Problem 2 (Ch. 1.5)

Let M be a monoid generated by a set S and suppose every element of S is invertible. Show that M is a group.

Solution. Since a group is just a monoid where every element is invertible, all that is required is to show that for all $m \in M$, there exists $m^{-1} \in M$ such that $mm^{-1} = m^{-1}m = 1_M$. Since M is generated by $S = \{s_1, s_2, \ldots, s_n\}$, then any $m \in M$ can be represented as

$$m = s_{j_1}^{e_{j_1}} s_{j_2}^{e_{j_2}} \cdots s_{j_n}^{e_{j_n}}$$

where $j_i \in \{1, 2, \ldots, n\}$ is some index on the generators of M. Since every s_i is invertible, $s_i^{-1} = M$, and by closure, $(s_i^{-1})^{e_i} = s^{-e_i} \in M$ as well. But then

$$m' = s_n^{-e_n} s_{n-1}^{-e_{n-1}} \cdots s_1^{-e_1} \in M$$

as well. We have that

$$\begin{aligned}
mm' &= s_{j_1}^{e_{j_1}} s_{j_2}^{e_{j_2}} \cdots s_{j_{n-1}}^{e_{j_{n-1}}} s_{j_n}^{e_{j_n}} s_{j_n}^{-e_{j_n}} s_{j_{n-1}}^{-e_{j_{n-1}}} s_{j_n} \cdots s_{j_1}^{-e_{j_1}} \\
&= s_{j_1}^{e_{j_1}} s_{j_2}^{e_{j_2}} \cdots s_{j_{n-1}}^{e_{j_{n-1}}} (s_{j_n}^{e_{j_n}} s_{j_n}^{-e_{j_n}}) s_{j_{n-1}}^{-e_{j_{n-1}}} s_{j_n} \cdots s_{j_1}^{-e_{j_1}} \\
&= s_{j_1}^{e_{j_1}} s_{j_2}^{e_{j_2}} \cdots s_{j_{n-1}}^{e_{j_{n-1}}} 1_M s_{j_{n-1}}^{-e_{j_{n-1}}} s_{j_n} \cdots s_{j_1}^{-e_{j_1}} \\
&= s_{j_1}^{e_{j_1}} s_{j_2}^{e_{j_2}} \cdots s_{j_{n-1}}^{e_{j_{n-1}}} s_{j_{n-1}}^{-e_{j_{n-1}}} s_{j_n} \cdots s_{j_1}^{-e_{j_1}} \\
&\ \ \vdots \\
&= s_{j_1}^{e_{j_1}} s_{j_1}^{-e_{j_1}} \\
&= 1_M
\end{aligned}$$

where we can introduce the parantheses on line 2 since monoids are associative. Likewise

$$\begin{aligned}
m'm &= s_{j_n}^{-e_{j_n}} s_{j_{n-1}}^{-e_{j_{n-1}}} \cdots s_{j_2}^{-e_{j_2}} s_{j_1}^{-e_{j_1}} s_{j_1}^{e_{j_1}} s_{j_2}^{e_{j_2}} \cdots s_{j_n}^{e_{j_n}} \\
&= s_{j_n}^{-e_{j_n}} s_{j_{n-1}}^{-e_{j_{n-1}}} \cdots s_{j_2}^{-e_{j_2}} (s_{j_1}^{-e_{j_1}} s_{j_1}^{e_{j_1}}) s_{j_2}^{e_{j_2}} \cdots s_{j_n}^{e_{j_n}} \\
&= s_{j_n}^{-e_{j_n}} s_{j_{n-1}}^{-e_{j_{n-1}}} \cdots s_{j_2}^{-e_{j_2}} 1_M s_{j_2}^{e_{j_2}} \cdots s_{j_n}^{e_{j_n}} \\
&= s_{j_n}^{-e_{j_n}} s_{j_{n-1}}^{-e_{j_{n-1}}} \cdots s_{j_2}^{-e_{j_2}} s_{j_2}^{e_{j_2}} \cdots s_{j_n}^{e_{j_n}} \\
&\ \ \vdots \\
&= s_{j_n}^{-e_{j_n}} s_{j_n}^{e_{j_n}} \\
&= 1_M
\end{aligned}$$

Thus, $m' = m^{-1}$, and since m was arbitrary, every element in M is invertible, making M a group.

Problem 5 (Ch. 1.5)

Show that any finitely generated subgroup of the additive group of rationals $(\mathbb{Q}, +, 0)$ *is cyclic. Use this to prove that this group is not isomorphic to the direct product of two copies of it.*

Solution. Let S be an arbitrary finitely generated subgroup of the additive rationals. That is, $\langle \frac{p_1}{d_1}, \frac{p_2}{d_2}, \ldots, \frac{p_n}{q_n} \rangle = S$, where the fractions are simplified (ie. $(p_i, d_i) = 1$). Let $q = \frac{1}{d_1 d_2 \cdots d_n}$. We claim that S is a subgroup of $\langle q \rangle$. We already know that S is a group, since it was generated by a set, but we need to show that the collection of elements in S is a subset of $\langle q \rangle$. Let $s \in S$. Then $s = j_1 \frac{p_1}{q_1} + j_2 \frac{p_2}{q_2} + \cdots + j_n \frac{p_n}{q_n}$ (since $(\mathbb{Q}, +, 0)$ is abelian, we can ignore when the $\frac{p_i}{d_i}$ is added after $\frac{p_k}{d_k}$ where $i < k$, since we can just move $\frac{p_i}{d_i}$ in front). Note

$$s = \frac{(j_1 p_1 d_2 d_3 \cdots d_n) + (j_2 p_2 d_1 d_3 \cdots d_n) + \cdots + (j_n p_n d_1 d_2 \cdots d_{n-1})}{d_1 d_2 \cdots d_n}$$

by just multipying each term by the factors not present in its denominator. But then

$$s = \big((j_1p_1d_2d_3\cdots d_n) + (j_2p_2d_1d_3\cdots d_n) + \cdots + (j_np_nd_1d_2\cdots d_{n-1})\big)q \in \langle q\rangle$$

Thus, since $s \in S$ was arbitrary, we can say $S \subseteq \langle q\rangle$.

