MID-TERM ALGEBRA I SOLUTION 09.PDF

(1) Any cyclic group is abelian. We prove the converse. Assume that G is a finite abelian group of order n. If n is 1 then G is trivial and the result holds. If G is a p-group for some prime p, i.e. $n = p^r$ for some $r \in \mathbb{N}$, then by hypothesis there is an element $g \in G$ such that $\mathrm{o}(g) = p^r$. The subgroup $< a >$ of G generated by a has order same as G, and so $G =< a >$, showing that G is cyclic.

Now let $n = p_1^{r_1} \cdots p_l^{r_l}$ be the prime power decomposition of G. We proceed via induction on l. When $l = 1$, G is a p_1-group and has been dealt with. Assume that for $i \leq l - 1$, G is cyclic whenever G is abelian of order $p_1^{r_1} \cdots p_{l-1}^{r_{l-1}}$, p_i's distinct primes, r_i's positive integers. By given hypothesis, there is an element $a \in G$ of order $p_l^{r_l}$. As every subgroup of an abelian group are normal, the quotient group $H = G/ < a >$ is also abelian and has order $p_1^{r_1} \cdots p_{l-1}^{r_{l-1}}$. So by hypothesis, H is cyclic. As G is abelian, $G = H\times < a >$. We know that direct product of two finite cyclic groups of relatively prime order is again cyclic. So G is cyclic. By mathematical induction, the statement holds.

To see the statement about product of cyclic groups, consider two groups $< a >$ and $< b >$ of order m and n respectively, $(m, n) = 1$. Consider the group homomorphism $\mathbb{Z} \to < a > \times < b >$, given by $t \mapsto (a^t, b^t)$. The homorphism is surjective by Chinese remainder theorem. Its kernel is l.c.m.$(m, n)\mathbb{Z} = mn\mathbb{Z}$. So $< a > \times < b > \cong \mathbb{Z}/mn\mathbb{Z}$, a cyclic group of order mn.

(2)

Theorem 0.1. *(Lagrange's Theorem) Let G be any finite group. For any subgroup H of G, order of H divides the order of G.*

Proof. Let H has m many right cosets in G. Any two distinct cosets are disjoint and their union is G it self. Also each coset has size $|H|$. Thus $|G| = m \cdot |H|$, and hence $|H$ divides $|G|$. □

(3) Let us first look at part (b).

Question: Let G be a cyclic group of order n. Determine all elements of order m in it.

If $m \nmid n$, there is no element of order m in G (Lagrange's Theorem). So assume that $m|n$. Since G is cyclic, there is a unique subgroup of order m in it, which can be seen as follows. For any surjection $f : \mathbb{Z} \to G$, $f(\frac{n}{m}\mathbb{Z})$ is a subgroup of G, and by Isomorphism theorem, $\mathbb{Z}/\frac{n}{m}\mathbb{Z} \cong G/f(\frac{n}{m}\mathbb{Z})$. So $f(\frac{n}{m}\mathbb{Z})$ is of index n/m in G, and hence has order m. For any subgroup H of G of order m, $f^{-1}(H) = r\mathbb{Z}$ for some positive integer r, and hence $H = f(r\mathbb{Z})$. Again by isomorphism theorem $G/H \cong \mathbb{Z}/r\mathbb{Z}$. So $r = n/m$, and $H = f(\frac{n}{m})$.

Now if a be any element in G of order m, $< a >$ is the unique subgroup of G of order m, and a is a generator for this group. This precisely describes all such elements, and there are $\phi(m)$ many of them.

For part (a), there is a unique subgroup of order 8 in $\mathbb{Z}/8888888\mathbb{Z}$, and any element of order 8 is a generator of this subgroup. There are $\phi(8) = 2^{3-2}(2-1) = 4$ such elements.

(4) Any automorphism of a cyclic group maps generator to a generator. Let $G =< g >= \{e, g, g^2, \cdots, g^{n-1}\}$ be a cyclic group of order n. Then g^i is a generator if and only if $(i, n) = 1$. Now let $f \in \mathrm{Aut}(G)$. Then $f(g) = g^i$ for some i. As f is an isomorphism, $< g^i >= G$, and so $(i, n) = 1$. Thus g^i is a generator of G. Conversely, for any homomorphism $f : G \to G$ with $g \mapsto g^i$, it is an isomorphism if $(i, n) = 1$, i.e. g^i is a generator for G. Thus the image of g fully describes the automorphism group, namely $\mathrm{Aut}(G) \cong \{0 \leq i \leq n-1 | (i, n) = 1\} = \mathbb{Z}/\phi(n)\mathbb{Z}$, a cyclic group of order $\phi(n)$.

