1 Exam 2 Review Questions

1. Recall from HW4, that if G is a finite group, H is a subgroup of G, then $\varphi\colon G \times G/H \to G/H$ by $\varphi(a, Hg) = Hga^{-1}$ is an action. Also recall that for each $g \in G$, $\sigma_g\colon S \to S$ by $\sigma_g(t) = \varphi(g, t)$ is a permutation of S, and $\theta\colon G \to A(S)$ by $\theta(g) = \sigma_g$ is a homomorphism. On HW4 we proved that $\ker\theta = \cap\{xHx^{-1}\colon x \in G\}$, and $\ker\theta \subseteq_g H$.

   (a) Assume $o(G) = 12$, and that P is a 3-Sylow subgroup of G. Using the above, prove that either $G \cong A_4$ or $\ker\theta = P$.

   Proof. Let $\varphi\colon G \times G/P \to G/P$ be the action described above, and let $\theta\colon G \to A(G/P)$ be the permutation representation associated with the action. Then we have that $\ker\theta \subseteq_g P$. Thus, by Lagrange's theorem, $o(\ker\theta) \mid 3$ which implies that $o(\ker\theta) = 1$ or $o(\ker\theta) = 3$.

   If $o(\ker\theta) = 1$, then $\ker\theta = \{e\}$. Note that in this case $G/\ker\theta \cong G$. Thus, by the FHT

   $$G \cong G/\ker\theta \cong \theta(G) \subseteq_g A(G/P) \cong S_4.$$

   Thus, G is isomorphic to a subgroup of S_4. Since $o(G) = 12$ and the only subgroup of S_4 is A_4, then $G \cong A_4$.

   If $o(\ker\theta) = 3$, then since $\ker\theta \subseteq P$ and $|\ker\theta| = |P|$, then it follows that $\ker\theta = P$. □

   (b) Assume that $G \ncong A_4$. Let $P = \langle t\rangle$, and prove that $[G\colon N(t)] = 1$ or 2.

   Proof. Let $\psi\colon G \times G \to G$ be the action given by $\psi(g, h) = ghg^{-1}$. Then the orbit of t, $G(t) = \{gtg^{-1}\colon g \in G\}$, is equal to the conjugacy class of t, $c(t)$. Also the stabilizer of t, $G_t = \{g \in G\colon gtg^{-1} = t\}$, is equal to the normalizer of t, $N(t)$. Since $o(t) = 3$, then any conjugate of t must also have order 3. In part (a) we showed that $P = \ker\theta$ and so $P \lhd G$. Thus, there is only one 3-Sylow subgroup of G. This implies that there are only two elements of G with order 3. Hence, $\big|c(t)\big| = 1$ or $\big|c(t)\big| = 2$. By the orbit-stabilizer theorem, we have that

   $$\big|c(t)\big| = \frac{|G|}{\big|N(t)\big|} = [G\colon N(t)].$$

   Therefore, $[G\colon N(t)] = 1$ or 2. □

   (c) Explain why it follows from (b) that there exists $g \in N(t)$ such that $o(g) = 2$.

   Proof. If $[G\colon N(t)] = 1$, then $\big|N(t)\big| = 12$ and since $2 \mid 12$, then by Cauchy's Theorem, there exists $g \in N(t)$ such that $o(g) = 2$. If $[G\colon N(t)] = 2$, then $\big|N(t)\big| = 6$. Since $2 \mid 6$, then by Cauchy's Theorem, there exists $g \in N(t)$ such that $o(g) = 2$. □

(d) Explain why $o(tg) = 6$.

Proof. Since for all $x \in N(t)$ we have that $xtx^{-1} = t$ which gives $xt = tx$, then for the $g \in N(t)$ from part (c), we have that $gt = tg$. Thus, from Exam 1, $o(tg) = o(t)o(g) = 3 \cdot 2 = 6$. □

2. Assume that $o(G) = p^2q$, where p and q are distinct odd primes. Prove that G contains a Sylow subgroup that is normal in G, and prove that G is solvable.

