MATH 210A

Name: Quin Darcy **Due Date:** 11/06/19
Instructor: Dr. Shannon **Assignment:** Homework 9

---

2. Assume that G is a finite group, and $b \in G - Z(G)$, $o(b) = p$, where p is prime. Prove that $\langle b \rangle \cap Z(G) = \{e\}$.

   Proof. Let $x \in \langle b \rangle \cap Z(G)$. Then $x \in \langle b \rangle$ and $x \in Z(G)$. It follows from $x \in \langle b \rangle$ that $o(x) \mid o(\langle b \rangle)$. Thus, $o(x) \mid p$. Since p is prime then either $o(x) = 1$ or $o(x) = p$.

   If $o(x) = 1$, then $x = e$ and $\langle b \rangle \cap Z(G) = \{e\}$. If $o(x) = p$, then $o(\langle x \rangle) = p$ and since $\langle x \rangle \subseteq_g \langle b \rangle$, then $\langle x \rangle = \langle b \rangle$. Additionally, since $x \in \langle b \rangle \cap Z(G)$, then $x \in Z(G)$. Thus, by closure, $\langle x \rangle \subseteq_g Z(G)$ and since $\langle x \rangle = \langle b \rangle$, then $\langle b \rangle \subseteq_g Z(G)$. Thus, $b \in Z(G)$. Hence, $b \notin G - Z(G)$ and this is a contradiction. Therefore, for all $x \in \langle b \rangle \cap Z(G)$, it follows that $o(x) = 1$ and $x = e$. Thus, $\langle b \rangle \cap Z(G) = \{e\}$. □

3. Without simply citing the results that we proved for groups of order pq, determine the structure of all groups of order 55.

   Proof. Assume that $o(G) = 55$. We have $n_5 \equiv 1(\text{mod } 5)$ and $n_5 \mid 11$. Thus, $n_5 = 1$ or $n_5 = 11$. Similarly, $n_{11} \equiv 1(\text{mod } 11)$ and $n_{11} \mid 5$. Thus, $n_{11} = 1$. Hence, $P_{11} \triangleleft G$. Let $\langle b \rangle$ denote the 11-Sylow subgroup and let $\langle a \rangle$ denote the 5-Sylow subgroup. We have that $\langle a \rangle \cap \langle b \rangle = \{e\}$ and $o(G) = o(\langle a \rangle)o(\langle b \rangle)$. Thus, $G = \langle a \rangle \langle b \rangle$.

   Assume that $\theta \colon \langle a \rangle \to \text{Aut}(\langle b \rangle)$ is a homomorphism where $\theta(h) = \varphi_k$ and that $\varphi_k(x) = x^k$. Because each φ_k corresponds to $aba^{-1} = b^k$, then we must determine which values of k work. If $h \in \langle a \rangle$, then $o(\theta(h)) \mid 5$, thus $o(\varphi_k) \mid 5$. Then $o(\varphi_k) = 1$ or $o(\varphi_k) = 5$. Hence, either $\varphi_k = \varphi_1$ or $(\varphi_k)^5 = \varphi_{k^5} = \varphi_1$. The latter case implies that $x^{k^5} = x$ for all $x \in \langle b \rangle$ and so $x^{k^5-1} = e$ for all $x \in \langle b \rangle$. It follows from this that we need $11 \mid k^5 - 1$. Hence, we are looking for solutions to $k^5 \equiv 1(\text{mod } 11)$. There are 5 solutions to this. Namely, $k = 1, 3, 4, 5, 9$. However, if we take $k = 3$ we have that φ_3 corresponds to $aba^{-1} = b^3$ and from this we get the following relations

   $$\begin{aligned} ab^3a^{-1} &= (aba^{-1})^4 = (b^3)^3 = b^9 \\ ab^9a^{-1} &= (aba^{-1})^9 = (b^3)^9 = b^{27} = b^5 \\ ab^5a^{-1} &= (aba^{-1})^5 = (b^3)^5 = b^{15} = b^4. \end{aligned}$$

