Problem 10 (Ch. 1.8)

Let G be a finite group, A and B non-vacuous subsets of G. Show that $G = AB$ if $|A| + |B| > |G|$.

Solution. Since inverses are determined uniquely in groups, there is a 1-1 correspondance between A and A^{-1}, so $|A| = |A^{-1}|$. Furthermore, for any $g \in G$, note that $|A^{-1}g| = |A^{-1}| = |A|$, since cosets have the same order as the original set. But then $|A^{-1}g| + |B| > |G|$, and since $A^{-1}g$ and B, by definition are subgroups of G, they have a nonempty intersect (otherwise if the intersect were empty, there would be $|A^{-1}g| + |B|$ elements in $|G|$, but that's a contradiction). Thus there exists some $a \in A$ and $b \in B$ so that $a^{-1}g = b$, or $g = ab$. But this is true for all $g \in G$, thus $G \subseteq AB$. But $AB \subseteq G$ since $a, b \in G$ for any $a \in A$ and $b \in B$, and $ab \in G$ since G is a group so its closed. Therefore, $AB = G$.

Problem 11 (Ch. 1.8)

*Let G be a group of order $2k$ where k is odd. Show that G contains a subgroup of index 2. (*Hint: *Consider the permutation group G_L of left translations and use exercise 13, p.36.*

Solution. Recall from previous chapters that G_L is a subgroup of S_{2k}, and $G_L \cong G$. Thus, it suffices to show that there is a subgroup of index 2 inside G_L.

First, since G is of even order, by exercise 13, there exists some $a \in G$ such that $a \neq 1$ and $a^2 = 1$, so it is of order 2. Consider the bijective map $a_L \in G_L$ given by $a_L \colon g \mapsto ag$ for all elements $g \in G$ (this is clearly a bijective map, since there is a well-defined inverse on G: $a_L^{-1} \colon g \mapsto a^{-1}g = ag$, so $a_L(a_L^{-1}(g)) = (a_L^{-1} \circ a_L)(g) = g$). Note $a_L = a_L^{-1}$. Thus, a_L is just swapping two elements, thus we can represent it as composition of transpositions, ie. if we number our elements in G correctly, we have $a_L = (12)(34) \cdots (2k-1\ 2k)$. Of note is that, since k is odd, a_L is an odd permutation.

Now, define $H_L = A_{2k} \cap G_L$ where A_{2k} is the group of even permutations of S_{2k}. Note that for any odd permutation $\alpha \in G_L$, we have $\alpha a_L \in H_L$, so $\alpha \in H_L \alpha_L^{-1} = H_L \alpha_L$. Thus, H_L are all the even permutations in G_L, and since α was arbitrary, $H_L a_l$ are all the odd permutations of G_L, thus $G_L = H_L \sqcup H_L a_L$. But then H_L is a subgroup of G_L with index 2, and since $G_L \cong G$, we have that there exists a subgruop of G with index 2.

Problem 2 (Ch. 1.9)

Let G be the set of triples of integers (k, l, m) and define $(k_1, l_1, m_1)(k_2, l_2, m_2) = (k_1 + k_2 + l_1 m_2, l_1 + l_2, m_1 + m_2)$. Verify that this defines a group with unit $(0,0,0)$. Show that $C = \{(k, 0, 0) \mid k \in \mathbb{Z}\}$ is a normal subgroup and that $G/C \cong$ the group $\mathbb{Z}^{(2)} = \{(l, m) \mid l, m \in \mathbb{Z}\}$ with the usual addition as composition.

