H/wk 14, Solutions to selected problems

Ch. 8.3, Problem 13
Let $G = (\mathbb{R}, +)$, and define $a \cdot z = e^{ia}z$ for $z \in \mathbb{C}$ and $a \in \mathbb{R}$.
Show that $\mathbb{C}$ is a $G$-set, describe the action geometrically and find all orbitz and stabilizers.

**Solution.**
First, we check that $\mathbb{C}$ is a $G$-set. For any $z \in \mathbb{C}$ we have $0 \cdot z = e^{0}z = z$. Also, for any $z \in \mathbb{C}$ and $a, b \in \mathbb{R}$ we have
$$a \cdot (b \cdot z) = a \cdot (e^{ib}z) = e^{ia}e^{ib}z = e^{i(a+b)}z = (a + b) \cdot z.$$ Thus this is indeed a group action of $G = (\mathbb{R}, +)$ on $\mathbb{C}$.

Recall, that in polar coordinates when two complex numbers are multiplies, their polar angles are added and their absolute values are multiplied. Recall also that $e^{ia} = \cos a + i\sin a$. Hence, geometrically, for $a \in \mathbb{R}$ and $z \in \mathbb{C}$ the point $a \cdot z = e^{ia}z$ is obtained by rotating the point $z$ around the origin counterclockwise by angle $a$.

Thus for $z_0 \neq 0$ we have $Gz_0 = \{z \in \mathbb{C} : |z| = |z_0|\}$, so that the orbit $Gz_0$ is the circle around the origin of radius $|z_0|$. For $z_0 = 0 \in \mathbb{C}$ we have $Gz_0 = \{z_0\} = \{0\}$.

For $z_0 \in \mathbb{C}$, $z_0 \neq 0$ the stabilizer of $z_0$ in $G$ is
$$\text{Stab}_G(z_0) = \{2\pi n : n \in \mathbb{Z}\}.$$ Finally, for $z_0 = 0 \in \mathbb{C}$ we have $\text{Stab}_G(z_0) = G$.

Ch. 8.3, Problem 23
Let $X$ be a $G$-set and let $x, y \in X$.
(a) Show that the stabilizer $S(x)$ is a subgroup of $G$.

**Solution.**
Note that by definition of a group action $e \cdot x = x$, so that $e \in S(x)$.
Let $g, h \in S(x)$, that is $g \cdot x = x$ and $h \cdot x = x$.
Then
$$(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x$$
and hence $gh \in S(x)$.
Finally, let $g \in S(x)$, so that $g \cdot x = x$.
Then
$$g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = e \cdot x = x$$
so that $g^{-1} \in S(x)$. Thus indeed $S(x) \leq G$ is a subgroup of $G$.

(b) If $x \in X$ and $g \in G$, show that $S(b \cdot x) = bS(x)b^{-1}$.

**Solution.**
Let $g \in S(b \cdot x)$ be arbitrary. Thus $g \cdot (b \cdot x) = b \cdot x$, so that $gb \cdot x = b \cdot x$. Applying $b^{-1}$ to both sides we get
$$b^{-1} \cdot (gb \cdot x) = b^{-1} \cdot (b \cdot x) \implies b^{-1}gb \cdot x = x.$$ Hence $h := b^{-1}gb \in S(x)$ and therefore $g = bhb^{-1} \in bS(x)b^{-1}$. This shows that $S(b \cdot x) \subseteq bS(x)b^{-1}$.
Suppose now that $g \in bS(x)b^{-1}$ be arbitrary. Thus $g = bhb^{-1}$ for some $h \in S(x)$, that is for some $h$ such that $h \cdot x = x$. Then
$$g \cdot (b \cdot x) = bhb^{-1} \cdot (b \cdot x) = bh \cdot ((b^{-1}b) \cdot x) = bh \cdot x = b \cdot (h \cdot x) = b \cdot x.$$
Thus \( g \in S(b \cdot x) \) and hence \( bS(x)b^{-1} \subseteq S(b \cdot x) \).

It follows that \( S(b \cdot x) = bS(x)b^{-1} \), as required.

(c) If \( S(x) \) and \( S(y) \) are conjugate subgroups of \( G \), show that \( |Gx| = |Gy| \).

**Solution**

We first need to establish the following general lemma:

**Lemma.** Let \( G \) be a group, \( H \leq G \) be a subgroup and let \( u \in G \). Then \([G : H] = [G : uHu^{-1}]\).

