MAT301 Groups and Symmetry

Assignment 3

Solutions

1. Let G be a cyclic group of order 40. Let g be a generator of G.

(a) How many generators does G have? List them. No explanation is necessary.
(b) Does G have a subgroup of order 15? Explain.
(c) Does G have a element of order 12? Explain.
(d) How many subgroups of order 8 does G have? Explain.
(e) Find the subgroup H of G that has order 8 (i.e. give its elements). List all the generators of H. No explanation necessary.
(f) List all the elements of order 8 in G. No explanation necessary.

Solution: (a) $\varphi(40) = 16$

(b) No. The order of every subgroup of G divides 40 and $15 \nmid 40$.

(c) No. The order of every element of G divides 40. (Indeed, every element of G is of the form g^k for some k, and $|g^k| = \frac{40}{\gcd(40,k)} \mid 40$.)

(d) Just one. A cyclic group of order n has a unique subgroup of order d for every divisor d of n.

(e) Since $|g| = 40$, $|g^5| = \frac{40}{5} = 8$. Thus $\langle g^5 \rangle = 8$. Since G has only one subgroup of order 8, we have

$$H = \langle g^5 \rangle = \{e, g^5, g^{10}, g^{15}, g^{20}, g^{25}, g^{30}, g^{35}\}.$$

Now note that H is a cyclic group of order 8 with generator $h := g^5$. Thus the generators of H are $h^1 = g^5, h^3 = g^{15}, h^5 = g^{25}$ and $h^7 = g^{35}$.

(f) g^5, g^{15}, g^{25} and $h^7 = g^{35}$ (i.e. the generators of the subgroup H of order 8 - see Problem 2a below).

2. (a) Let n be a positive integer and G a cyclic group of order n. Let d be a positive divisor of n. Show that G has $\varphi(d)$ elements of order d.

(b) Show that $U(2^n)$ is not cyclic for $n \geq 3$. (Suggestion: Find the orders of $[2^{n-1} + 1]$ and $[-1] = [2^n - 1]$. Is $[2^{n-1} + 1] = [-1]$?)

Solution: (a) By the fundamental theorem of cyclic groups, G has a unique subgroup of order d. Let us call this subgroup H. By the fundamental theorem of cyclic groups, H is cyclic. A cyclic group of order d has $\varphi(d)$ generators (see page 29, Corollary 4 of the notes), so that H has $\varphi(d)$ generators. We claim that the generators of H are exactly the elements of G that have order d. Indeed, let A be the set of elements of G that have order d. Let B be the set of generators of H. Given any $g \in A$, the subgroup $\langle g \rangle$ has order d (why?), and thus we must have $\langle g \rangle = H$ (as there is only one subgroup of order d). This shows $g \in B$. Thus $A \subset B$. On the other hand, given $h \in B$, $\langle h \rangle = H$ (by definition of B) and hence $|h| = |H| = d$, so that $h \in A$.

This gives $B \subset A$.

(b) In view of Part (a), it is enough to show that there is more than one element of order 2 in $U(2^n)$ when $n \geq 3$ (as a cyclic group of even order has $\varphi(2) = 1$ element of order 2). For this, we shall show that the elements $[-1]$ and $[2^{n-1}+1]$ of $U(2^n)$ are different and they both have order 2. We have $[-1] \neq [1]$ (why?), and $[-1]^2 = [(-1)^2] = [1]$. Thus $|[-1]| = 2$. We now show that $[2^{n-1}+1]$ also has order 2. Indeed, since $2n-2 \geq n$, we have

$$(2^{n-1}+1)^2 = 2^{2n-2} + 2^n + 1 \equiv 1 \pmod{2^n},$$

so that $[2^{n-1}+1]^2 = [1]$. Putting together with $[2^{n-1}+1] \neq [1]$, we get that $|[2^{n-1}+1]| = 2$.

So far we have shown that $[-1]$ and $[2^{n-1}+1]$ both have order 2. Since $n \geq 3$,

$$0 < 2^{n-1} + 2 < 2^{n-1} + 2^{n-1} = 2^n,$$

so that $2^{n-1}+1 \equiv -1 \pmod{2^n}$ and $[2^{n-1}+1] \neq [-1]$.

3. (a) Let $m \mid n$. Show that $\mu_m \subset \mu_n$.

(b) As before, let $m \mid n$. Suppose H is a subgroup of μ_n of order m. What is H? Explain. (Do not do any computation.)

(c) Describe all subgroups of μ_n.

(d) Suppose K is a finite subgroup of $\mathbb{C}^\times$. Show that $K = \mu_m$ for some m.

Solution: (a) Yes. If α is an m-th root of unity and $m \mid n$, then $\alpha^n = (\alpha^m)^{n/m} = 1^{n/m} = 1$ (note that n/m is an integer), thus α is also an n-th root of unity.

(b) The subgroup H is simply μ_m. Indeed, since μ_n is cyclic, it has a unique subgroup of order m. We know μ_m is a subgroup of μ_n that has order m. By uniqueness, it is the only such subgroup.

(c) By the fundamental theorem of cyclic groups and Part (a), the only subgroups of μ_n are the μ_m with $m \mid n$. (For example, the subgroups of μ_6 are $\mu_1, \mu_2, \mu_3, \mu_6$.)

(d) For brevity denote $|K|$ by m. Let $K = \{\alpha_1, \ldots, \alpha_m\}$. (Thus one of the α_i is 1.) Since K is finite, each α_i has finite order. In other words, for each α_i, there is a positive integer k_i such that $\alpha_i^{k_i} = 1$. Let $n = k_1 \cdot k_2 \cdots k_m$. (Note that we are multiplying finitely many numbers.) Then for every α_i, we have $\alpha_i^n = (\alpha_i^{k_i})^{n/k_i} = 1$, so that $\alpha_i \in \mu_n$. Thus $K \subset \mu_n$. By Part (c) above $m \mid n$ and $K = \mu_m$.