Solution. Note that G is closed, since if $k_1, k_2, l_1, l_2, m_1, m_2 \in \mathbb{Z}$, then $k_1 + k_2 + l_1 m_2, l_1 + l_2, m_1 + m_2 \in \mathbb{Z}$, since $\mathbb{Z}$ is closed under addition and multiplication, so $(k_1, l_1, m_1)(k_2, l_2, m_2) \in G$. We have associativity:

$$\begin{aligned}
((k_1, l_1, m_1)(k_2, l_2, m_2))(k_3, l_3, m_3) &= (k_1 + k_2 + l_1 m_2, l_1 + l_2, m_1 + m_2)(k_3, l_3, m_3) \\
&= (k_1 + k_2 + l_1 m_2 + k_3 + (l_1 + l_2) m_3, l_1 + l_2 + l_3, m_1 + m_2 + m_3) \\
&= (k_1 + k_2 + k_3 + l_2 m_3 + l_1(m_2 + m_3), l_1 + l_2 + l_3, m_1 + m_2 + m_3) \\
&= (k_1, l_1, m_1)(k_2 + k_3 + l_2 m_3, l_2 + l_3, m_2 + m_3) \\
&= (k_1, l_1, m_1)((k_2, l_2, m_2)(k_3, l_3, m_3))
\end{aligned}$$

Furthermore, $(0,0,0)$ is the identity: $(k, l, m)(0,0,0) = (k + 0 + 0, l + 0, m + 0) = (k, l, m)$ and $(0,0,0)(k, l, m) = (0 + k + 0, 0 + l, 0 + m) = (k, l, m)$. Finally, we have inverses: we give that the inverse of $(k, l, m) \in G$ is $(-k + lm, -l, -m)$. We can verify: $(k, l, m)(-k + lm, -l, -m) = (-k + lm, -l, -m)(k, l, m) = (0, 0, 0)$.

We show that C is in the kernel of some homomorphism ϕ, and so by the fundamental theorem of homomorphisms, C is normal. Furthermore, for the sake of efficiency, we will construct our homomorphism from G to $\mathbb{Z}^{(2)}$, which also by the fundamental theorem, G/C is isomorphic to $\mathbb{Z}^{(2)}$. We claim that $\phi \colon G \to \mathbb{Z}^{(2)}$ is defined by $(k, l, m) \mapsto (l, m)$. So what remains to show? All we need to show is that ϕ is a homomorphism, and that

$C = \{(k, 0, 0) \mid k \in \mathbb{Z}\}$ is the kernel of ϕ. ϕ is obviously a well-defined map to $\mathbb{Z}^{(2)}$, and

$$\begin{aligned}\phi((k_1, l_1, m_1)(k_2, l_2, m_2)) &= \phi(k_1 + k_2 + l_1 m_2, l_1 + l_2, m_1 + m_2)\\ &= (l_1 + l_2, m_1 + m_2)\\ &= (l_1, m_1) + (l_2, m_2)\\ &= \phi(k_1, l_1, m_1) + \phi(k_2, l_2, m_2)\end{aligned}$$

So ϕ is a homomorphism. Now, $\ker \phi = C$. The identity of $\mathbb{Z}^{(2)}$ is $(0, 0)$, and note that ϕ will map any element in G to $(0, 0)$ if and only if the last two elements in G are 0. This is exactly $C = \{(k, 0, 0) \mid k \in \mathbb{Z}\}$, thus $C = \ker \phi$.

Problem 4 (Ch. 1.9)

Determine $\operatorname{Aut} G$ *for (i)* G *an infinite cyclic group, (ii) a cyclic group of order six, (iii) for any finite cyclic group.*

Solution. Consider an infinite cyclic group, $G = \langle g \rangle$. Since G is infinite, there is are only two possible generators, namely g and g^{-1}. In order for the image of our homomorphism to be equal to $\langle g \rangle$, we need the image to be equal to $\langle g \rangle = \langle g^{-1} \rangle$. By Theorem 1.7. we need only specify how a homomorphism acts on the generator for G to specify a homomorphism. The only homomorphisms that have a range of G is $\phi(g) = g$ and $\phi(g) = g^{-1}$. Thus, $\operatorname{Aut} G =$ the identity map, and the inverse map (mapping each element to its inverse).