**Proof of Lemma.** By definition \([G : H] = |G/H| = |\{gH : g \in G\}|\) and \([G : uHu^{-1}] = |G/uHu^{-1}| = |\{guHu^{-1} : g \in G\}|\). Thus it suffices to construct a bijection between the sets \( G/H \) and \( G/uHu^{-1} \). Define \( f : G/H \to uHu^{-1} \) by \( f(gH) := ugu^{-1}uHu^{-1} \) for \( g \in G \). Note first that \( f \) is well-defined. We claim that \( f \) is one-to-one. We have verified that \( f \) is onto. Suppose now that \( f(g_1H) = f(g_2H) \) so that \( ugu^{-1}uHu^{-1} = ugu^{-1}uHu^{-1} \). Hence \( uga^{-1}u^{-1}z \) for some \( z \in uHu^{-1} \), that is for some \( h \in H \) we have \( uga^{-1}u^{-1} = uga^{-1}u^{-1} \). Therefore \( g_2 = g_1h \) and hence \( g_1H = g_2H \). Thus \( f \) is one-to-one. We have verified that \( f \) is bijective so that \([G : H] = [G : uHu^{-1}]\) as claim. This completes the proof of the lemma.

Now let \( x \) and \( y \) be as in part (c) of the problem. By the orbit-stabilizer formula (Lemma 3 in Ch 8.3) we have \([Gx] = [G : S(x)]\) and \([Gy] = [G : S(y)]\). Since \( S(x) \) and \( S(y) \) are conjugate in \( G \), the Lemma implies that \([G : S(x)] = [G : S(y)]\) and hence \([Gx] = [Gy]\) as required.

**Ch. 8.4, Problem 2**

Find all Sylow 2-subgroups of \( D_n \), where \( n \) is odd, and show explicitly that they are conjugate.

**Solution.**

Let \( n \geq 3 \) be odd. Then \(|D_n| = 2n\), so every Sylow 2-subgroup of \( D_n \) has order 2 and has the form \( \langle g \rangle = \{1, g\} \) where \( g \in D_n \) is an element of order 2. Thus to find all the Sylow 2-subgroups of \( D_n \) we need to find all elements of order 2 in \( D_n \).

Recall that \( D_n = \{1, a, a^2, \ldots, a^{n-1}, b, ba, \ldots ba^{n-1}\} \)

where \(|a| = n, |b| = 2\) and \( aba = b \).

Since \(|a| = |\langle a \rangle| = n \) is odd, for every \( g \in \langle a \rangle \) we have \(|g||n \) and hence \(|g| \neq 2 \).

We claim that \(|ba^i| = 2\) for every \( i = 0, 1, \ldots, n - 1 \). Indeed, \( aba = b \) implies \( ab = ba^{-1} \) and \( a^ib = a^{-i}b \) for all \( i \). Hence 

\[
(ba^i)^2 = ba^iaba = bba^{-i}a^i = b^2 = 1.
\]

Since \( ba^i \neq 1 \), it follows that \(|ba^i| = 2\) for \( i = 0, 1, \ldots, n - 1 \). Thus \( D_n \) has \( n \) elements of order 2 and, correspondingly, \( n \) Sylow 2-subgroups, namely, the subgroups \( \langle ba^i \rangle = \{1, ba^i\} \) for \( i = 0, \ldots, n - 1 \). To see that they are all conjugate, it suffices to show that \( ba^i \) is conjugate to \( b \) for every \( i = 0, \ldots, n - 1 \).
Note that for every \( j \) we have \( a^{-j}ba^j = ba^j = b(a^2)^j \). Since \( n \) is odd and \( gcd(n, 2) = 1 \), it follows that \( (a) = (a^2) \). Thus for every \( i = 0, \ldots, n-1 \) there exists \( j \) such that \( a^j = a^{2j} \) and hence \( ba^j = a^{-j}ba^j \) and \( \langle ba^j \rangle = a^{-j}(b)a^j \). Thus indeed all Sylow 2-subgroups of \( D_n \) are conjugate in \( D_n \).

**Ch. 8.4, Problem 3**

If \( P \) is a Sylow \( p \)-subgroup of \( G \), prove that \( P \) is the only Sylow \( p \)-subgroup of \( N(P) \).

**Solution.**

Let \( |G| = p^n \, m \) where \( n \geq 1 \) and \( gcd(p, m) = 1 \). Since \( P \leq G \) is a Sylow \( p \)-subgroup of \( G \), we have \( |P| = p^n \). We have \( P \leq N(P) \leq G \). Hence \( |P|/|N(P)| \) and \( |N(P)|/|G| \). Thus \( p^n/|N(P)| \) and \( |N(P)|/p^m \). Hence \( |N(P)| = p^n \, m' \) where \( m' \mid m \) and \( gcd(p, m') = 1 \).