(5) (a) The inclusion $H \subseteq \Phi^{-1}\Phi(H)$ follows from the definition of set theoretic inverse. To see the other inclusion, consider an element $g \in \Phi^{-1}\Phi(H)$. So $\Phi(g) = \Phi(h)$ for some $h \in H$. As Φ is a group homomorphism, $\Phi(g^{-1}h) = e'$, where e' is the identity element in G'. Thus $g^{-1}h \in \ker(\Phi) = K$. So $g^{-1} = h^{-1}k$ for some $k \in K$. As $K \subseteq H$, $g^{-1} \in H$ implying $g \in H$.

(b) $\Phi : G \to G'$ is a surjective group homomorphism with kernel K. Define the following map

$$f : \{H \leq G | K \subseteq H\} \to \{H' \leq G'\}$$

$f(H) := \Phi(H)$. Clearly, this is a well defined map of sets. Let $f(H_1) = f(H_2)$. Choose $h_1 \in H_1$ arbitrarily. Then $\Phi(h_1 h_2^{-1}) = e'$ for some $h_2 \in H_2$, and hence $h_1 \in h_2 K \subseteq H_2$. This shows that $H_1 \subset H_2$. Similarly replacing h_1 by an element in H_2, we see that $H_1 = H_2$. This the map f is injective. As Φ is a surjection, for any subgroup H' of G', $\Phi^{-1}(H')$ is a subgroup of G containing K. Now by set theory, $f(\Phi^{-1}(H')) = H'$, showing that f is also onto.

Let H be a normal subgroup of G containing K, and $g' \in G'$. As Φ is a surjection, there is $g \in G$ with $\Phi(g) = g'$. So $g'^{-1}\Phi(H)g' = \Phi(g^{-1}Hg) = \Phi(H)$, showing that $f(H)$ is a normal subgroup of G'. Conversely, let H' be normal in G', $g \in G$ arbitrary. Let $\Phi(g) = g'$. Then $\Phi(g^{-1}\Phi^{-1}H'g) = g'^{-1}H'g' = H'$. As $\Phi^{-1}(H')$ contains K, we have $g^{-1}\Phi^{-1}(H')g = \Phi^{-1}(H')$.

(6) Let us first look at the geometric picture. $\mathbb{Z}\times\mathbb{Z}$ is an abelian group and so $< (1, 1) >$ (in fact any subgroup) is normal. $< 1, 1 >$ is the diagonal i.e. contains all the integral points (i.e. both coordinates integer) on the line $x = y$. Any element in the group $\mathbb{Z}^2/ < (1, 1) >$ is a coset $(a, b) < 1, 1 >= \{(i \cdot a, i \cdot b) | i \in \mathbb{Z}\}$, $a, b \in \mathbb{Z}$. These points lie on the line $y = \frac{b}{a}x$ passing through the origin. Also if (c, d) is any integral point on this line, $ad = bc$ and so $(c, d) = (a, b)\cdot(c/a, d/b) = (a, b)\cdot(c/a, c/a)$, and hence is an element of the coset with representitive (a, b). Thus we may view the group $\mathbb{Z}^2/ < (1, 1) >$ as the integral points on the lines passing through the origin with rational slope.

Define a map $f : \mathbb{Z}^2/ < (1, 1) > \to \mathbb{Q}$ as $(a, b) < (1, 1) > \mapsto b/a$. Then by the observation above, this map is well defined. $f((a, b) < (1, 1) > \cdot (c, d) < (1, 1) >) = f((ac, bd) < (1, 1) >) = bd/ac = b/a \cdot d/c = f((a, b) < (1, 1) >) \cdot f((c, d) < (1, 1) >)$. So f is indeed a group homomorphism. To show that f is onto, consider an element $a/b \in \mathbb{Q}$. Then $f((a, b) < (1, 1) >) = b/a$. If $(a, b) < (1, 1) >$ and $(c, d) < (1, 1) >$ are mapped to the same element under f, then $b/a = d/c$ and so they are on the same line passing through origin, and by the previous discussion, lies in the same coset. This shows that f is injective. Thus $\mathbb{Z} \times \mathbb{Z}/ < (1, 1) > \cong \mathbb{Q}$.

(7) Let $g = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in G$. The left coset of H in G with g as representative is given by $\{\begin{pmatrix} ax & b \\ 0 & 1 \end{pmatrix} | 0 \neq x \in \mathbb{R}\}$. Under the identification of g with the point (a, b) in

$\mathbb{R}^2 \setminus \{x = 0\}$, this coset corresponds to the line $y = b$ except the point $(0, b)$. So the left coset partition consists of all such lines. The right coset of H with representative g is given by $\{\begin{pmatrix} ax & bx \\ 0 & 1 \end{pmatrix} | 0 \neq x \in \mathbb{R}\}$. This corresponds to the line passing through (a, b) and $(0, 0)$ except the origin. So the right coset partition consists of all such lines.

From the partitions as above it is clear that H is not normal in G. To be precise, consider g as above, and let $h = \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} \in H$. Then $ghg^{-1} = \begin{pmatrix} x & b - bx \\ 0 & 1 \end{pmatrix} \notin H$ for $x \neq 1$.