Now consider a cyclic group of order six, ie. $G = \langle g \rangle$ and $g^6 = 1_G$. Note that $\langle g^5 \rangle = G$ as well, thus g^5 is also a generator for G. Note that for all other elements $g' \in G \setminus \{g, g^5\}$, $\langle g' \rangle \neq G$. Thus, any automorphism must map all g into g or g^5. Thus $\operatorname{Aut} G =$ the identity map, and $\phi\colon g \to g^5$.

Finally, consider an arbitrary finite cyclic group. Let $G = \langle g \rangle$ where g is of order n. The potential generators of G are all a^k such that $(n, k) = 1$ and $k \leq n$ (as we proved in problem 4 of Jacobson 1.5). Thus $\operatorname{Aut} G = \{\phi\colon a \mapsto a^k \mid k \leq n, (n, k) = 1\}$.

Problem 5 (Ch. 1.9)

Determine $\operatorname{Aut} S_3$.

Solution. Note that (12) and (123) are generators of S_3. Define $a = (12)$ and $b = (123)$. Note that $S_3 = \langle a, b \mid a^2 = b^3 = 1, ab = b^2 a\rangle$. Also, $((12), (123)), ((13), (123)), ((23), (123)), ((12), (132)), ((13), (132))$ are generators of S_3. By theorem 1.7, we need only specify mapping the generators of S_3. But mapping our generators to each of these generators is a map from S_3 to S_3 (since both generate S_3). Thus any map from (a, b) to one of our generators above is an automorphism, and since these are the only generators, it must be of this form. Thus

$$\operatorname{Aut} S_3 = \{\phi(a, b) = (a, b), \phi(a, b) = (a, ba), \phi(a, b) = (a, ba^2), \phi(a, b) = (a^2, b), \phi(a, b) = (a^2, ba), \phi(a, b) = (a^2, ba^2)\}$$

Problem 8 (Ch. 1.9)

Let G *be a group such that* $\operatorname{Aut} G = 1$. *Show that* G *is abelian and that every element of* G *satisfies the equation* $x^2 = 1$. *Show that if* G *is finite then* $|G| = 1$ *or* 2 *(*Hint: *Use the procedure of finding a base for a vector space to show that* G *contains elements* $a_1, a_2, \ldots, a_r$ *such that every element of* G *can be written in one and only one way in the form* $a_1^{k_1} a_2^{k_2} \cdots a_r^{k_r}, k_i = 0, 1$. *Then show that there exists an automorphism interchanging* a_1 *and* a_2*.)*

Solution. Recall from Jacobson problem 6 from 1.9: we have $I_a \in \operatorname{Aut} G$ where $I_a\colon x \mapsto axa^{-1}$, and if $\operatorname{Inn} G = \{I_a \mid a \in G\}$ then $\operatorname{Inn} G \cong G/C$ (where C is the center of G). So $\operatorname{Inn} G \subseteq \operatorname{Aut} G$. But since $\operatorname{Aut} G = 1$, $\operatorname{Inn} G$ only has one element, namely I_{1_G}. But since $\operatorname{Inn} G \cong G/C$, $|G/C| = 1$ as well. Since G/C are the cosets of C in G, and there is only one possible coset, this must mean $C = G$. But if the center of G is the entire group, we know that G is abelian.

Further, from Jacobson problem 3 from 1.9, which states that $x \to x^{-1}$ is an automorphism of G if and only if G is abelian, we have that the inverse map is an automorphism of G. But since $\operatorname{Aut} G = 1$, $x \to x^{-1}$ must also be the identity map, thus each element in G is its own inverse. Thus $x^2 = 1$ for all $x \in G$.