Since \( |P| = p^n \) and \( P \leq N(P) \), it follows that \( P \) is a Sylow \( p \)-subgroup of \( N(P) \). By definition, every subgroup is normal in its normalizer, and hence \( P \triangleleft N(P) \).

By the Second Sylow Subgroup Theorem every Sylow \( p \)-subgroup \( P' \) of \( N(P) \) is conjugate to \( P \) in \( N(P) \). Since \( P \triangleleft N(P) \), this implies that \( P' = P \). Hence \( P \) is the unique Sylow \( p \)-subgroup of \( N(P) \), as claimed.

**Ch. 8.4, Problem 4**

Prove that every group of order 15 is cyclic.

**Solution.**

Let \( G \) be a group such that \( |G| = 15 = 3 \cdot 5 \). Let \( n_3 \) be the number of Sylow 3-subgroups of \( G \). Then by the Third Sylow Subgroup Theorem \( n_3 \mid 5 \) and \( n_3 \equiv 1 \) mod 3. The condition \( n_3 \mid 5 \) implies that \( n_3 = 1 \) or \( n_3 = 5 \). The case \( n_3 = 5 \) is impossible since \( 5 \not\equiv 1 \) mod 3. Thus \( n_3 = 1 \). Let \( H \leq G \) be the Sylow 3-subgroup of \( G \), so that \( |H| = 3 \). Since for every \( g \in G \) we have \( |gHg^{-1}| = |H| = 3 \) and \( gHg^{-1} \leq G \) is also a Sylow 3-subgroup of \( G \), the condition \( n_3 = 1 \) implies that \( gHg^{-1} = H \). Hence \( H \triangleleft G \) is normal in \( G \).

Let \( n_5 \) be the number of Sylow 5-subgroups of \( G \). Then by the Third Sylow Subgroup Theorem \( n_5 \mid 3 \) and \( n_5 \equiv 1 \) mod 5. The condition \( n_5 \mid 3 \) implies that \( n_5 = 1 \) or \( n_5 = 5 \). The case \( n_5 = 3 \) is impossible since \( 3 \not\equiv 1 \) mod 5. Thus \( n_5 = 1 \).

As above, this implies that if \( K \leq G \) is a Sylow 5-subgroup (that is \( |K| = 5 \)) then \( K \triangleleft G \).

We claim that \( H \cap K = \{1\} \). Indeed, suppose \( a \in H \cap K \). Then, since \( a \in H \), we have \( |a||H| \), that is \( |a| \mid 3 \). Similarly, since \( a \in K \), we have \( |a||K| \), that is \( |a| \mid 5 \).

Hence \( |a| = 1 \) and therefore \( a = 1 \). Thus indeed \( H \cap K = \{1\} \).

Finally we have \( |H| \cdot |K| = 3 \cdot 5 = |G| \).

Thus \( H \triangleleft G \) and \( K \triangleleft G \). Then \( K \cap H = \{1\} \) and \( |H| \cdot |K| = |G| < \infty \). Hence by Theorem 6 in Ch 2.8 we have \( G \cong H \times K \). Since \( |H| = 3 \) is a prime, it follows that \( H \) is cyclic of order 3 and thus \( H \cong \mathbb{Z}_3 \). Similarly, since \( |K| = 5 \) is a prime, it follows that \( K \) is cyclic of order 5 and thus \( K \cong \mathbb{Z}_5 \). Thus \( G \cong H \times K \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \). Since \( gcd(3, 5) = 1 \), we have \( \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15} \). Therefore \( G \cong \mathbb{Z}_{15} \), so that \( G \) is cyclic, as required.

**Ch. 8.4, Problem 13**

If \( |G| = p^n \, m \) where \( n \geq 1 \), \( p \) is a prime and \( p > m \), show that the Sylow \( p \)-subgroup of \( G \) is normal in \( G \).
Solution.
Let \( n_p \) be the number of Sylow \( p \)-subgroups of \( G \). By the 3-d Sylow Subgroup Theorem we know that \( n_p |m \) and that \( n_p \equiv 1 \mod p \).

Since \( m < p \) and \( n_p |m \), it follows that \( 1 \leq n_p \leq m < p \). Since we also know that \( n_p \equiv 1 \mod p \), it follows that \( n_p = 1 \). Let \( P \) be a Sylow \( p \)-subgroup of \( G \). Since for every \( q \in G \), \( g^{-1}Pg \) is also a Sylow \( p \)-subgroup of \( G \) and since \( n_p = 1 \), it follows that for every \( g \in G \), \( g^{-1}Pg = P \). Hence \( P \) is normal in \( G \), as claimed.

