Homework 2

Andrew Tindall
Algebra I

February 3, 2020

1 Problems

Problem 1. In a letter to C. Hermite, E. Betti states that the following substitutions generate a group of order 12:

$$w = 4z, w = \frac{1}{z}, w = 3\frac{z+1}{z-1} (\text{mod } 5).$$

Verify this statement.

Proof. The three substitutions can be viewed as fractional linear transformations of the projective line over $\mathbb{Z}_5$, where we view $4z$ as $\frac{4z+0}{0z+1}$, and $\frac{1}{z}$ as $\frac{0z+1}{1z+0}$. We use the action of a fractional linear transformation on the projective line as $\frac{ax+b}{cx+d}([k:j]) = [ak+bj : dj+ck]$. The projective line over $\mathbb{Z}_5$ has 6 points corresponding to the 5 points of $\mathbb{Z}_5$ along with a "point at infinity," so the three transformations will generate a subgroup of S_6. In order to use cycle notation, we will map the points of the projective line to $1, \dots, 6$:

$$\begin{aligned}
[1:1] &:= 1 \\
[2:1] &:= 2 \\
[3:1] &:= 3 \\
[4:1] &:= 4 \\
[0:1] &:= 5 \\
[1:0] &:= 6
\end{aligned}$$

The first, $z \mapsto 4z$, takes

$$\begin{aligned}
1 = [1:1] \mapsto [4:1] &= 4 \\
2 = [2:1] \mapsto [8:1] = [3:1] &= 3 \\
3 = [3:1] \mapsto [12:1] = [2:1] &= 2 \\
4 = [4:1] \mapsto [16:1] = [1:1] &= 1 \\
5 = [0:1] \mapsto [0:1] &= 5 \\
6 = [1:0] \mapsto [4:0] = [1:0] &= 6
\end{aligned}$$

So, as a cycle, it is (14)(23). The second, $z \mapsto \frac{1}{z}$, takes

$$\begin{aligned}
1 = [1:1] &\mapsto [1:1] &&= 1\\
2 = [2:1] &\mapsto [3:1] &&= 3\\
3 = [3:1] &\mapsto [2:1] &&= 2\\
4 = [4:1] &\mapsto [4:1] &&= 4\\
5 = [0:1] &\mapsto [1:0] &&= 6\\
6 = [1:0] &\mapsto [0:1] &&= 5
\end{aligned}$$

So as a cycle it is (23)(56). The third, $z \mapsto 3\frac{z+1}{z-1} = \frac{3z+3}{1z-1}$, takes

$$\begin{aligned}
1 = [1:1] &\mapsto [6:0] = [1:0] &&= 6\\
2 = [2:1] &\mapsto [9:1] = [4:1] = [1:1] &&= 4\\
3 = [3:1] &\mapsto [12:2] = [2:2] = [1:1] &&= 1\\
4 = [4:1] &\mapsto [15:3] = [0:3] = [0:1] &&= 5\\
5 = [0:1] &\mapsto [3:-1] = [3:4] = [2:1] &&= 2\\
6 = [1:0] &\mapsto [3:1] &&= 3
\end{aligned}$$

So, as a cycle, it is (163)(245).

So, we are looking at a subset of S_6 generated by (14)(23), (23)(56), and (163)(245). Because (163)(245) = (25)(24)(13)(16), every generator has an even number of transpositions in its cycle decomposition, meaning this is a subgroup of A_6. In fact, it will turn out to be the "twisted" embedding of A_4 in A_6.

Let $a = (14)(23), b = (23)(56)$, and $c = (163)(245)$, and let $G = \langle a, b, c\rangle$ We will see in the next problem that a and b generate the Klein 4-group, so G contains $\mathbb{Z}_2 \times \mathbb{Z}_2$ as a subgroup. Also, c has order 3, so $\langle c\rangle = \mathbb{Z}_3$; therefore G contains $\mathbb{Z}_3$ as well.

Now, we assume for the moment that G is of order 12.In classifying the groups of order 12 in the last problem, we will see that there are three groups of order 12 which contain the Klein 4-group. One is $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$, which is abelian; one is D_6, which contains exactly three elements of order 3, and one is A_4. After making some calculations, we will be able to rule two of these out.

$$\begin{aligned}
ab = ba = (14)(23)(23)(56) &= (14)(56)\\
ac = (14)(23)(163)(245) &= (162)(345)\\
bc = (23)(56)(163)(245) &= (153)(246)\\
ca = (163)(245)(14)(23) &= (152)(346)
\end{aligned}$$

By the existence of at least 4 elements of order 3, we see that $G \neq D_6$, and by the fact that $ac \neq ca$, we see that $G \neq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$. So, that leaves A_4 - if G is of order 12, then it is isomorphic to A_4.