Finally, let G be finite. Then we have a finite set of generators for G, $a_1, a_2, \cdots, a_r$. Thus, every element $g \in G$ can be written as a finite string $g = a_{i_1}^{\alpha_{i_1}} a_{i_2}^{\alpha_{i_2}} \cdots a_{i_j}^{\alpha_{i_j}}$, but since the group is abelian, we can rearrange it the a

to get $g = a_1^{k_1} a_2^{k_2} \cdots a_r^{k_r}$, and since $a^2 = 1$ for any a, we have that $k_i = 0, 1$ for all $1 \le i \le r$. To show that the k_i are unique (namely $k_i = 0$), we have $g = a_1^{k_1'} a_2^{k_2'} \cdots a_r^{k_r'}$ where $k_i' = 0, 1$ for all $1 \le i \le r$ as well. Then $a_1^{k_1} a_2^{k_2} \cdots a_r^{k_r} = a_1^{k_1'} a_2^{k_2'} \cdots a_r^{k_r'}$, which implies $a_1^{k_1 - k_1'} a_2^{k_2 - k_2'} \cdots a^{k_r - k_r'} = 1$. If $k_i - k_i' = 0$, we are done. Otherwise, there exists some $a_j^{k_j - k_j'}$ such that $k_j - k_j' \in \{-1, 1\}$. Then $1 = a_j^{\pm 1} a_1^{k_1 - k_1'} \cdots$ so $a_j^{\mp 1} = a_1^{k_1 - k_1'} \cdots$, so the right hand side generates the element on the left. Repeat this process without a_j, which we can do since there is a finite set of them. Eventually, we reach some set of generators $a_1, \dots, a_k$ such that there is no a_j, otherwise there are no generators and $G = 1$ and we are done anyway. If there is some set, we have that the only representation of 1 with the generators is with $1 = a_1^0 \cdots a_q^0$. Then $g = a_1^{k_1} \cdots a_q^{k_q} = a_1^{k_1'} \cdots a_q^{k_q'}$ implies that $k_i = k_i'$ for all $1 \le i \le q$, thus the representation of g by these generators are unique.

Consider the map $\phi\colon G \to G$ that swaps $a_1 \to a_j$ for some $1 \le j \le k$. This map is well-defined, since the representation of an element in g is uniquely determined, as we just proved, and so g will always get mapped to the same element. We claim that this is a automorphism. First, we show that it is a homomorphism:

$$\begin{aligned}
\phi(a_1^{k_1} \cdots a_q^{k_q})\phi(a_1^{k_1'} \cdots a_q^{k_q'}) &= (a_j^{k_1} \cdots a_1^{k_j} \cdots a_q^{k_q})(a_j^{k_1'} \cdots a_1^{k_j'} \cdots a_q^{k_q'}) \\
&= a_j^{k_1 + k_1'} \cdots a_1^{k_j + k_j'} \cdots a_q^{k_q + k_q'} \\
&= \phi(a_1^{k_1 + k_1'} \cdots a_q^{k_q + k_q'}) \\
&= \phi((a_1^{k_1} \cdots a_q^{k_q})(a_1^{k_1'} \cdots a_q^{k_q'}))
\end{aligned}$$

Now, we show that it is a bijection to show that it is an isomorphism. But we have a well-defined inverse, namely itself, since swapping a_1 with a_j and swapping them again is just the identity map (and it is well-defined since ϕ is well-defined). Thus, ϕ is an isomorphism. Finally, $\phi \in \operatorname{Aut} G$, since any bijection on a finite set (and G is finite) to itself must map each element in G to another element in G. Now recall that $\operatorname{Aut} G = 1$, thus swapping a_1 with an arbitrary a_j keeps $g \in G$ the same, thus $a_1 = a_2 = \cdots = a_q$. But then G is a group with only one generator, or $G = \langle a_1 \rangle$. But $a_1^2 = 1$, thus $G = \{1, a_1\}$, so $|G| = 2$. Recall earlier that we could also have $G = 1$ (if there are no generators), so we can also have $|G| = 1$, as desired.