But then, by Theorem 1.3 in Jacobson, which states that any subgroup of cyclic group is also cyclic, we have that S is also cyclic since $\langle q\rangle$ is cyclic. Since S was arbitrary, any finitely generated subgroup of $(\mathbb{Q}, +, 0)$ is cylic.

We have $S = \langle q\rangle$ where q is defined as above. We now prove that $S \not\cong S\times S$. Let $\phi\colon S \to S\times S$ be a homomorphism. It is sufficient to show that ϕ is not surjective. For the sake of contradiction, let ϕ be surjective. Then for any $s \in S$, we have that $s = mq$ for some $q \in \mathbb{Z}$. Thus $\phi(s) = \phi(mq) = m\phi(q)$. Thus, any element in $S\times S$ is of the form $m\phi(q)$ for some $\phi(q) \in S\times S$. We can write $\phi(q) = (a, b)$ for $a, b \in S$, and since $m(a, b) = (ma, mb)$, all elements in $S\times S$ can be written in the form (ma, mb), But since $b \in S$, we also have $2b \in S$, so $(a, 2b) \in S\times S$. But this contradicts that every element in $S\times S$ can be written as $m(a, b)$. Thus, ϕ is not surjective, and the two groups are not isomorphic.

Problem 6 (Ch. 6)

Let a, b be as in Lemma 1. Show that $\langle a\rangle\cap\langle b\rangle = 1$ and $\langle a, b\rangle = \langle ab\rangle$.

Solution. Given an abelian group G, we let a, b be elements with orders m, n respectively, such that $(m, n) = 1$.

To prove $\langle a\rangle\cap\langle b\rangle = 1$, assume the opposite, specifically there exists some $g \in G$ where $g \neq 1_G$, and $g \in \langle a\rangle\cap\langle b\rangle$. Necessarily, $g = a^j = b^k$ where $0 < j < m$ and $0 < k < n$. We have $g^m = (a^j)^m = (a^m)^j = 1_G$ and $g^n = (b^k)^n = (b^n)^k = 1_G$. Note that if $g^m = 1_G$, then $\mathrm{ord}(g) \mid m$. To see this, assume the opposite, that is $\mathrm{ord}(g) \nmid m$. Then by division algorithm, $m = \mathrm{ord}(g)q + r$ where $0 < r < \mathrm{ord}(g)$. But $1_G = g^m = g^{\mathrm{ord}(g)q+r} = (g^{\mathrm{ord}(g)})^q g^r = 1_G g^r = g^r$, and since $r < \mathrm{ord}(g)$, and $\mathrm{ord}(g)$ is the least value such that g to the power of it is 1_G, we have that $g^r \neq 1_G$, which is a contradiction. Thus, $\mathrm{ord}(g) \mid m$ and $\mathrm{ord}(g) \mid n$. But recall that $(m, n) = 1$, but the only element that this is true is 1_G, thus, we cannot have $g \neq 1_G$. Thus, $\langle a\rangle\cap\langle b\rangle = 1_G$.

We now prove that $\langle a, b\rangle = \langle ab\rangle$. Let $c \in \langle a, b\rangle$. Then $c =$ some sequences of a's and b's. Note that we can then say $c = a^jb^k$ where $0 \le j < m$ and $0 \le k < n$, since G is abelian (we can rearrange to get $c = a^\alpha b^\beta = a^{mq_1+j}b^{nq_2+k}$, where j, k are as above, but then $c = (a^m)^{q_1}a^j(b^n)^{q_1}b^k = 1_Ga^j1_Gb^k = a^jb^k$). Then $c = (ab)^jb^{k-j}$. But note that $k - j$ ... what now?

Assuming we get to $c \in \langle ab\rangle$ and so $\langle a, b\rangle \subseteq \langle ab\rangle$, we now show the other direction, so let $c \in \langle ab\rangle$. Trivially $c \in \langle a, b\rangle$, since $c =$ to some sequence of a's and b's. Thus, we have shown $\langle a, b\rangle = \langle ab\rangle$.

Problem 7 (Ch. 1.5)

Show that if $o(a) = n = rs$, where $(r, s) = 1$, then $\langle a\rangle \cong \langle b\rangle\times\langle c\rangle$, where $o(b) = r$ and $o(c) = s$. Hence, prove that any finite cyclic group is isomorphic to a direct product of cyclic groups of prime power orders.

Solution. Note that, by Theorem 1.3 in Jacobson, there exists only one subgroup of order r, s in $\langle a\rangle$. Note that by Problem 4 in Ch. 1.5 (which we did on the last homework), we know that a^r has order $[n, r]/r = s$, and likewise a^s has order $[n, s]/s = r$. Thus our unique groups with order r, s are $\langle a^s\rangle, \langle a^r\rangle$ respectively. We let $\phi\colon \langle a\rangle \to \langle b\rangle\times\langle c\rangle$ such that

$$\phi(a^j) = (b^m, c^k)$$

where $m \in \mathbb{N}, 0 \le m < r$ such that $j = ms$, and $k \in \mathbb{N}, 0 \le k < s$ such that $j = kr$. I'm running out of time before the deadline, so I will just sketch what I would have done: I would show that this is a bijective map, using the fact that since $(r, s) = 1$. Then, I would have shown the multiplication is respected by just pushing the symbols.