Lemma 1. If $G = \langle A, B\rangle$ is generated by the subgroups A and B, the two subgroups have trivial intersection, and A is normal in G, then $G = A \rtimes B$, i.e. G is the semidirect product of A with B, along some homomorphism $B \to \mathrm{Aut}(A)$.

Proof. It is a theorem in Dummit & Foote that a group G is the semidirect product of A and B if and only if $G = AB$, A is normal in G, and $A \cap B = \{e\}$. So, we only need to see that $\langle A, B\rangle = AB$.

It is clear that $AB \subset \langle A, B\rangle$, so we need to see that $\langle A, B\rangle \subset AB$. Because $\langle A, B\rangle$ is the smallest subgroup of G containing A and B, it will suffice to show that AB is a subgroup of G containing A and B.

First, we see that $A \subset AB$, as if $a \in A$ then $a = ae \in AB$, and similarly if $b \in B$ then $b = eb \in AB$.

Next, we see that AB is a subgroup. If $a_1b_1, a_2b_2 \in AB$, then $b_1a_2 = a'b'$ for some $a' \in A$ and $b' \in B$, by the fact that A is normal, and therefore $BA = AB$. So, the element $(a_1b_1)(a_2b_2) \in AB$ as well, which we can see by calculation:

$$\begin{aligned}(a_1b_1)(a_2b_2) &= a_1(b_1a_2)(b_2 \\ &= a_1(a'b')b_2 \\ &= (a_1a')(b'b_2) \in AB\end{aligned}$$

So AB is closed under multiplication. Also, if $x = ab \in AB$, then $b^{-1}a^{-1} = a'b'$ for some $a' \in A$, $b' \in B$, and so

$$\begin{aligned}x^{-1} &= (ab)^{-1} \\ &= b^{-1}a^{-1} \\ &= a'b' \in AB\end{aligned}$$

So AB is also closed under inverses, and is a subgroup. Since $A \cup B \subset AB$ and $\langle A, B\rangle$ is the smallest subgroup containing $A \cup B$, we see that $\langle A, B\rangle \subset AB$.

Therefore, $G = AB$, and the criteria for the semidirect product tells us that $G = A \rtimes B$, with the product defined over some homomorphism $B \to \mathrm{Aut}(A)$. □

Now, since we have

$$G = \langle a, b, c\rangle = \langle\langle a, b\rangle, \langle c\rangle\rangle,$$

we need only see that $\langle a, b\rangle$ is normal in $\langle a, b, c\rangle$.

Lemma 2. Let A and B be finite sets. The group $\langle A\rangle$ generated by A is normal in $\langle A, B\rangle$ if and only if $bab^{-1} \in \langle A\rangle$ for all $a \in \langle A\rangle$, $b \in \langle B\rangle$.

Proof. Assume that $bab^{-1} \in \langle A\rangle$ for all $a \in \langle A\rangle$ and $b \in \langle B\rangle$. Let $a' \in \langle A\rangle$ and $x \in \langle A, B\rangle$; we wish to show that $xax^{-1} \in \langle A\rangle$.

Let $x = \prod_{1 \le i \le n} x_i^{k_i}$, where $x_i \in A \cup B$ and $k_i \in \mathbb{Z}$. We will induct on n, the number of terms in the product.

First, we see that it holds for $n = 1$, as either $x_1 \in A$, in which case $xa'x^{-1} \in \langle A\rangle$ trivially, or $x_1 \in B$, in which case $x \in \langle B\rangle$ and $xa'x^{-1} \in \langle A\rangle$ by assumption.

Now, assume that $xa'x^{-1} \in \langle A \rangle$ for all $x = \prod_{1 \leq i \leq (n-1)} x_i^{k_i}$, where $x_i \in A \cup B$, and let $x' = \prod_{1 \leq i \leq n} x_i^{k_i}$. Then

$$\begin{aligned} x'a'x'^{-1} &= \left(\prod_{1 \leq i \leq n} x_i^{k_i} \right) a' \left(\prod_{1 \leq i \leq n} x_i^{k_i} \right)^{-1} \\ &= x_1^{k_1} \left(\prod_{1 \leq i \leq n-1} x_{i+1}^{k_{i+1}} \right) a' \left(\prod_{1 \leq i \leq (n-1)} x_{i+1}^{k_{i+1}} \right)^{-1} x_1^{k_1}. \end{aligned}$$

By assumption, the inner term $\left(\prod_{1 \leq i \leq n-1} x_{i+1}^{k_{i+1}} \right) a' \left(\prod_{1 \leq i \leq (n-1)} x_{i+1}^{k_{i+1}} \right)^{-1}$ is in $\langle A \rangle$, so it is equal to a_1, for some $a_1 \in \langle A \rangle$. So,

$$x'a'x^{-1} = x_1^{k_1} a x_1^{-k_1}.$$

Either $x_1 \in \langle A \rangle$, so that $x_1^{k_1} \in \langle A \rangle$ and $x'a'x'^{-1} \in \langle A \rangle$ trivially, or $x_1 \in \langle B \rangle$, so that $x_1^{k_1} \in \langle B \rangle$, and $x'a'x'^{-1} \in \langle A \rangle$ by assumption.

