# Math 322 Homework 4

Xander Naumenko

03/10/23

**Question 2.** Let $a \in M$. Since $M = \langle S \rangle$, we can write $a$ as $a = s_1 \cdot s_2 \cdots s_k, s_i \in S \forall i = 1, 2 \ldots, k$. Then we have $a^{-1} = s_k^{-1} \cdots s_1^{-1}$, so each element in $M$ is invertible and thus $M$ is a group.

**Question 5.** Let $S = \{q_1, q_2, \ldots, q_n\} \subset \mathbb{Q}$. We can write each $q_i$ as $q_i = \frac{a_i}{b_i}$ for some $a_i \in \mathbb{Z}, b_i \in \mathbb{N}, \gcd(a_i, b_i) = 1$. Define $q = \frac{1}{\operatorname{lcm}(b_1, b_2, \ldots, b_n)}$. Then for each $q_i$, we can write $q_i = qm$ for some $m \in \mathbb{Z}$. Thus $\langle S \rangle = \langle q \rangle$, i.e. $S$ is cyclic.

For the second part, let $\phi : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ be a map, we will show by contradiction that $\phi$ can't be an isomorphism, so for now assume that it is one. Let $G$ be the group generated by $(1, 0)$ and $(0, 1)$. By the result from the first part and the fact that $\phi$ is supposedly an isomorphism we have that $G = \langle (q_1, q_2) \rangle$ with at least one of $q_1, q_2 \neq 0$. However then $(1, 0) = a(q_1, q_2), (0, 1) = b(q_1, q_2)$ for some $a, b$ since $(1, 0) \in G, (0, 1) \in G$. However this implies that $a = 0, b = 0 \implies q_1 = 0$ or $q_2 = 0$ which is clearly a contradiction, so $\mathbb{Q}$ isn't isomorphic to the direct product of itself.

**Question 6.** By way of contradiction let $x \in \langle a \rangle$ and $x \in \langle h \rangle$ with $x \neq 1$. Then since $x$ is in a cyclic subgroup generated by $a$ we can write $x = a^k$ for some $k < m$, and it must be that $x^m = x^n = 1$. Without loss of generality assume $m > n$, then $x^{m-n} = a^{k(m-n)} = 1 \implies m | k(m - n)$. However $k < m$ and $m - n$ shares no factors with $m$, so this is clearly impossible and it must instead be that $\langle a \rangle \cap \langle b \rangle = 1$.

For the second part, note firstly that clearly $\langle ab \rangle \subset \langle a, b \rangle$ since any $ab^k = a^k b^k$. For the other direction, let $x = a^k b^l \in \langle a, b \rangle$. Let $c$ be a solution to the set of modular equations $c \equiv 0 \mod n, c \equiv k \mod m$ and similarly $d$ be the solution to $d \equiv 0 \mod m, d \equiv l \mod n$. Such solutions are guaranteed to exist since $(m, n) = 1$. Then $(ab)^{c+d} = a^{c+d} b^{c+d} = a^c b^d = a^k b^l$. Thus both sets contain one another and $\langle a, b \rangle = \langle ab \rangle$.

**Question 7.** For an element $p \in \langle a \rangle$ with $p = a^{sx+y}$ for some $0 \leq x < r, 0 \leq y < s$ (we can write it this way due to the division algorithm), define $\phi : \langle a \rangle \to \langle a \rangle \times \langle b \rangle$ as $\phi(p) = (a^x, b^y)$. Clearly the identity is preserved over this map, so only the preservation of the product is required. Let $p, q \in \langle a \rangle$ with $p = a^{sx_1+y_1}$ and $q = a^{sx_2+y_2}$. Then $\phi(pq) = \phi\left(a^{s(x_1+x_2)+y_1+y_2}\right) = (b^{x_1+x_2}, c^{y_1+y_2}) = \phi(p)\phi(q)$ as required.

We can apply what we just proved iteratively $k$ times to any $o(a) = n = P_1^{\alpha_1} \cdots P_k^{\alpha_k}$ to show that $\langle a \rangle = \langle P_1^{\alpha_1} \rangle \cdots \langle P_k^{\alpha_k} \rangle$. Thus any finite cyclic group is isomorphic to a direct product of cyclic groups of prime power orders.