 \in H\} \cup \{[k_1, k_2] \mid k_1, k_2 \in K\}.$$

If $h_1, h_2 \in H$, then since $H \leqslant \langle H, K\rangle$, we have $[h_1, h_2] \in \langle H, K\rangle'$. Similarly, $[k_1, k_2] \in \langle H, K\rangle'$ for all $k_1, k_2 \in K$. Hence $\langle H, K\rangle'$ contains $\mathcal{C}$ and since $\langle H, K\rangle'$ is a group, we have

$$\langle H', K'\rangle = \langle \mathcal{C}\rangle \leqslant \langle H, K\rangle',$$

as claimed. □

§5.4 #19(c): *If H is a perfect subgroup of G, then any conjugate of H is a perfect group.*

Proof. First note that, in general, if $A \subseteq G$, then for $a, b \in A$ and $g \in G$, we have that $g(ab)g^{-1} = (gag^{-1})(gbg^{-1})$ and $ga^{-1}g^{-1} = (gag^{-1})^{-1}$. It follows that $g\langle A\rangle g^{-1} = \langle gAg^{-1}\rangle$.

Let $H \leqslant G$ with $H = H'$, and let $g \in G$. Then

$$\begin{aligned}
(gHg^{-1})' &= \left\langle [gh_1g^{-1}, gh_2g^{-1}] \mid h_1, h_2 \in H \right\rangle \\
&= \left\langle g[h_1, h_2]g^{-1} \mid h_1, h_2 \in H \right\rangle \\
&= g\,\langle [h_1, h_2] \mid h_1, h_2 \in H\rangle\, g^{-1}, \text{ by the remark above,} \\
&= gH'g^{-1} \\
&= gHg^{-1}.
\end{aligned}$$

Hence $(gHg^{-1})' = gHg^{-1}$ and gHg^{-1} is a perfect group. □

§5.5 #2: *If $G = H \rtimes_\varphi K$, then $C_H(K) = N_H(K)$.*

Proof 1. Identify H and K with the subgroups H^* and K^* of G. Thus we have $H \trianglelefteq G$ and $H \cap K = \langle 1 \rangle$. In any case, $C_H(K) \leqslant N_H(K)$, so it suffices to show $N_H(K) \leqslant C_H(K)$.

Let $h \in N_H(K)$. If $k \in K$, then $h^{-1}kh \in K$, hence $[k, h] = k^{-1}h^{-1}kh \in K$. Since $H \trianglelefteq G$, we have $k^{-1}h^{-1}k \in H$, and hence $[k, h] = k^{-1}h^{-1}kh \in H$. Therefore, $[h, k] \in H \cap K = \langle 1 \rangle$, so $[h, k] = 1$ and h commutes with k. Since k was an arbitrary element of K, $h \in C_H(K)$ and so $N_H(K) \leqslant C_H(K)$. □

Proof 2. In this case we do not identify H, K with H^*, K^* and we prove explicitly that $C_{H^*}(K^*) = N_{H^*}(K^*)$. For $k \in K$, denote $\varphi(k) = \sigma_k$. If $(h, 1_K) \in H^*$ and $(1_H, k) \in K^*$, then

$$(h, 1_K)(1_H, k) = (h\sigma_{1_K}(1_H), 1_K k) = (h1_H, 1_K k) = (h, k)$$

and

$$(1_H, k)(h, 1_K) = (1_H \sigma_k(h), k1_K) = (\sigma_k(h), k).$$

Hence $(h, 1_K)$ and $(1_H, k)$ commute if and only if $\sigma_k(h) = h$.

We also have

$$\begin{aligned}
(h, 1_K)^{-1}(1_H, k)(h, 1_K) &= (\sigma_{1_K^{-1}}(h^{-1}), 1_K^{-1})(1_H \sigma_k(h), k1_K) \\
&= (h^{-1}, 1_K)(\sigma_k(h), k) \\
&= (h^{-1}\sigma_{1_K}(\sigma_k(h)), 1_K k) \\
&= (h^{-1}\sigma_k(h), k).
\end{aligned}$$

Thus $(h, 1_K)^{-1}(1_H, k)(h, 1_K) \in K^*$ if and only if $h^{-1}\sigma_k(h) = 1_H$, so if and only if $\sigma_k(h) = h$.

Hence $(h, 1_K)$ and $(1_H, k)$ commute if and only if $(h, 1_K)^{-1}(1_H, k)(h, 1_K) \in K^*$. It follows that $(h, 1_K) \in C_{H^*}(K^*)$ if and only if $(h, 1_K) \in N_{H^*}(K^*)$, and so $C_{H^*}(K^*) = N_{H^*}(K^*)$. □

§5.4 #3: *Let $G = H \rtimes_\varphi K$, where H is an abelian group, $K = \{1_K, x\}$ is a cyclic group of order 2, and $\varphi : K \to \mathrm{Aut}(H)$ is defined by $\varphi(x) = \sigma_x$, where $\sigma_x(h) = h^{-1}$ for $h \in H$.*

a. *Every element of $G - H$ is of order 2.*

b. *The group G is abelian if and only if $h^2 = 1_H$ for all $h \in H$.*

Proof. **(a)** Since $K = \{1_K, x\}$, each element of $G - H$ is of the form $g = (h, x)$. We have

$$g^2 = (h, x)(h, x) = (h\sigma_x(h), xx) = (hh^{-1}, x^2) = (1_H, 1_K) = 1_G.$$

Thus $g^2 = 1_G$, but $x \neq 1_K$ so $g \neq 1_G$, hence the order of g is 2.

(b) Since H and K are abelian, the subgroups

$$H^* = \{(h, 1_K) \mid h \in H\} \cong H,$$

$$K^* = \{(1_H, 1_K), (1_H, x)\} \cong K$$

are abelian. Moreover $G = H^*K^*$, so G is abelian if and only if every element of H^* commutes with every element of K^*. Certainly, every element of H^* commutes with $(1_H, 1_K) = 1_G$, hence G is abelian if and only if $(h, 1_K)$ commutes with $(1_H, x)$ for all $h \in H$.

As shown in Proof 2 of §5.4 #2 above, $(h, 1_K)$ commutes with $(1_H, x)$ if and only if $\sigma_x(h) = h$. In this case, $\sigma_x(h) = h^{-1}$, so G is abelian if and only if $h = h^{-1}$, i.e., $h^2 = 1_H$, for all $h \in H$. □

Remark: The group H must be abelian for this construction to work. If H is not abelian, then $\varphi(x) = \sigma_x$ is not an automorphism of H.