Proof. By Sylow I, G contains a Sylow subgroup, P, of order p^2 and a Sylow subgroup, Q, of order q. Assume that $p > q$. By Sylow III, $n_p \equiv 1(\text{mod } p)$ and $n_p \mid q$. The first relation implies that $n_p = 1$ or $n_p > p$. The second relation implies that $n_p \leq q$. If $n_p \neq 1$, then $n_p > p$ and $n_p \leq q$, but since $p > q$, then this cannot occur. Thus, if $p > q$, then $n_p = 1$ and hence $P \triangleleft G$.

Assume that $p < q$. By Sylow III, $n_q \equiv 1(\text{mod } q)$ and $n_q \mid p^2$. The first relation implies that $n_q = 1$ or $n_q > q$. The second relation implies that $n_q = 1$, $n_q = p$, or $n_q = p^2$. If $n_q = p$, then $n_q \neq 1$ and thus $n_q > q$ which implies $p > q$ and this contradicts our assumption. Thus, $n_q = 1$ or $n_q = p^2$. If $n_q = p^2$, then $p^2 \equiv 1(\text{mod } q)$. Thus, $q \mid (p^2 - 1)$. Thus, $q \mid (p-1)(p+1)$. Since q is prime, then $q \mid (p-1)$ or $q \mid (p+1)$. Since $p < q$, then $q \nmid p$ and so $q \nmid (p-1)$. Thus, $q \mid (p+1)$. Moreover, since $q \nmid p$ and $q \mid (p+1)$, then $q = p+1$. However, since p is an odd prime, then $p+1$ is even and thus $q = p+1$ is even. This contradicts our assumption that q is an odd prime. Thus, $n_q \neq p^2$. Therefore, $n_q = 1$ which implies $Q \triangleleft G$.

If $P \triangleleft G$, then G/P is a group in which $o(G/P) = q$. Thus, G/P is abelian. Hence, $\{e\} \triangleleft P \triangleleft G$ is a normal series of G in which each factor is abelian. Thus, G is solvable. If $Q \triangleleft G$, then G/Q is a group in which $o(G/Q) = p^2$ and by (4) of HW6, G/Q is abelian. Thus, $\{e\} \triangleleft Q \triangleleft G$ is a normal series of G in which each factor is abelian. Thus, G is solvable. □

3. Assume that P is p-Sylow subgroup of G. Prove that if $N \triangleleft G$, $N \neq G$, and $NP \neq N$, then NP/N is a p-Sylow subgroup of G/N.

Proof. Let $o(P) = p^k$. Since $N \cap P \subseteq_g P$, then $o(N \cap P) \mid p^k$. Let $o(N \cap P) = p^i$. Since $P \subseteq_g G$ and $N \triangleleft G$, then $NP \subseteq_g G$. Thus, $N \triangleleft NP$ and NP/N is a group. It follows that

$$o(NP/N) = \frac{o(NP)}{o(N)} = \frac{\frac{o(N)o(P)}{o(N\cap P)}}{o(N)} = \frac{o(P)}{o(N \cap P)} = \frac{p^k}{p^i} = p^{k-i}.$$

Note that if $i = k$, then $o(N \cap P) = p^k$ which would imply that $N = P$ and thus $NP = N$ which contradicts our assumption. Thus, $i < k$ and $k - i > 0$. If $i = 0$, then $o(NP/N) = p^k$ and thus NP/N is a p-Sylow subgroup of G/N. Assume that $i > 0$ and that $Q/N \subseteq_g G/N$ such that $o(Q/N) = p^j$ where $j > k - i$. Then $o(Q) = p^j o(N)$. However, since $N \cap P \subseteq_g N$, then $p^i \mid o(N)$. Thus, $p^{i+j} \mid o(Q)$. However, $i + j > k$ and so no such Q can exist. Thus, NP/P is a p-Sylow subgroup of G/N. □

4. Assume that $o(G) = 108$. Prove that G has a normal subgroup of order 9, or of order 27.

Proof. To begin, first note that $108 = 2^2 \cdot 3^3$. By Sylow I, G contains a 3-Sylow subgroup of order 27. By Sylow III, $n_3 \equiv 1(\text{mod } 3)$ and $n_3 \mid 4$. Thus, $n_3 = 1$ or $n_3 = 4$. Assume that $n_3 = 1$. Then the 3-Sylow subgroup is normal in G which implies that G contains a normal subgroup of order 27.

