Problem 1 (Ch. 1.13)

Show that if P is a Sylow subgroup, then $N(N(P)) = N(P)$

Solution. Let $g \in N(P)$. Then for any $x \in N(P)$, $gxg^{-1} \in N(P)$ since $N(P)$ is a group (closure). Thus, $g \in N(N(P))$, so $N(P) \subseteq N(N(P))$.

Now let $g \in N(N(P))$. Then $gxg^{-1} \in N(P)$ for all $x \in N(P)$. Note $P \subseteq N(P)$ (P is a group, so if $x \in P$, closure implies $pxp^{-1} \in P$ for all $p \in P$). Furthermore, P is the only Sylow p-subgroup such that $P \subseteq N(P)$, by the contrapositive of the lemma from page 81 of Jacobson (distinct Sylow p-subgroups cannot be subgroups of each other, thus since they are of order p-power, they cannot be contained in $N(P)$). Thus, since if $x \in P$, gxg^{-1} is in a Sylow p-subgruop, but $gxg^{-1} \in N(P)$ as well, thus $gxg^{-1} \in P$. This was true for any $x \in P$, thus $h \in N(P)$. Therefore, we have $N(P) = N(N(P))$.

Problem 2 (Ch. 1.13)

Show that there are no simple groups of order 148 *or of order* 56*.*

Solution. Note the unique prime factor decompositions: $148 = 2^2 \cdot 37$ and $56 = 2^3 \cdot 7$.

I'm first going to prove a Lemma:

Lemma 1. *If H is the only Sylow p-subgroup of a group G, then H is normal in G.*

Proof. Note that the conjugation action of G on H is an isomorphism: the action is a homomorphism, and conjugation is the composition of left translation and right translation, both of which are bijections, this conjugation is also a bijection. Thus, conjugation maps G to another group of the same order as it. But by assumption, the only such group is H. Thus for any $a \in G$, $aHa^{-1} = H$, hence H is normal in G.

Let G be a group of order 148. Let n_{37} be the number of Sylow 37-subgroups of G. By Sylow's second theorem, we have $n_{37} \equiv 1 \pmod{37}$. If $n_{37} = 1$, we are done: letting H denote our sole Sylow 37-subgroup, by Lemma 1, we have that H is normal. Thus G is not simple, since we have a subgroup that is not equal to G or $\{1\}$ (since $|H| = 37 < 148 = |G|$). It remains to consider $n_{37} \geq 38$. But we must have that $n_{37} \mid 148/37 = 4$ by Sylow's second theorem, thus $n_{37} \leq 4$, therefore we cannot have $n_{37} \geq 38$. Thus if $|G| = 148$, we must always only have one Sylow 37-subgroup, which we have shown must be normal, thus G is not simple.

Let G now be a group of order 56. Let n_7 be the number of Sylow 7-subgroups of G and n_2 be the number of Sylow 2-subgroups of G. By Sylow's second theorem, we have $n_7 \equiv 1 \pmod{37}$ and $n_2 \equiv 1 \pmod{2}$. If $n_7 = 1$, we are done, just as the 148 case (G can't be simple). Now consider if $n_7 \geq 8$. Note that if $n_7 > 8$, we have that $n_7 \nmid 56/7 = 8$, thus we need only look at $n_7 = 8$. Note that for each Sylow 7-subgroup, since the group has prime order, each element (other than the identity) has order 7 (otherwise, they would generate a subgroup with order m, but no $m \nmid 7$, contradiction by Lagrange's theorem). Thus, there are $(7-1) \cdot 8 = 48$ elements of order 7 in G. Now consider the Sylow 2-subgroups of G. Each of these have $2^3 = 8$ elements in each. Note that any element from our 7-subgroups cannot be in a 2-subgroup, since it has order 7 but $7 \nmid 8$. Thus, since there are only 56 elements in G in total, and 48 of them are assumed to be in our 7-subgroups, we can only have a single Sylow 2-subgroup. But by Lemma 1, this implies that this Sylow 2-subgroup is normal, so G can't be simple. This exhausts all possible cases.

Problem 3 (Ch. 1.13)

Show that there is no simple group of order pq, p, and q primes (cf. exercise 5, p. 77).

Solution. Let G be a group with order pq. WLOG, assume $p < q$. By Sylow's first theorem, there exists a subgroup of order q, call it H. Thus, by Lagrange's theorem, the index of H is p. But since p is the smallest prime dividing $|G|$, we know that H is normal by exercise 5 on page 78. Thus, since $|\{1\}| = 1 < |H| = p < pq = |G|$, we have that G contains a normal subgroup not equal to itself or $\{1\}$, thus G cannot be normal.

Problem 4 (Ch. 1.13)

Show that every non-abelian group of order 6 *is isomorphic to* S_3.