So, by induction, to check that $\langle A \rangle$ is normal in $\langle A, B \rangle$, it suffices to check that each element in $\langle B \rangle$ normalizes A. □

By this lemma, to see that $\langle a, b \rangle$ is normal in $\langle a, b, c \rangle$, we need only see that $xyx^{-1} \in \langle a, b \rangle$ for all $y \in \langle a, b \rangle$ and $x \in \langle c \rangle$. There are only 3 nontrivial elements in $\langle a, b \rangle$, and 2 nontrivial elements in c, so we can check these directly:

$$\begin{aligned} cac^{-1} &= (163)(245)(14)(23)(136)(254) = (14)(56) = ab \\ cbc^{-1} &= (163)(245)(23)(56)(136)(254) = (14)(23) = a \\ cabc^{-1} &= (163)(245)(14)(56)(136)(254) = (23)(56) = b \\ c^{-1}ac &= (136)(254)(14)(23)(163)(245) = (23)(56) = b \\ c^{-1}bc &= (136)(254)(23)(56)(163)(245) = (14)(56) = ab \\ c^{-1}abc &= (136)(254)(14)(56)(163)(245) = (14)(23) = a \end{aligned}$$

So, $\langle a, b \rangle$ is normal in $G = \langle a, b, c \rangle$. We have seen that this suffices to give $G = \langle a, b, \rangle \rtimes \langle c \rangle$; which in particular gives $|G| = |\langle a, b \rangle| \cdot |c| = 4 \cdot 3 = 12$. Finally, we have seen that if $|G| = 12$, then $G \simeq A_4$. So, G is the alternating group on 4 elements. □

Prove that the first two substitutions generate the noncyclic group of order 4.

Proof. The noncyclic group of order 4 is the group $\mathbb{Z}_2 \times \mathbb{Z}_2$, with elements $e = (0, 0)$, $(1, 0)$, $(0, 1)$, and $(1, 1)$. Since a and b both have order 2, the groups $\langle a \rangle$ and $\langle b \rangle$ are both of order 2, meaning they must be $\mathbb{Z}_2$. Since $ab = ba$, both groups must lie in the center of G; in particular, both are normal, and we can write $|G| = \langle a \rangle \rtimes \langle b \rangle$, for some homomorphism $\langle b \rangle \to \mathrm{Aut}(\langle a \rangle)$. Since both groups are isomorphic to $\mathbb{Z}_2$, this is the same as a homomorphism $\mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_2)$. Because $\mathrm{Aut}(\mathbb{Z}_2)$ is trivial, this homomorphism must be trivial, and so in fact $G = \langle a \rangle \times \langle b \rangle \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. □

Prove that the third and either of the first two substitutions generate the group of order 12 mentioned above.

Proof. Since $\langle a, c\rangle \leq \langle a, b, c\rangle$, and similarly $\langle b, c\rangle \leq \langle a, b, c\rangle$, to see that $\langle a, c\rangle = \langle b, c\rangle = \langle a, b, c\rangle$, it suffices to show that $a \in \langle b, c\rangle$, and $b \in \langle a, c\rangle$.

Both of these follow from the conjugacy calculations carried out above. Because $cbc^{-1} = a$, we see that $a \in \langle b, c\rangle$, and because $c^{-1}ac = b$, it is true that $b \in \langle a, c\rangle$. So, either a and c or b and c generate the whole group A_4. □

Problem 2. Prove that the tranformations of the form $w = \frac{az+b}{cz+d} (\text{mod } 3)$, with a, b, c, d being integers such that $ad - bc = 1 (\text{mod } 3)$, constitute a group of order 12, which has the same number of elements of each order as the group in Exercise 1.

Proof. Incomplete, Not for credit Much of the background here I gained from Wikipedia's article on the projective linear groups over finite fields.

We show that these transformations form a faithful action of the group $\mathrm{PSL}_2(\mathbb{Z}_3)$ on the projective space $\mathbb{P}^1(\mathbb{Z}_3)$, and then show that this group has order 12, and find the number of elements in the group of each order.