Assume that $n_3 = 4$. Then let P and Q be two distinct 3-Sylow subgroups of G. Since $PQ \subseteq G$, then it follows that

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} \leq |G| \Leftrightarrow \frac{729}{108} \leq |P \cap Q| \, .$$

With this relation and the fact that $|P \cap Q| \mid P$, then $|P \cap Q| = 9$ or $|P \cap Q| = 27$. If $|P \cap Q| = 27$, then $P = Q$ and this would contradict our assumption that P and Q distinct 3-Sylow subgroups of G. Thus, $|P \cap Q| = 9$. Since $o(P/(P \cap Q)) = 3$ and 3 is the smallest prime factor of $o(P)$, then $P \cap Q \triangleleft P$. Similarly, $P \cap Q \triangleleft Q$. It follows then that $P \subseteq N(P \cap Q)$ and $Q \subseteq N(P \cap Q)$. Thus, $PQ \subseteq N(P \cap Q)$. However, since $|PQ| = 81$ and $o(N(P \cap Q)) \mid o(G)$, then $o(N(P \cap Q)) = o(G)$, which implies that $N(P \cap Q) = G$. Finally, since $P \cap Q \triangleleft N(P \cap Q)$, then $P \cap Q \triangleleft G$. Therefore, G contains a normal subgroup of order 9. □

5. Determine the structure of all groups of order 57.

Proof. We begin by first noting that $57 = 3 \cdot 19$. Thus, Sylow I guarantees us that $o(G) = 57$, then G contains a 3-Sylow subgroup of order 3 and a 19-Sylow subgroup of order 19. From Sylow III it follows that $n_3 \equiv 1(\text{mod } 3)$ and $n_3 \mid 19$. Thus, $n_3 = 1$ or $n_3 = 19$. Similarly, $n_{19} \equiv 1\text{mod } 19)$ and $n_{19} \mid 3$. Thus, $n_{19} = 1$. Hence, the 19-Sylow subgroup is normal in G. Let $\langle a \rangle$ denote a 3-Sylow subgroup of G and let $\langle b \rangle$ denote the 19-Sylow subgroup of G. Assume that $\theta \colon \langle a \rangle \to \text{Aut}(\langle b \rangle)$ be a homomorphism defined by $\theta(g) = \sigma_k$ and $\sigma_k(x) = x^k$. Each map σ_k corresponds to a relation $aba^{-1} = b^k$. So we must determine for which values of k this relation holds. Note that by the properties of homomorphisms, $o(\theta(a)) \mid o(a)$. Hence, $o(\varphi_k) \mid 3$. Thus, $o(\varphi_k) = 1$ or $o(\varphi_k) = 3$. If $o(\varphi_k) = 1$, then φ_k is the identity map and $k = 1$. This then corresponds to $aba^{-1} = b$. If $o(\varphi_k) = 3$, then $(\varphi_k)^3 = \varphi_{k^3} = \varphi_1$. This implies that for all $x \in \langle b \rangle$, $\varphi_{k^3}(x) = x^{k^3} = x$. Thus, $x^{k^3 - 1} = e$ for all $x \in \langle b \rangle$. Hence, $o(x) \mid (k^3 - 1)$. And so $19 \mid (k^3 - 1)$. Then we are looking for solutions to $k^3 \equiv 1(\text{mod } 19)$, of which there are 3. Checking all $1 \leq k \leq 19$, we find that $1, 7$, and 11 are solutions to this. However, taking $k = 7$, we find that $7^2 \equiv 11(\text{mod } 19)$ and $7^3 \equiv 1(\text{mod } 19)$. This implies that φ_7 and φ_{11} both yield the same structure.

Finally, if $k = 1$, then $aba^{-1} = b$, thus $ab = ba$, thus G is Abelian. Hence, $\langle a \rangle \triangleleft G$, $\langle a \rangle \cap \langle b \rangle = \{e\}$, and $G = \langle a \rangle$. Thus, $G \cong \mathbb{Z}_3 \times \mathbb{Z}_{19} \cong \mathbb{Z}_{57}$.

