Problem 2 (Ch. 1.3)

Show that the two groups given in examples 11 and 13 on pages 33 and 34 are isomorphic. Obtain a subgroup of S_n isomorphic to these groups.

Solution. We provide the bijection $\phi\colon R_n \to U_n$ below. If $\tau = \frac{2j\pi}{n} \in R_n$ where $j \in \mathbb{Z}$, $0 \leq j < n$, then

$$\phi(\tau) = e^{i2j\pi/n}$$

If $\tau_1 = \frac{2j_1\pi}{n}$, $\tau_2 = \frac{2j_2\pi}{n}$, (so $0 \leq j_1, j_2 < n$) and $\phi(\tau_1) = \phi(\tau_2)$, in other words $e^{i2j_1\pi/n} = e^{i2j_2\pi/n}$, then $\tau_1 = \tau_2$ (since if $\theta \in [0, 2\pi)$, $e^{i\theta}$ is unique so we must have $\theta_1 = \theta_2 \implies i2j_1\pi/n = i2j_2\pi/n \implies \tau_1 = \tau_2$). So ϕ is injective. Now let $y \in U_n$ where $y = e^{i2j\pi/n}$ for $0 \leq j < n$, we have that $\phi(\frac{i2j\pi}{n}) = y$, so ϕ is surjective, therefore ϕ is bijective.

Now we show that ϕ respects the group operations. Let $\tau_1 = \frac{2j_1\pi}{n}$, $\tau_2 = \frac{2j_2\pi}{n}$ $(0 \leq j_1, j_2 < n)$. We have

$$\begin{aligned}
\phi(\tau_1\tau_2) &= \phi(\frac{2j_1\pi}{n} + \frac{2j_2\pi}{n}) \\
&= \phi(\frac{2(j_1+j_2)\pi}{n}) \\
&= e^{i2(j_1+j_2)\pi/n} \\
&= e^{i2j_1\pi/n}e^{i2j_2\pi/n} \\
&= \phi(\tau_1)\phi(\tau_2)
\end{aligned}$$

Thus, $R_n \cong U_n$.

Problem 4 (Ch. 1.3)

Is the additive group of integers isomorphic to the additive group of rationals (examples 1 and 2 on p. 32)?

Solution. For the sake of contradiction, assume there exists a bijection $\phi\colon (\mathbb{Z}, +) \to (\mathbb{Q}, +)$ that preserves the group operations (it's isomorphic). Note that there exists an element $n \in (\mathbb{Z}, +)$ such that for all $z \in \mathbb{Z}$, there exists $m \in \mathbb{Z}$ where $z = n^m$. For concreteness, we know that $n = 1$. Thus, for all $q \in \mathbb{Z}$, we must have a $m \in \mathbb{Z}$ such that $q = \phi(n)^m$, otherwise we have $z \in \mathbb{Z}$ such that $q = \phi(z)$ by surjectivity of ϕ, but $q \neq \phi(\underbrace{n + n + \cdots + n}_{m \text{ times}}) = \underbrace{\phi(n) + \phi(n) + \cdots + \phi(n)}_{m \text{ times}} = \phi(z) = q$ which is a contradiction. Let $\frac{p}{r} = \phi(n)$ where $p \in \mathbb{Z} \setminus \{0\}, r \in \mathbb{N} \setminus \{0\}$ and $\gcd(p, r) = 1$ (we have excluded $\phi(n) \neq 0$ by saying $p \neq 0$, because $\underbrace{0 + 0 + \cdots + 0}_{m \text{ times}} = 0$ and so will never have the desired property since $\{0\} \neq \mathbb{Q}$). But for all $m \in \mathbb{N}$, $\underbrace{\frac{p}{r} + \frac{p}{r} + \cdots \frac{p}{r}}_{m \text{ times}} = \frac{pm}{r} \neq \frac{1}{r+1} \in \mathbb{Q}$, since if we did have m where $\frac{pm}{r} = \frac{1}{r+1}$, then we would have $pm(r+1) = r$, but if $p < 0$ since $m, r+1 \geq 0$ then $pm(r+1) \leq 0 < r$ and so we can't have equality, and if $p > 0$ (and $m \neq 0$, otherwise $pm(r+1) = 0 < r$) then the left side of the equality is $r+1$ times positive constants, so $pm(r+1) \geq r+1 > r$, so we can't have equality again. But then we have $q \in \mathbb{Q}$ that is not $\phi(n)^m$, which is a contradiction, thus ϕ is not an isomorphism.

Problem 5 (Ch. 1.3)

Is the additive group of rationals isomorphic to the multiplicative group of non-zero rationals (examples 2 and 5 on p. 32)?

Solution. For the sake of contradiction, assume that $\phi\colon (\mathbb{Q}, \times) \to (\mathbb{Q}, +)$ that preserves the group operation (it's isomorphic). Then, we have $\phi(4) = \phi(2 \times 2) = \phi(2) + \phi(2)$. We also hae $\phi(4) = \phi(-2 \times -2) = \phi(-2) + \phi(-2)$. So $\phi(2)+\phi(2) = \phi(-2)+\phi(-2)$. But $2 \neq -2$ so $\phi(2) \neq \phi(-2)$ since ϕ is injective. Now for $q_1, q_2 \in \mathbb{Q}$, if $q_1 \neq q_2$ then we know that $2q_1 \neq 2q_2$ (a property we know of the rationals). But then $\phi(4) = \phi(2) + \phi(2) \neq \phi(-2) + \phi(-2) = \phi(4)$, but then ϕ maps 4 to more than one value in $\mathbb{Q}$, thus ϕ is not a function, a contradiction.