The projective space $\mathbb{P}^1(\mathbb{Z}_3)$ is defined as $(\mathbb{Z}_3^2)/\sim$, where $(x, y) \sim (z, w)$ whenever there is some $q \in Z_3$ such that $qx \equiv z$ and $qy \equiv w$. There are 4 points in this projective space, which we map to the numbers 1 through 4 to work with cycle notation:

$$\begin{aligned}[1:1] &= 1\\ [1:2] &= 2\\ [1:0] &= 3\\ [0:1] &= 4\end{aligned}$$

The tranformations $w = \frac{az+b}{cz+d}$ take a point $[x : y]$ to the point $[ax + by : cx + dy]$.We see that any pair of points in $\mathbb{P}^1(\mathbb{Z}_3)$ can be mapped to any other two points by one of these transformations: Say we wish to take $x_1 \mapsto x_2$ and $y_1 \mapsto y_2$, where $x_1 \neq y_1$ and $x_2 \neq y_2$. Let

$$\begin{aligned}x_1 &= [x_1^1 : x_1^2]\\ x_2 &= [x_2^1] : x_2^2]\\ y_1 &= [y_1^1 : y_1^2]\\ y_2 &= [y_2^1 : y_2^2]\end{aligned}$$

Finding a single $w = \frac{az+b}{cz+d}$ which will take x_1 to x_2 and y_1 to y_2 is equivalent to choosing a, b, c, d such that

$$\begin{aligned}x_2^1 &= ax_1^1 + bx_1^2\\ x_2^2 &= cx_1^1 + dx_1^2\\ y_2^1 &= ay_1^1 + by_1^2\\ y_2^2 &= cy_1^1 + dy_1^2\\ ad - bc &= 1\end{aligned}$$

Solving for a, b, c, d, we get

$$a = \frac{x_1^2 y_2^1 - x_2^1 y_1^2}{x_1^2 y_1^1 - y_1^2 x_1^1}$$
$$b = \frac{x_1^1 y_2^1 - y_1^1 x_2^1}{x_1^1 y_1^2 - y_1^1 x_1^2}$$
$$c = \frac{x_1^2 y_2^2 - y_1^2 x_2^2}{x_1^2 y_1^1 - y_1^2 x_1^1}$$
$$d = \frac{x_1^1 y_2^2 - y_1^1 x_2^2}{x_1^1 y_1^2 - y_1^1 x_1^2}$$

The choice $x_1^1/x_1^2 \neq y_1^1/y_1^2$ ensures that none of the denominators here are 0.

It is not immediately obvious that the condition $ad - bc$ is satisfied, but it is. □

Are the two groups isomorphic?

Proof. Yes, they are both the alternating group A_4. □

Problem 3. By means of Sylow's theorem prove that every group of order 20 contains only one subgroup of order 5, and either one or five subgroups of order 4.

Proof. By Sylow, every group G of order $20 = 5 \cdot 2^2$ contains at least one Sylow subgroup of order 5, and at least one of order 4. Further, the number n_5 of order-5 subgroups is equal to 1 modulo 5. The options are $1, 6, 11, 16, \ldots$. Finally, $n_5 = [G : N_G(P)]$, where P is any Sylow 5-subgroup. Because $[G : N_G(P)] = |G|/|N_G(P)|$, and the order $|N_G(P)|$ must divide the order of G, we see that n_5 must divide the order of G as well. The only number which divides 20 and is equal to 1 modulo 5 is 1, so there must be exactly one Sylow 5-subgroup. Every subgroup of order 5 must be Sylow, so there is only one subgroup with this order.

In the case of the Sylow subgroup of order $2^2 = 4$, we see that there must be at least one, and that the number n_2 of these subgroups must be $1, 5, 9, 13, \ldots$. Also, n_2 must divide the order of G. There are now 2 options: 1 and 5. So, there may be one subgroup of order 4, or there may be five of them. □

Problem 4. Prove that a group of order 15 is cyclic.

Proof. Let G be the group of order 15. By Sylow's theorems, there must be at least one Sylow 5-subgroup, and at least one Sylow 3-subgroup. Also, the number n_5 of 5-subgroups must be 1, because 6 and 11 do not divide 15; similarly, the number n_3 of 3-subgroups must be 1, because 4, 7, 10 and 14 do not divide 15.

Let H_3 and H_5 be the Sylow 3-and 5-subgroup, respectively. Because n_5 and n_3 are the index of the normalizers of the Sylow 5-subgroup and Sylow 3-subgroup, respectively, we see that the normalizer of each is the whole group, i.e. that both Sylow subgroups are normal.