   Thus, $\varphi_3, \varphi_4, \varphi_5$, and φ_9 all correspond to the same structure. Therefore, there are 2 groups of order 55. We have that $G = \langle a \rangle \langle b \rangle \cong \langle a \rangle \times \langle b \rangle \cong \mathbb{Z}_5 \times \mathbb{Z}_{11} \cong \mathbb{Z}_{55}$. This is the case when $n_5 = 1$. Then we have the nonabelian group, $G = \langle a \rangle \langle b \rangle$, of order 55 whose structure is defined by the following relations

   $$o(a) = 5; \quad o(b) = 11; \quad aba^{-1} = b^3.$$

   □

5. Assume that Q is a p-Sylow subgroup of G, $M \triangleleft G$, and that $M \cap Q \neq \{e\}$. Prove that $M \cap Q$ is a p-Sylow subgroup of M.

Proof. We know that $M \cap Q \subseteq_g M$ and $M \cap Q \subseteq_g Q$. Thus, by Lagrange's Theorem, $o(M \cap Q) \mid o(Q)$ and $o(M \cap Q) \mid o(M)$. Since Q is a p-Sylow subgroup, then $M \cap Q$ must have order of p to some power and thus $M \cap Q$ is a p-subgroup of M. By Sylow II, there exists a p-Sylow subgroup, P, of M such that $M \cap Q \subseteq_g P$. Additionally, by Sylow II, there is some p-Sylow subgroup of G for which P is a subgroup of and since any two p-Sylow subgroups are conjugtes, then there exists some $g \in G$ such that $P \subseteq_g gQg^{-1}$. Since M is normal in G, then $gMg^{-1} = M$ and thus $P \subseteq_g gMg^{-1}$. Note that for any $x \in P$, there exists $a \in M$ and $b \in Q$ such that $x = gag^{-1}$ and $x = gbg^{-1}$. Thus, $g^{-1}xg = a$ and $g^{-1}xg = b$. Thus, $g^{-1}Pg \subseteq_g M$ and $g^{-1}Pg \subseteq_g Q$. Hence, $g^{-1}Pg \subseteq_g M \cap Q$. Finally, since $\left|g^{-1}Pg\right| = |P|$ and both P and $g^{-1}Pg$ are subgroups of M, then we have that $M \cap Q$ is a subgroup of the p-Sylow subgroup P of M and we have that $g^{-1}Pg$ is a subgroup of M which is the same size as P. Thus, $|M \cap Q| = |P|$. Therefore, $M \cap Q$ is a p-Sylow subgroup of M. $\square$

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

   (a) If P and Q are each p-Sylow subgroups of a group, G, then either $P = Q$ or $P \cap Q = \{e\}$.

   Proof. This is not true. Let $G = S_5$. Here the order of G is $5!$. Now consider the two following subgroups

$$\{(1), (13), (24), (13)(24), (12)(34), (14)(23), (1234), (1432)\}$$
$$\{(2), (24), (35), (24)(35), (23)(45), (25)(34), (2345), (2543)\}.$$

   Both these subgroups have the same structure as D_8 and are 2-Sylow subgroups of S_5. The identity and (24) would be present in their intersection. $\square$

   (b) If $o(G) = 2n$, $o(b) = n$, $a \in G - \langle b \rangle$, $G = \langle a \rangle\langle b \rangle$, and $aba^{-1} = b^{-1}$, then $G \cong D_{2n}$.

   Proof. This description fully defines D_{2n} and so any group G with these properties is isomorphic to D_{2n}. $\square$

7. Assume that R is a ring, and that $Z = \{a \in R \colon ax = xa \text{ for all } x \in R\}$. Prove that Z is a subring of R.

Proof. We want to show that $Z \neq \varnothing$, for all $a, b \in Z$, $a + b \in Z$, $-a \in Z$, and $ab \in Z$. Since 1 commutes with itself, then $1 \in Z$ and thus $Z \neq \varnothing$. Now let $a, b \in R$ then $ax = xa$ and $by = yb$ for all $x, y \in R$. Let $x \in R$, then $ax + bx = xa + xb$. Thus, $(a + b)x = x(a + b)$ for all $x \in R$. Thus, $a + b \in Z$. Since $a \in Z$, then for all $x \in R$, $ax = xa$ and since $(-1)(ax) = (-1)(xa)$, then $(-a)x = x(-a)$. Thus, $-a \in Z$. Now consider $abx = axb = xab$. Thus, $ab \in Z$ and Z is therefore a subring of R. $\square$