If $k = 7$, then G is a non-abelian group of order 57 defined by $o(a) = 3$; $o(b) = 19$; $aba^{-1} = b^7$. □

6. Assume that G is a group, p is a prime, $N \triangleleft G$, $o(N) = m$, $p \nmid m$, and $o(Ng) = p$. Prove that $o(g^m) = p$.

   Proof. Since $o(Ng) = p$, then $(Ng)^p = Ng^p = N$. Thus, $g^p \in N$. Since $o(N) = m$, then $(g^p)^m = (g^m)^p = e$. Now assume that for some $k \in \mathbb{Z}^+$, $(g^m)^k = e$. Then $g^{mk} = e$. It then follows that $(Ng)^{mk} = Ng^{mk} = N$. Since $o(N) = p$, then $p \mid mk$. However, since p is prime and $p \nmid m$, then $(p, m) = 1$ and thus $p \mid k$. Thus, $p \leq k$. Therefore, $(g^m)^p = e$ and for all $k \in \mathbb{Z}^+$, if $(g^m)^k = e$, then $p \leq k$. Hence, $o(g^m) = p$. □

7. Assume that G is a finite Abelian group, and that G is not cyclic. Prove that there exists a prime p such that G has a subgroup isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$.

   Proof. By the fundamental theorem of finite abelian groups, G is isomorphic to a product of cyclic groups. In particular, if $o(G) = p_1^{r_1} \cdots p_n^{r_n}$ is the prime decomposition of the order of G, then $G \cong \mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_n^{r_n}}$. Now consider $\mathbb{Z}_{p_i^{r_i}} \times \mathbb{Z}_{p_j^{r_j}}$, this is clearly in the above product and $\mathbb{Z}_p \times \mathbb{Z}_p$ is a subgroup of this product. Thus, G has a subgroup isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$. □

8. Assume that $G \cong A \times B$ and θ is an isomorphism from G onto $A \times B$. Let $N = \{g \in G \colon \theta(g) \in A \times \{e\}\}$. Prove that N is a normal subgroup of G and that $N \cong A$. Let $M = \{g \in G \colon \theta(g) \in \{e\} \times B\}$. Explain how to express G as an internal direct product.

   Proof. It is easily shown that both N and M are subgroups of G. Let $n \in N$ and $g \in G$. We want to show that $gng^{-1} \in N$. Thus, we need to show that $\theta(gng^{-1}) \in A \times \{e\}$. Let $\theta(n) = (a, e)$ and let $\theta(g) = (x, y)$.

   $$\theta(gng^{-1}) = \theta(g)\theta(n)\theta(g^{-1}) = (x, y)(a, e)(x^{-1}, y^{-1}) = (xax^{-1}, e).$$

   Thus, $\theta(gng^{-1}) \in A \times \{e\}$ and so $gng^{-1} \in N$. Thus, $N \triangleleft G$. By a similar argument, $M \triangleleft G$.

   We have $N \cap M = \{e\}$, since if $x \in N \cap M$, then $\theta(x) = (a, e)$ and $\theta(x) = (e, b)$ and so $\theta(x) = (e, e)$. Furthermore, since θ is an isomorphism, then $\ker \theta = \{e\}$ and so $x = e$. Thus, $G = NM \cong N \times M$. □

9. Determine, with explanation, if the following are always true.

   (a) If $N \triangleleft G$ and $M \triangleleft G$, then $NM \triangleleft G$.

   Proof. We have that $NM \subseteq_g G$. Let $x \in NM$ and let $g \in G$. Then we want to show that $gxg^{-1} \in NM$. Since $x \in NM$, then for some $n \in N$ and $m \in M$, we can write $x = nm$. Thus,

   $$gxg^{-1} = gnmg^{-1} = (gng^{-1})(gmg^{-1}).$$

   Since both N and M are normal in G, then the left term is an element of N and the right term is an element of M. Thus, the product is an element of NM. Therefore, $NM \triangleleft G$. □

(b) If M and N are Abelian subgroups of G, $N \cap M = \{e\}$, and $G = NM$, then G is Abelian.

Proof. This is not true. Not enough time to think of a counter example! □

(c) If I and J are ideals of R, then $I + J$ is an ideal of R.