Further, the only groups of orders 3 and 5 are $\mathbb{Z}_3$ and $\mathbb{Z}_5$, respectively, so the two Sylow subgroups are cyclic. Also, since every element in $\mathbb{Z}_3$ except the identity has order 3, and every element of $\mathbb{Z}_5$ except the identity has order 5, the two Sylow groups have trivial intersection. Since $|H_3 H_5| = |H_3| \cdot |H_5|/|H_3 \cap H_5| = 3 \cdot 5/1 = 15$, it must be true that

$H_3H_5 = G$. Further, if two groups have trivial intersection and are normal, $H_3H_5 = H_3 \times H_5$. Therefore, we see that every group of order 15 is isomorphic to the direct product $\mathbb{Z}_3 \times \mathbb{Z}_5$. Specifically, because $\mathbb{Z}_{15}$ is of order 15, we see both that $\mathbb{Z}_{15} \simeq \mathbb{Z}_3 \times \mathbb{Z}_5$, and that every group of order 15 is isomorphic to $\mathbb{Z}_{15}$. □

Problem 5. A group of order pq, with p and q being distinct primes and $p > q$, is cyclic, unless q divides $p-1$, in which case there are exactly two groups of order pq. Describe these two groups.

Proof. Let G be a group of order pq, with $p > q$. As in the previous proof, there must be Sylow subgroups of order p and q in G, and the numbers of the Sylow subgroups have very few possibilities. Because $n_p \,|\, q$, it must be either 1 or q. And, because $n_p = 1 (\text{mod } p)$, and $q < p$, it cannot be equal to q, therefore $n_p = 1$.

In the case of n_q, there are two possibilities. In any case, $n_q \mid p$, so $n_q = 1$ or $n_q = p$. Also, $n_q = 1 (\text{mod } q)$. First, taking the hypothesis that $q \nmid (p-1)$, we see that $p \not\equiv 1 (\text{mod } q$, and so it must be true that $n_q = 1$. If both n_q and n_p are 1, then, as in the last problem, the two Sylow subgroups are normal, and have trivial intersection; thus they are cyclic, and $G \simeq \mathbb{Z}_p \times Z_q \simeq Z_{pq}$.

If $q \mid (p-1)$, then $p \equiv 1 (\text{mod } q)$, and the theorems of Sylow allow for two possibilities: $n_p = n_q = 1$, and $G = \mathbb{Z}_{pq}$, or $n_p = 1$ and $n_q = p$. In this case, G can still be reconstructed from the two Sylow groups $\mathbb{Z}_p$ and $\mathbb{Z}_q$ as a semidirect product. □

Problem 6. Show that there are $(p-2)!$ subgroups of order p in the symmetric group on p letters, p being a prime. Conclude that $(p-2)! = 1 (\text{mod } p)$.

Proof. First, we see that every element of order p in S_p is of the form $(1, a_1, \ldots, a_p)$, where $a_1, \ldots, a_p$ is a permutation of $2, \ldots, p$. The cyclic group $\langle (1, a_1, \ldots, a_p) \rangle$ is of order p, and so every element aside from the identity also has order p. Every subgroup of order p must be cyclic, so it is of this form, and finally any two non-equal subgroups of order p must have trivial intersection.

So, every permutation of $1, \ldots, p$ determines an element of order p, and each group of order p contains $p-1$ unique elements of order p. Since there are $(p-1)!$ permutations of $1, \ldots, p$, the total number of subgroups of order p in S_p is

$$\frac{(p-1)!}{p-1} = (p-2)!$$

□

Problem 6.5. The symmetric group of degree n does not contain any subgroup of index m, if m is greater than 2 but less than the largest prime factor on n.

Proof. The following theorem is from Dummit & Foote:

If $H \subset G$ and $[G : H] = \ell$, then there exists some homomorphism $\varphi : G \to S_l$ such that $\text{Ker}(\varphi) \subset H$.

Now, let H be a subset of S_n with index m. There must be some $\varphi : S_n \to S_m$ with $\text{Ker}(\varphi) \subset H$. However, a kernel is a normal subgroup, and there are very few normal subgroups in S_n; only $1, A_n$, and S_n itself.

If $\mathrm{Ker}(\varphi) = 1$, then φ is an injective homomorphism $S_n \to S_m$, implying that $m \geq n$. If $\mathrm{Ker}(\varphi) = A_n$, then either $H = A_n$, meaning it has index 2, or $H = S_n$, meaning it has index 1. If $\mathrm{Ker}(\varphi) = S_n$, then $H = S_n$. In any case, either $[S_n : H] \leq 2$ or $[S_n : H] \geq n$, meaning in particular that the index of H is greater than the largest prime factor of n. □

Problem 9. If a group contains a subgroup of index 2 then this subgroup is normal.

Proof. We use the fact that the index of a subgroup $H \leq G$ is the number of cosets of H, and that the condition of normality of H is equivalent to saying that $xH = Hx$ for all $x \in G$.