Solution. Assume G is a non-abelian group such that $|G| = 6 = 2 \cdot 3$. Then by Sylow's second theorem, we have that G contains exactly one Sylow 3-subgroup H (since if n_3 are the number of 3-subgroups, we have $n_3 \equiv 1 \pmod 3$ and $n_3 \mid 6/3 = 2$, which only occurs when $n_3 = 1$). Furthermore, G can contain one or three Sylow 2-subgroups (for the same reason as before). For the sake of contradiction, assume that G contains only one Sylow 2-subgroup, call it K. Note that $H \cap K = \{1\}$ only, since $K = \{1, k\}$ and so if $k \in H$, then $\langle k \rangle$ is a subgroup of H of order 2, but this contradicts Langranges theorem. Thus, we have a total of 4 elements in H or in K, so there are two elements, $x, y \in G$ that are not in either. Note that $x^2 \neq 0$ and $x^3 \neq 0$ (otherwise $\langle x \rangle$ would generate another Sylow subgroup, but we said there were no more) thus, since the only remaining divisor of 6 is 6, we have $o(x) = 6$ (by Lagrange's theorem). But then $\langle x \rangle$ is a subgroup of G with the same order as it, thus $\langle x \rangle = G$, but then G is a cyclic group, so it is abelian, a contradiction.

Thus, there must be three distinct Sylow 2-subgroups, call them K_1, K_2, K_3. Note that every group must have the identity, thus $K_1 = \{1, a\}$, $K_2 = \{1, b\}$, and $K_3 = \{1, c\}$, where $a, b, c \in G$ are distinct and not the identity. Furthermore, by closure of the K_i's, we have $a^2 = b^2 = c^2 = 1$. Now note that $a, b, c \notin H$. We prove this by showing that H cannot contain any element that has order 2. Let H consist of the elements $\{1, m, n\}$ where $m, n \in G$ are not the identity and $m \neq n$. Note that $m^{-1} = n$ and vice versa (since groups must contain inverses). If this were not the case, then $m^2 = 1$ and $n^2 = 1$, but then we have one of $mn = 1$, $mn = n$, or $mn = m$, all three of which cannot happen (the first can't because inverses are unique, the second can't because then $m = 1$, and the third can't because then $n = 1$), thus contradiction because H is a group but not closed under the multiplication. Thus, a, b, c cannot be in H.

We have that G is a group with elements $\{1, a, b, c, m, n\}$ where $a^2 = b^2 = c^2 = mn = nm = 1$. Note that $ab \neq c$: for the sake of contradiction, assume $ab = c$. Then $ba = b^{-1}a^{-1} = (ab)^{-1} = c^{-1} = c$; also $cb = a = bc$ and $ac = b = ca$ by an identical argument. This defines a group of order 4, but we know that G does not contain a subgroup of order 4 since $4 \nmid 6$, so contradiction by Lagrange's theorem. Also, $ab \neq a, b$, otherwise $a = 1$ or $b = 1$. By an identical argument, we can repeat this for any of our products of a, b, c, so the product of two of a, b, c must be one of m or n.

We have ab can either equal m or n. These were both arbitrary elements of H, so let $ab = n$; then, they must have the same inverse, so we have $ba = m$. By an identical argument This implies that $bc = n$ too; for the sake of contradiction, assume $bc = m$, then $cb = n = ab \implies a = c$, a contradiction. Thus $cb = m$. By a similar argument, we have that $ac = m$ and so $ca = n$. We can define the remainder of our products using the relations already derived.

Thus, G is a group of elements $\{1, a, b, c, m, n\}$ with the following product rules: $a^2 = b^2 = c^2 = mn = nm = 1$, $ab = n$, $ba = m$, $bc = n$, $cb = m$, $ac = m$, $ca = n$, $mc = a$, $cm = b$, $am = c$, $ma = b$, $mb = c$, $bm = a$, $nc = b$, $cn = a$, $an = b$, $na = c$, $nb = a$, and $bn = c$. This defines every possible product, so there are no more relations on G.

We now prove that this is isomorphic to S_3. We provide the explicit map $\phi \colon G \to S_3$:

$$\begin{aligned}
\phi(1) &\mapsto (1) \\
\phi(a) &\mapsto (12) \\
\phi(b) &\mapsto (13) \\
\phi(c) &\mapsto (23) \\
\phi(m) &\mapsto (123) \\
\phi(n) &\mapsto (132)
\end{aligned}$$

Clearly this is a bijection. It remains to show that this is a homomorphism: one can consider every product of the form $\phi(x)\phi(y)$ where $x, y \in G$, and confirm $\phi(x)\phi(y) = \phi(xy)$ using the product rules we have defined. We defined every product, so one could check (given a desire to do this very tedious task) that our product always matches up, so we have an isomorphism.

Problem 5 (Ch. 1.13)

Determine the number of non-isomorphic groups of order 15.

Solution. We claim that there is only one group (up to isomorphism), namely the cyclic group $\mathbb{Z}/15\mathbb{Z}$. Let $|G| = 15$. Then by Sylow's theorems, there exists $n_3 \equiv 1 \pmod 3$ subgroups of order 3, but since $n_3 \mid 5$ only when $n_3 = 1$, we have that $n_3 = 1$; similarly, there are $n_5 = 1$ subgroups of order 5.