Proof. In order for $I + J$ to be an ideal of R, we need $(I + J, +)$ to be a subgroup of R and if $a \in I + J$ and $r \in R$, then $a \cdot r \in I + J$ and $r \cdot a \in I + J$. Clearly, $I + J \subseteq R$. So then let $a, b \in I + J$. Then $a = g_1 + h_1$ and $b = g_2 + h_2$. Thus, $a - b = (g_1 - g_2) + (h_1 - h_2) \in I + J$. Thus, $I + J$ is a subgroup of R. Now let $a \in I + J$ and $r \in R$. Then call $a = x + y$. Then $r \cdot (x + y) = r \cdot x + r \cdot y \in I + J$ and $(x + y) \cdot r = x \cdot r + y \cdot r \in I + J$. Thus, $I + J$ is an ideal of R. □

10. Assume that R is a commutative ring with identity, and $J = \{a \in R \colon a^{-1} \in R\}$. Prove that $(J, \cdot)$ is a group. Determine J for $R = \mathbb{Z}_n$ and for $R =$ a field.

Proof. First we must show that J is non-empty. Since $1 \in R$ and $1 \cdot 1 = 1$, then $1 \in J$. Now let $a, b \in J$. Then we want to show that $a \cdot b \in J$. Since R is a ring, then $a \cdot b \in R$ and $b^{-1} \cdot a^{-1} \in R$. Next, since $(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = 1$, then $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$. Therefore, $a \cdot b \in J$. Now let $a, b, c \in J$. Then since $a \cdot b \in R$ and $b^{-1} \cdot a^{-1} \in R$, and $c \in R$ and $c^{-1} \in R$, then $(a \cdot b) \cdot c \in J$. Similarly, $a \cdot (b \cdot c) \in J$. Thus, $((a \cdot b) \cdot c) \cdot (a \cdot (b \cdot c))^{-1} = ((a \cdot b) \cdot c) \cdot c^{-1} \cdot b^{-1} \cdot a^{-1} = 1$. Thus, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. Finally, since $a \in J$, then $a^{-1} \in J$ since $(a^{-1})^{-1} = a$.

Now let $R = \mathbb{Z}_n$. Then by HW 1, $J = \mathbb{Z}_{(n)}$. Lastly, if R is a field, then $J = R - \{0\}$. □

2 Ring Theory Results

1. Assume that $(R, +, \cdot)$ is a commutative ring with identity, and that $n1_R = 0$. Then $\text{char}(R) \mid n$.

Proof. Let char(R) $= m$. By the Quotient Remainder Theorem, there exists $q, r \in \mathbb{Z}$ such that $n = qm + r$ and $0 \leq r < m$. Then

$$n1_r = (qm + r)1_R = qm1_r + r1_r = q(m1_R)_r1_R = 0 + r1_R = 0.$$

Since $r < m$, then $r = 0$. Thus, $n = qm$ and, therefore, $m \mid n$. □

2. Assume that $(R, +, \cdot)$ is a commutative ring with identity and $a \in R$. Let $(a)_i = \{r \cdot a \colon r \in R\}$. Then $(a)_i$ is an ideal of R, and $(a)_i$ is the smallest ideal of R that contains a.

Proof. First we must prove that $((a)_i, +)$ is a subgroup of $(R, +)$. Note that $1 \in R$ and so $1 \cdot a \in (a)_i$. Thus $(a)_i \neq \varnothing$. It is also clear that $(a)_i \subseteq R$. Now let $x, y \in (a)_i$. Then for some $r_1, r_2 \in R$, $x = r_1 \cdot a$ and $y = r_2 \cdot a$. Additionally, since $r_2 \in R$, then $-r_2 \in R$. Moreover, since $-r_2 \cdot y = -(r_2 \cdot y) = -y$, then $-y \in R$. Thus, $x - y = r_1 \cdot a + -(r_2 \cdot a) = (r_1 - r_2) \cdot a \in (a)_i$. Thus, $((a)_i, +)$ is a subgroup of $(R, +)$. Let $r \in R$ and let $x \in (a)_i$, then for some $r' \in R$, $x = r' \cdot a$ and $r \cdot x = r \cdot r' \cdot a \in (a)_i$. Similarly, $x \cdot r = r' \cdot a \cdot r$ □