Assume that H is of index 2. Then there are only two cosets of H: the subgroup H itself, and the complement of H in G: $G \backslash H$. Let $x \in G$. Then there are two possibilities, either $x \in H$, in which case $xH = H = Hx$, or else $x \notin H$, in which case $xH = G \backslash H = Hx$. So, $xH = Hx$ for all $x \in G$, meaning that H is normal. □

Problem 12. Determine the number of elements of each order in each of the four Abelian groups of order 100.

Proof. First, there is the cyclic group $\mathbb{Z}_{100} = \mathbb{Z}_{25} \times \mathbb{Z}_4$:

$$\begin{aligned}
\text{Elements of order } 1 &: 1 \ (0) \\
2 &: 1 \ (50) \\
4 &: 2 \ (25, 75) \\
5 &: 4 \ (20, 40, 60, 80) \\
10 &: 4 \ (10, 30, 70, 90) \\
25 &: 20 \ (4, 8, \ldots, 96) \\
50 &: 21 \ (2, 6, \ldots, 98) \\
100 &: 48 \ (1, 3, 7, \ldots, 99)
\end{aligned}$$

In general, in a cyclic group, the number of elements of order d, $n(d)$, is equal to $|G|/d - \sum_{k|d} n(k)$.

Now, we have $\mathbb{Z}_25 \times \mathbb{Z}_2 \times \mathbb{Z}_2$: Each element can be represented (a, b, c), where $a \in \mathbb{Z}_25$ and $b, c \in \mathbb{Z}_2$, and the order of an element (a, b, c) is equal to the least common multiple of the orders of the three numbers a, b, and c. We can count the number of □

Problem 13. A group of order p^2q must be Abelian when q is a prime number which is less than the prime number p and does not divide $p^2 - 1$.

Proof. Let G be a group of order p^2q. By the theorems of Sylow, there myst be a q-sylow subgroup C_q with order q, meaning $C_q \simeq \mathbb{Z}_q$. The number of q-sylow subgroups, n_q, must divide p^2, and must be equal to 1 mod q. The only numbers which divide p^2 are 1, p, and p^2.

If $n_q = p^2$, then it must be true that $p^2 \cong 1 (\mathrm{mod}\ q)$; but then $q \mid p^2 - 1$, contradicting the assumption that $q \nmid p^2 - 1$.

If $n_q = p$, then it must be true that $p \cong 1 (\mathrm{mod}\ q)$. But then $q \mid p - 1$, contradicting the assumption that $q \nmid p^2 - 1 = (p - 1)(p + 1)$.

Therefore, it must be true that $n_q = 1$, and the q-subgroup is normal. Thus it must be that $G = \mathbb{Z}_q \times C_p$, where C_p is the Sylow subgroup of order p^2. There are only two groups of order p^2: $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p$.

In either case, we see that the homomorphism $C_p \to \mathrm{Aut}(\mathbb{Z}_q)$ defining the semidirect product must be trivial. The automormphism group of a cyclic group is itself cyclic: $\mathrm{Aut}(\mathbb{Z}_q) \simeq \mathbb{Z}_{q-1}$. Since every element of C_p has order 1, p or p^2, the image of every element under the homomorphism $C_p \to Z_{q-1}$ must have order 1, since $p > q-1$ and so $p \nmid q-1$. A homomorphism under which every element has order 1 is trivial, so the semidirect product $\mathbb{Z}_q \rtimes C_p$ must be a direct product.

In either case, $G \simeq \mathbb{Z}_q \times \mathbb{Z}_{p^2}$ or $G \simeq \mathbb{Z}_q \times \mathbb{Z}_p \times \mathbb{Z}_p$, G is abelian. □

Problem 14. Show that a group in which all elements besides 1 are of order 2 is Abelian.

Proof. Let G be a group such that, for all $g \in G$, $g^2 = e$. Then for any two $x, y \in G$,

$$\begin{aligned} e &= (xy)^2 \\ &= xyxy \end{aligned}$$

So, $xyxy = e$. Multiplying on the left by x, we get $x = x^2yxy = yxy$, and on the right by y, we get $xy = yxy^2 = yx$. So $xy = yx$ for all $x, y \in G$, showing that it is Abelian. □

Problem 16. Up to isomorphism, find all groups of order 15 or less.

Proof. For all groups of non-composite order, there is one option: the cyclic group. The first composite order is 4. Every group of order 4 must be abelian, because it is either $\mathbb{Z}_4$, or every element is of order 2, which we have seen forces it to be abelian. The only other abelian group of order 4 is $\mathbb{Z}_2 \times \mathbb{Z}_2 = D_2$, the Klein 4-group.

The next composite order is 6. Since $6 = 3 \cdot 2$, and $2 \mid (3-1)$, we have seen in exercise 5 that there is only one noncyclic group with this order. Since $D_3 = S_3$ has $2! = 6$ elements and is nonabelian, any noncyclic group of order 6 must be D_3.