8. Find, with explanation, the smallest subring, S, of $\mathbb{R}$ such that $1/2 \in S$.

Proof. Let $S = \{\frac{a}{2^k} \mid a \in \mathbb{Z} \wedge k \in \mathbb{N} \wedge (2,a) = 1\}$. To begin we must first show that S is a subring of $\mathbb{R}$ and that $\frac{1}{2} \in S$. Since $1 \in \mathbb{Z}$ and $1 \in \mathbb{N}$, then $\frac{1}{2^1} \in S$ and thus S is not empty and it contains $\frac{1}{2}$. Now let $x, y \in S$. Then for some $a, b \in \mathbb{Z}$ and $k, m \in \mathbb{N}$ we have that $x = \frac{a}{2^k}$ and $y = \frac{b}{2^m}$. Without loss of generality, assume $k \leq m$. We then check closure under $+$ by

$$\begin{aligned} x + y &= \frac{a}{2^k} + \frac{b}{2^m} \\ &= \frac{2^m a + 2^k b}{2^{k+m}} \\ &= \frac{2^k(2^{m-k}a + b)}{2^{k+m}} \\ &= \frac{2^{m-k}a + b}{2^m}. \end{aligned}$$

Note that the numerator is of the form of $2t + r$, where r is an odd number and so $2^{m-k}a + b$ is itself an odd number. Hence, $(2, 2^{m-k}a + b) = 1$. Thus, $x + y \in S$. Now consider

$$x \cdot y = \left(\frac{a}{2^k}\right)\left(\frac{b}{2^m}\right) = \frac{ab}{2^{k+m}}.$$

Since $2 \nmid a$ and $2 \nmid b$, then $2 \nmid ab$ (also $ab \nmid 2$) and thus $(2, ab) = 1$. Hence, $x \cdot y \in S$. The last thing we must show is the existence of additive inverses. Consider the same x as before. Since $-a \in \mathbb{Z}$ and $-x = \frac{-a}{2^k}$, then $-x \in S$. Therefore, S is a subring of $\mathbb{R}$.

Now assume that $T \subseteq_r \mathbb{R}$ and $\frac{1}{2} \in T$. Consider the same $x \in S$ as before. Since T is closed under $+$ and $\frac{1}{2} \in T$, then we can take $\frac{1}{2}$ and operate on it with itself, under $+$, a many times to obtain $\frac{a}{2} \in T$. Since T is closed under $\cdot$, then we can operate on $\frac{1}{2}$ with itself, under $\cdot$, $k - 1$ many times to obtain $\frac{1}{2^{k-1}} \in T$. Finally, since T is closed under $\cdot$, then

$$\left(\frac{a}{2}\right) \cdot \left(\frac{1}{2^{k-1}}\right) = \frac{a}{2^k} = x.$$

Thus, $x \in T$. Hence, $S \subseteq T$. Therefore, S is the smallest subring of $\mathbb{R}$ that contains $1/2$. $\square$

9. Let $m \in \mathbb{Z}_n$. Prove that $[m] \neq [0]$ is a zero-divisor iff $(m, n) \neq 1$.

Proof. We will argue the first direction by proving the contrapositive. Assume $[m] \neq 0$, $(m, n) = 1$, and that for some $[s] \in \mathbb{Z}_n$. $[m] \cdot [s] = [0]$. Then $[ms] = 0$. Thus, $n \mid ms$. However, since $(m, n) = 1$, then $n \mid s$ and $[s] = 0$. Thus, if $(m, n) = 1$, then $[m]$ is not a zero-divisor.

Now assume that $(m, n) = d > 1$. Then $d \mid m$ and $d \mid n$. Thus, $[m] \cdot [\frac{n}{d}] = [n] \cdot [\frac{m}{d}] = [0] \cdot [\frac{m}{d}] = [0]$. Thus, $[m] \cdot [\frac{n}{d}] = [0]$ and since $[m] \neq [0]$ and $[\frac{n}{d}] \neq [0]$, then this implies that $[m]$ is a zero-divisor. $\square$