Problem 1 (Ch. 1.5)

*As in section 1.4, let $C(A)$ denote the centralizer of the subset A of a monoid M (or a group G). Note that $C(C(A)) \supset A$ and if $A \subset B$ then $C(A) \supset C(B)$. Show that these imply that $C(C(C(A))) = C(A)$. Without using the explicit form of the elements of $\langle A \rangle$ show that $C(A) = C(\langle A \rangle)$. (*Hint: *Note that if $c \in C(A)$ then $A \subset C(c)$ and hence $\langle A \rangle \subset C(c)$.) Use the last result to show that if a monoid (or a group) is generated by a set of elements A which pair-wise commute, then the monoid (group) is commutative.*

Solution. Let A be an arbitrary subset of a monoid M (or group G). Since $A \subset C(C(A))$, then we know that $C(A) \supset C(C(C(A)))$ by the second given property. Now let $B = C(A)$, then plugging B into the first given property, we have $C(C(B)) \supset B$. But substituting $C(A)$ back in for B, we get $C(C(C(A))) \supset C(A)$. Thus, we have set inclusion in both ways, so $C(C(C(A))) = C(A)$.

Note that by definition, $\langle A \rangle$ is the smallest submonoid of M (or subgroup of G) that contains A, thus $\langle A \rangle \supset A$. From the hint, we know that $\langle A \rangle \subset C(c)$ where $c \in C(A)$, but then applying the second property we have $C(\langle A \rangle) \supset C(C(c))$. But we know that $c \in C(C(c))$, since if c commutes with element $m \in M$, then $m \in C(c)$ and $c \in C(m)$. But this is for all $m \in C(c)$, thus $c \in C(C(c))$. And since since $C(\langle A \rangle \supset C(C(c))$, we have that $c \in C(\langle A \rangle)$. But since c was an arbitrary element in $C(A)$, we have that $C(A) \subset C(\langle A \rangle)$. Thus $C(\langle A \rangle) = C(A)$.

Now let M be generated by a set of elements A which pair-wise commute. Then $M = \langle A \rangle$ and $C(A) \supset A$. We are seeking to prove that $M = C(M)$. Since M and $\langle A \rangle$ are equal, we have that their centralizer is the same, so $C(M) = C(\langle A \rangle)$. But recall we jsut proved $C(\langle A \rangle) = C(A)$, thus $C(M) = C(A)$. But $C(A)$ is a submonoid that contains A, and $\langle A \rangle$ is, by definition, the smallest submonoid that contains A and is contained in all submonoids that contain A, thus $\langle A \rangle \subset C(A) = C(M)$. But then $M \subset C(M)$. But note that we also have $M \supset C(M)$, since $C(M)$ is a submonoid of M, thus we have proved $M = C(M)$.

Problem 3 (Ch. 1.5)

Let G be an abelian group with a finite set of generators which is periodic *in the sense that all of its elements have finite order. Show that G is finite.*

Solution. Let $g_1, g_2, \ldots, g_k$ be the generators with orders $o_1, o_2, \ldots, o_k$ respectively. If $g \in G$, then $g = g_1^{e_1} g_2^{e_2} \cdots g_k^{e_k}$ where $0 \leq e_1 < o_1$, $o \leq e_2 < o_2$ etc. Note that we do not care about the permutations of $g_1, g_2, \ldots, g_k$, because the set is abelian and so changing the order does not change the value. Thus, the number of possible elements in g is the different combinations of $e_1, e_2, \ldots, e_k$, which is a finite value. Thus, G contains finite number of elements, so G is finite.

Problem 4 (Ch. 1.5)

Show that if g is an element of a group and $o(g) = n$ then $g^k, k \neq 0$, has order $[n,k]/k = n/(n,k)$. Show that the number of generators of $\langle g \rangle$ is the number of positive integers $< n$ which are relatively prime to n. This number is denoted as $\phi(n)$ and ϕ is called the Euler ϕ-function.

Solution. We assert that $[n,k]/k$ is the order of g^k. First, we have $(g^k)^{[n,k]/k} = g^{[n,k]} = (g^n)^j = 1^j = 1$ (where $j \in \mathbb{N} \setminus \{0\}$). Now we show that this is the smallest value. Assume that $e \in \mathbb{N} \setminus \{0\}$ where $e < [n,k]/k$ and $(g^k)^e = g^{ke} = 1$. But then we must have ke be some multiple of n, say nm ($m \in \mathbb{N} \setminus \{0\}$), however, $nm = ke < [n,k]$, which contradicts that $[n,k]$ is the lowest common multiple of n and k. Thus, we have $[n,k]/k$ is the order, and since $kn = [n,k](n,k)$, thus $n/(n,k) = [n,k]/k$.

We know g^k is a generator of $\langle g \rangle$ if and only if $o(\langle g^k \rangle) = n$. We just showed that $o(g^k) = \frac{n}{(n,k)}$ so we require that $(n,k) = 1$, thus they must be coprime.