Ch. 8.4, Problem 14
If \( |G| = p^2q \) where \( p \) and \( q \) are primes, show that \( G \) is not simple.

Solution.
Suppose first that \( p = q \). Then \( |G| = p^3 \) and \( G \) is a finite \( p \)-group. As was proved in class, every finite \( p \)-group has a nontrivial center, \( Z(G) \neq \{1\} \). If \( Z(G) \neq G \) then \( Z(G) \triangleleft G \) and \( Z(G) \neq G, Z(G) \neq \{1\} \), so that \( G \) is not simple. If \( Z(G) = p^3 \) then \( G \) is abelian. By the First Sylow Subgroup Theorem \( G \) has a subgroup \( H \) of order \( p \). Then \( H \neq \{1\}, H \neq G \) and \( H \triangleleft G \) and hence \( G \) is not simple.

Suppose now that \( p \neq q \). By the Third Sylow Subgroup Theorem \( n_p |q \) and \( n_p \equiv 1 \mod p \). Hence \( n_p \in \{1, q\} \) and \( n_p = 1 + pk \) for some integer \( k \). If \( n_p = 1 \) then the Sylow \( p \)-subgroup of \( G \) is a proper normal subgroup in \( G \) and hence \( G \) is not simple.

Suppose now that \( n_p = q \). Since \( n_p - 1 = pk \), we have \( q - 1 = pk \) and hence \( p \leq q - 1 \).

Again applying the Third Sylow Subgroup Theorem we get \( n_p |p^2 \) and \( n_p \equiv 1 \mod q \). Thus \( n_p \in \{1, p, p^2\} \). If \( n_p = 1 \), then he Sylow \( q \)-subgroup of \( G \) is a proper normal subgroup in \( G \) and hence \( G \) is not simple, as required.

If \( n_p = p \) then the condition \( n_p \equiv 1 \mod q \) implies \( q |p - 1 \) and hence \( q \leq p - 1 \).

Since we already know that \( p \leq q - 1 \), this yields a contradiction.

Thus \( n_p = p^2 \). Hence \( n_p \equiv 1 \mod q \) implies \( q |(p^2 - 1) \), that is \( q |(p - 1)(p + 1) \).

Since \( q \) is a prime, it follows that \( q |p + 1 \) or \( q |p - 1 \).

If \( q |p - 1 \) then \( q \leq p - 1 \). Since we already know that \( p \leq q - 1 \), this again yields a contradiction.

Thus \( q |p + 1 \) and hence \( q \leq p + 1 \). Since we already know that \( p \leq q - 1 \), we have \( p + 1 \leq (q - 1) + 1 = q \). Thus \( q \leq p + 1 \leq q \) and hence \( q = p + 1 \).

Since both \( p \) and \( q \) are primes and \( q = p + 1 \), the numbers \( p \) and \( q \) cannot both be odd. The only even prime is 2 and hence \( p = 2, q = 3 \). Therefore \( |G| = p^2q = 2^2 \cdot 3 = 12 \).

By Theorem 5 in Ch 8.4 every group of order 12 is isomorphic to one of \( C_{12}, C_6 \times C_2, A_4, D_6 \) or \( Q_6 \). None of these groups are simple and hence \( G \) is not simple, as required.

We can check that none of the groups in the above list are simple directly. Indeed, if \( C_{12} = \langle x \rangle \) is cyclic of order 12, then \( \langle x^2 \rangle \) has order 6 and is a proper normal subgroup of \( C_{12} \).

Similarly, the subgroup \( C_6 \times \{1\} \) is a subgroup of order 6 in the abelian group \( C_6 \times C_2 \) and thus is a proper normal subgroup.

We have seen in class that \( V = \{e, (1 \ 2)(3 \ 4), (1 \ 3)(2 \ 4), (1 \ 4)(2 \ 3)\} \leq A_4 \) is a proper normal subgroup in \( A_4 \) (for example, because it has index 2).

Also, for \( D_6 = \{1, a, \ldots, a^5, b, ba, \ldots, ba^5\} \) with \(|a| = 6, |b| = 2 \) and \( aba = b \) the subgroup \( \langle a \rangle \) has index 2 in \( D_6 \) and is therefore a proper normal subgroup.
Finally, for the group $Q_6 = \{1, a, \ldots, a^5, b, ba, \ldots, ba^5\}$, where $|a| = 6$, $aba = b$ and $b^2 = a^3$, the subgroup $\langle a \rangle$ has index 2 in $D_6$ and is therefore a proper normal subgroup.