Now, let G be a group of order $8 = 2^3$. We have seen that the groups $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ are the only abelian groups of order 8. There are also two nonabelian options: the dihedral group D_4 has 8 elements and is nonabelian, so it is distinct from these options; and the Quaternion group Q also has order 8, and is nonabelian.

(The following proof is from proofwiki): These groups exhaust the groups of order 8. To see this, assume that G is nonabelian. All elements of G are of order 2, 4, or 8. If there is an element of order 8, it must generate the whole group, and then G would be cyclic and therefore abelian. On the other hand, if every element was of order 2, then G would be abelian. So, there must be an element of order 4.

Let a be an element of G of order 4, and let A be the subgroup generated by a. G is partitioned into two cosets, A and $G - A$. Find any element $b \in G - A$, then $\{a, b\}$ generates the group. Therefore, all nonabelian groups of order 8 are determined by presentations on two generators. We will see there are only two possibilities for these presentations.

Let $x = bab^{-1}$. Because $x \in bAb^{-1}$, and A is normal, $x \in A$, i.e. $x \in \{e, a, a^2, a^3\}$ If $x = a$, then G is abelian, which we know it is not. If $x = e$ or $x = a^2$, then it has order 0 or

2, while a has order 4. Since conjugates have equal order, this is also a contradiction. So, $bab^{-1} = a^3$.

Since the order of b must be 2 or 4, we see that there are two possibilities for G:

$$G \simeq \langle a, b \mid bab^{-1} = a^3, a^4 = b^2 = e \rangle \simeq D_2$$
$$G \simeq \langle a, b \mid bab^{-1} = a^3,\ a^4 = b^4 = e \rangle \simeq Q$$

Next, let G be a subgroup of order 9. We see that there are two abelian structures on G: $\mathbb{Z}_9$ and $\mathbb{Z}_3 \times \mathbb{Z}_3$. There are no nonabelian groups of order 9, as any group of order p^2, where p is a prime, is abelian.

Now, let G be a subgroup of order 10. Since $|G| = 5 \cdot 2$, and $2 \mid (5-1)$, by problem 5 there are exactly 2 group structures G can have. One is the cyclic group, and the other must be the dihedral group D_5, as it is nonabelian.

Next, we look at subgroups of order 12. There will turn out to be five groups with this order, one of which we have already looked at in this homework.

First, there are two abelian groups. There are two ways to decompose 12 which give distinct abelian groups: $\mathbb{Z}_4 \times \mathbb{Z}_3 \simeq \mathbb{Z}_{12}$, adn $\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, which is isomorphic to$\mathbb{Z}_3 \times D_2$.

Next, assume G is nonabelian. It has Sylow subgroups of order 3 and 4, respectively; we will see that at least one of these subgroups is normal. Let n_3 be the number of Sylow 3-subgroups. Since $n_3 = 1 (\text{mod } 3)$ and $n_3 \mid 4$, we see that $n_3 = 1$ or $n_3 = 4$. If $n_3 = 1$, the 3-subgroup is normal, and we are done. If, on the other hand, $n_3 = 4$, let Q_1, Q_2, Q_3, Q_4 be the sylow 3-subgroups. Since these groups are cyclic and nonequal, they must have trivial intersection; so, their union $Q = \cup_i Q_i$ has $3 + 2 \cdot 3 = 9$ elements. Every nonidenity element of a Sylow 2-subgroup cannot be in this union, so it must be in the complement, which has $12 - 9 = 3$ elements. Since this is only enough elements to make one Sylow 2-subgroup, it must be unique, and therefore normal.

There are thus three possibilities: either the 3-subgroup is normal, the 2-subgroup is, or they both are. If both Sylow subgroups are normal, the group must be abelian, which is a case we have dealt with.

So, assume first that the Sylow 2-subgroup, which we call C_2, is normal and the 3-subgroup C_3 is not. In this case, G must be a semidirect product $C_2 \rtimes C_3$, and it must be a nontrivial semidirect product, as a direct product would make G abelian. This product is equivalent of a choice of a nontrivial homomorphism $C_3 \to \text{Aut}(C_2)$. The choice of this homomorphism depends on the structures of the Sylow groups.

It is certainly true that $C_3 \simeq \mathbb{Z}_3$. There are two options for our order-4 subgroup. In the case that $C_2 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, the Klein 4-subgroup, we see that the automorphism group of C_2 is S_3, as any permutation of the three nonidentity elements of $\mathbb{Z}_2 \times \mathbb{Z}_2$ gives a group automorphism. Thus any nontrivial homomorphism $\mathbb{Z}_3 \to S_3$ gives a semidirect product $C_2 \rtimes C_3$.