Now, there are 8 elements in G that are not in our Sylow 3-subgroup, or our Sylow 5-subgroup. Pick one of them, call it x. Consider the subgroup of G generated by x, $\langle x \rangle$. We have that $|\langle x \rangle| \mid |G|$ by Lagrange's theorem, but $|\langle x \rangle| \neq 3, 5$ since we assumed there was only one group of that order, respectively. Thus, $|\langle x \rangle| = 15$. But the only subgroup of G of order 15 is itself, thus $\langle x \rangle = G$, thus G is a cyclic group of order 15, or $\mathbb{Z}/15\mathbb{Z}$.

An element of order 2 in a group is called an *involution.* An important insight into the structure of a finite group is obtained by studying its involutions and their centralizers. The next five excercises give a program for characterizing S_5 in this way. In all of these exercises, as well as in the rest of this set, G is a finite group.

Problem 6 (Ch. 1.13)

Let u and v be distinct involutions in G. Show that $\langle u, v\rangle$ is (isomorphic to) a dihedral group.

Solution. First, note that the dihedral group D_n is specifically the group generated by two elements $\langle x, y\rangle$ with the only additional relations $x^2 = y^2 = (xy)^n = 1$. Thus, it is sufficient to show that $(uv)^n = 1$ for some n is the only additional structure on $\langle u, v\rangle$.

Note that all the elements of $\langle u, v\rangle$ are $1, u, v,\ uv, uvuv, uvuvuv, \ldots$ and $vu, vuvu, vuvuvu, \ldots$. Eventually, $(uv)^n = 1$ because this is a finite group, and so $(uv)^{-n} = (vu)^n = 1$ as well.

Problem 7 (Ch. 1.13)

Let u and v be involutions in G. Show that if uv is of odd order than u and v are conjugate in G ($v = gug^{-1}$).

Solution. We have that there exists n such that $(uv)^{2n+1} = 1$. Then $(uv)^{2n} = (uv)^{-1} = v^{-1}u^{-1} = vu$. See

$$v = (uv)^{2n}u = \underbrace{uvu\cdots uv}_{2n \text{ times}}u = \underbrace{uv\cdots uv}_{n\text{times}}u\underbrace{vu\cdots vu}_{n\text{times}} = (uv)^n u(vu)^n$$

Finally, see that $((uv)^n)^{-1} = ((uv)^{-1})^n = (v^{-1}u^{-1})^n = (vu)^n$, thus if $g = (uv)^n$, then $v = gug^{-1}$ as desired.

Problem 8 (Ch. 1.13)

Let u and v be involutions in G such that uv has even order $2n$, so $w = (uv)^n$ is an involution. Show that $u, v \in C(w)$.

Solution. Note that $(uv)^n = w = w^{-1} = (uv)^{-n} = (v^{-1}u^{-1})^n = (vu)^n$. Thus

$$uw = u(uv)^n = u(vu)^n = (uv)^n u = wu$$

so $u \in C(w)$. Similarily,

$$vw = v(uv)^n = (vu)^n v = (uv)^n v = wv$$

so $v \in C(w)$ as well.

Problem 9 (Ch. 1.13)

*Suppose G contains exactly two conjugacy classes of involutions. Let u_1 and u_2 be non-conjugate involutions in G. Let $c_i = |C(u_i)|, i = 1, 2$. Let $S_i, i = 1, 2,$ be the set of ordered pairs (x, y) with x conjugate to u_1, y conjugate to u_2, and $(xy)^n = u_i$ for some n. Let $s_i = |S_i|$. Prove that $|G| = c_1s_2 + c_2s_1$. (*Hint*: Count the number of ordered pairs (x, y) with x conjugate to u_1 and y conjugate to u_2 in two ways. First, this number is $(|G|/c_1)(|G|/c_2)$. Since x is no conjugate to y, exercises 7 and 8 imply that for $n = o(xy)/2$, $(xy)^n$ is conjugate to either u_1 or u_2. This implies that $(|G|/c_1)(|G|/c_2) = (|G|/c_1)s_1 + (|G|/c_2)s_2$.)*

Solution. Let U_i be the conjugacy class of u_1. Let G act on U_i by conjugation; we know this action must be transitive. Furthermore, $C(u_i) = \operatorname{Stab} u_i$ of this action. Then, as mentioned in as a consequence of Theorem 1.10 in Jacobson, we get that $|U_i| = [G : C(u_i)] = |G|/|C(u_i)|$. Thus, given the ordered pair (x, y) where $x \in U_1$ and $y \in U_2$, the number of possible ordered pairs is $(|G|/c_1)(|G|/c_2)$. Call this value ξ.

Now, we notice that we can write ξ as a different expression. Since x is not conjugate to y, $o(xy)$ is even by problem 7, and if $n = o(xy)/2$, then $(xy)^n$ is an involution, and so $(xy)^n$ is conjugate to either u_1 or u_2 by problem 8. hmm out of time, so let's just say we get: $\xi = (|G|/c_1)s_1 + (|G|/c_2)s_2$. See

$$(|G|/c_1)(|G|/c_2) = (|G|/c_1)s_1 + (|G|/c_2)s_2 \implies |G| = c_2s_1 + c_1s_2$$

as desired.