Basic Algebra (Solutions)

by Huah Chu

Exercises (§1.5, p.47)

1. 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 pairwise commute, then the monoid (group) is commutative.

Proof. (1) $C(C(C(A))) = C(A)$:

¿From $C(C(A)) \supset A$, we have $C(C(C(A))) \subset C(A)$. On the other hand, replacing A in $C(C(A))$ by $C(A)$, we have $C(C(C(A))) \supset C(A)$. Hence these two sets are equal.

(2) $C(A) = C(\langle A \rangle)$:

For any $c \in C(A)$, $A \subset C(c)$. Thus $\langle A \rangle \subset C(c)$ since $C(c)$ is a monoid. $\langle A \rangle$ commute with every element of $C(A)$, hence $C(A) \subset C(\langle A \rangle)$.

(3) If a monoid M is generated by S and $st = ts$ for all $s, t \in S$, then M is commutative:

$S \subset C(S)$ since the elements of S are commutative. Applying (2), we have $C(S) = C(\langle S \rangle) = C(M)$ and hence $S \subset C(M)$. Thus $M = \langle S \rangle \subset C(M)$ and M is commutative. □

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

Proof. Every element of M has the form $s_1 s_2 \cdots s_r$, $s_i \in S$, which is invertible with inverse $s_r^{-1} s_{r-1}^{-1} \cdots s_1^{-1} \in M$. Hence M is a group. □

3. Let G be a finitely generated abelian group which is periodic in the sense that all of its elements have finite order. Show that G is finite.

Proof. Suppose G is an abelian group generated by $\{g_1, \ldots, g_n\}$ and $o(g_i) = \ell_i$. Then any element of G has the form $g_1^{\alpha_1} \cdot \cdots \cdot g_n^{\alpha_n}$ with $0 \leq \alpha_i < \ell_i$. Hence $|G| \leq \prod_{i=1}^{n} \ell_i$. □

4. 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.

Proof. (1) Let $g \in G$ with $o(g) = n$ and $o(g^k) = h$. It's clear that $(g^k)^{[n,k]/k} = 1$. Thus $h|[n,k]/k$ and $hk|[n,k]$. On the other hand, $(g^k)^h = 1$ implies $n|hk$. Hence hk is a common multiple of n and k and divides $[n,k]$. Therefore $hk = [n,k]$, $h = [n,k]/k = n/(n,k)$.

(2) $g^k \in \langle g \rangle$ is a generator of $\langle g \rangle$ if and only if $o(g^k) = n$. By the result of (1), $o(g^k) = n/(n,k)$. Hence g^k is a generator if and only if $(n,k) = 1$. □

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.

Proof. (1) Let H be the subgroup of $(\mathbb{Q}, +)$ generated by $\{\frac{q_1}{p_1}, \ldots, \frac{q_n}{p_n}\}$. Then H is contained in the cyclic group $\langle \frac{1}{p_1 \cdots p_n} \rangle$. Hence H is cyclic.

(2) Let H be the subgroup of $\mathbb{Q} \oplus \mathbb{Q}$ which is generated by (1,0) and (0,1). We shall show that H is not cyclic. Thus $\mathbb{Q} \oplus \mathbb{Q} \ncong \mathbb{Q}$.

Suppose that H is cyclic with generator $(a,b) \neq (0,0)$. Then $(1,0) = n(a,b)$ and $(0,1) = m(a,b)$ for some $n, m \neq 0$. Which implies $a = b = 0$ and leads to a contradiction. □

Remark. Given a finitely generated subgroup $H = \langle \frac{q_1}{p_1}, \ldots, \frac{q_n}{p_n} \rangle$, $(p_i, q_i) = 1$, of $(\mathbb{Q}, +)$, the reader is urged to construct a generator of H explicitly.

Exercise: Show that if $o(a) = n = rs$ where $(r,s) = 1$, then $\langle a \rangle \simeq \langle b \rangle \times \langle c \rangle$ 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 order.