In fact, there are two homomorphisms $\mathbb{Z}_3 \to S_3$, taking 1 to either of the 3-cycles in S_3. Both of these give isomorphic embeddings of Z_3 as A_3, so they give isomorphic groups $C_2 \rtimes C_3$. We also know from exercise 2 that the alternating group A_4 is a nonabelian order-12 group with a normal subgroup of order 4; since there is only one such group, it must be the one we have just constructed.

If $C_2 \simeq \mathbb{Z}_4$, then $\mathrm{Aut}(C_2) \simeq \mathbb{Z}_2$, and there is no nontrivial homomorphism $\mathbb{Z}_3 \to \mathbb{Z}_2$. So, there is only one order-12 group where the Sylow 2-subgroup is normal, and the Sylow 3-subgroup is not.

Now, we have the case when the 3-subgroup is normal and the 2-subgroup is not. Again, because one subgroup is normal and their product generates the whole group, G must be a semidirect product $C_3 \rtimes C_2$. So, we look for nontrivial homomorphisms $C_2 \to \mathrm{Aut}(C_3)$.

Because $C_3 \simeq \mathbb{Z}_3$, the automorphism group is also cyclic: $\mathrm{Aut}(C_3) \simeq \mathbb{Z}_2$. In the case when $C_2 \simeq \mathbb{Z}_4$, there is one nontrivial homomorphism $C_2 \to \mathrm{Aut}(C_3)$, given by the map $\mathbb{Z}_4 \to \mathbb{Z}_2$ with kernel $\{0, 2\}$. This gives a nonabelian order-12 group with a cyclic 2-Sylow group and a normal, cyclic 3-Sylow group, where the 2-group acts as transpositions on the nonidentity elements of the 3-group. In fact, this is the dicylic group $\mathrm{Dic}(12)$.

Finally, we have the case where $C_3 \simeq \mathbb{Z}_3$ and is normal, and $C_2 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ and is not. A semidirect product $C_3 \rtimes C_2$ is determined by a homomorphism $\mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2$. Here, there are actually three nontrivial homomorphisms, with kernels $\{e, (1,1)\}$, $\{e, (1,0)\}$, and $\{e, (0,1)\}$, respectively. However, there is only one homomorphism up to isomorphism, as there are automorphisms of $\mathbb{Z}_2 \times \mathbb{Z}_2$ taking each of the kernels to either of the others. So, there is a unique nonabelian 12-group with normal 3-subgroup and non-normal 2-subgroup isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. In fact, this group is isomorphic to D_6, the dicyclic group of order 12. We have determined all groups of order 12.

Next, let G have order 14. Because $14 = 7 \cdot 2$, and $2 \mid (7-1)$, there are two groups; the cyclic group, and a nonabelian group, which must be the dihedral group D_7.

Finally, let G have order 15. Because $15 = 5 \cdot 3$, and $3 \nmid (5-1)$, there is a unique group of order 15, the cyclic group. We have thus determined the groups of every order up to 15:

$$
\begin{aligned}
\text{Groups of order } 1 &: 1 \\
2 &: \mathbb{Z}_2 \\
3 &: \mathbb{Z}_3 \\
4 &: \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2 \\
5 &: \mathbb{Z}_5 \\
6 &: \mathbb{Z}_6, D_3 \\
7 &: \mathbb{Z}_7 \\
8 &: \mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, D_4, Q \\
9 &: \mathbb{Z}_9, \mathbb{Z}_3 \times \mathbb{Z}_3 \\
10 &: \mathbb{Z}_{10}, D_5 \\
11 &: \mathbb{Z}_{11} \\
12 &: \mathbb{Z}_{12}, \mathbb{Z}6 \times \mathbb{Z}_2, A_4, D_6, \mathrm{Dic}(12) \\
13 &: \mathbb{Z}_{13} \\
14 &: \mathbb{Z}14, D_7 \\
15 &: \mathbb{Z}_{15}
\end{aligned}
$$

□

2 Corrections

First, the internal definition of the subgroup generated by a subset $S \subset G$: the group $\langle S \rangle$ is the subset of G that consists of all elements of the form

$$x = \prod_{1 \leq i \leq n} s_i^{k_i},$$

where $s_i \in S$ and $k_i \in \mathbb{Z}$, along with the identity element. This subset is closed under multiplication and inverses, so it is a subgroup; also, it contains S, and every subgroup of G containing S contains the subgroup $\langle S \rangle$, so it satisfies the universal-property description of $\langle S \rangle$.

I claimed in problem 19 that if $H \leq G$ and $K \leq G$ have coprime order, then $|\langle H, K \rangle| = |H| \cdot |K|$, which is false. For example, let $G = \langle a, b \mid a^2 = b^2 = e \rangle$. Then the groups $\langle a \rangle$ and $\langle b \rangle$ have order 2, but the group $G = \langle a, b \rangle$ has infinite order.