REMARK. In our argument above for Part (d) we did not want to use the general statement of Lagrange's theorem; we only used Lagrange for the special case of cyclic groups (i.e. that the order of every subgroup of a finite cyclic group divides the order of the group), which is more elementary to prove than the general case (see for instance, see the first few lines of the argument for Theorem 2(b) on page 41 of the notes). If we allow ourselves to use the general Lagrange, the proof of (d) becomes very short: Let $|K| = m$ as before. By Lagrange, every $\alpha \in K$ satisfies $\alpha^m = 1$ and hence belongs to μ_m. Thus $K \subset \mu_m$. Putting this together with $|K| = |\mu_m| = m$ it follows that $K = \mu_m$.

4. (a) Prove that for any positive integer n,

$$\sum_{d \mid n} \varphi(d) \;=\; n.$$

(Here φ is Euler's function and the sum is over the positive divisors of n. Suggestion: Let G be a cyclic group of order n. For every $d \mid n$, let $\psi(d)$ denote the number of elements of G that have order d. Is it true that $n = \sum_{d \mid n} \psi(d)$?)

(b) Let K be a finite group with the following property: for every divisor $d \mid |K|$, there is a unique subgroup of order d in K. Show that K is cyclic.

Solution: (a) Let G be a cyclic group of order n (e.g. μ_n). For each divisor d of n, let A_d be the set of all elements of G that have order d. Since the order of every element of G divides n, we have

$$G = \bigcup_{d \mid n} A_d.$$

(The notation on the right means the union of all the A_d as d runs through the divisors of n.) Of course, the A_d are disjoint. Denote the number of elements of A_d by $|A_d|$. Problem 2(a) tells use $|A_d| = \varphi(d)$. We have

$$n = |G| \overset{\text{why?}}{=} \sum_{d \mid n} |A_d| = \sum_{d \mid n} \varphi(d).$$

(b) Let $|K| = n$. For every $d \mid n$, let $\psi(d)$ denote the number of elements of K that have order d. We will show that $\psi(d) = \varphi(d)$ for every divisor d of n; this will prove the result, since in particular, it tells us there are $\varphi(n)$ (which is > 0) elements of of order n in K, and hence K is cyclic (why?).

Step 1: We prove (as an intermediate step) that if $\psi(d) \neq 0$, that is, if K contains an element of order d, then $\psi(d) = \varphi(d)$. Indeed, suppose K contains an element g of order d. Then the subgroup $\langle g \rangle$ is a subgroup of order d, and thus by the hypothesis the unique such subgroup, in K. Being a cyclic group of order d, the group $\langle g \rangle$ contains $\varphi(d)$ elements of order d (i.e. generators), namely the elements g^k with $1 \leq k \leq d$ and $\gcd(k, d) = 1$. But these are the only elements of order d in K, as if $h \in K$ is any element of order d, then $\langle h \rangle$ is a subgroup of order d, and hence by uniqueness of such subgroup, we must have $\langle h \rangle = \langle g \rangle$. In particular, $h \in \langle g \rangle$ and (having order d) h must be one of the elements g^k with $1 \leq k \leq d$ and $\gcd(k, d) = 1$. We have proved that (assuming K contains an element of order d, then) there are exactly $\varphi(d)$ elements of order d in K, i.e. $\psi(d) = \varphi(d)$.

Step 2: Denoting the set of elements of order d in K by A_d, on recalling that the order of every element of K divides $|K| = n$, we have

$$K = \bigcup_{d \mid n} A_d,$$

so that (since the A_d are disjoint),

$$n = |K| = \sum_{d \mid n} |A_d| = \sum_{d \mid n} \psi(d).$$

Step 3: We now use the conclusions of the previous two steps together with the identity of Part (a) to show that $\psi(d) = \varphi(d)$ for *every* divisor $d \mid n$. Indeed, Step 1, in particular, tells us that $\psi(d) \leq \varphi(d)$ for every $d \mid n$ (if $\psi(d) = 0$, the estimate is trivial, otherwise it holds thanks to Step 1). Putting this together with the fact that

$$\sum_{d \mid n} \psi(d) = \sum_{d \mid n} \varphi(d)$$

(both being equal to n, thanks to Step 2 and the identity of Part (a)), it follows that $\psi(d) = \varphi(d)$ for every divisor d of n. (To see this formally, combine $\sum_d (\varphi(d) - \psi(d)) = 0$ with $\varphi(d) - \psi(d) \geq 0$.)

5. For each permutation σ given below, determine if σ is even or odd, write σ as a product (i.e. composition) of disjoint cycles, and find the order of σ.

(a) $\sigma = (1245)(245)(321)$
(b) $\sigma = (12)(123)(3214)^{-1}$
(c) $\sigma = (1245)^2$
(d) $\sigma = (1238)(457)(69)$
(e) $\sigma = (135)(246)(1265)(78)$
(f) $\sigma = (12)(23)(34)(45)$
(g) $\sigma = (15)(14)(13)(12)$

Solution:

(a) Odd, $\sigma = (1354)$, order is 4.
(b) Even, $\sigma = (134)$, order is 3.
(c) Even, $(14)(25)$, order is 2.
(d) Even, $(1238)(457)(69)$, order is 12.
(e) Even, $(146)(35)(78)$, order is 6.
(f) Even, (12345), order is 5.
(g) Even, (12345), order is 5.

6. (a) Find all values that occur as the order of some element of S_6. (Your final list should include a number d if and only if there exists an element of order d in S_6.)

(b) Find the number of elements of S_6 of each order you listed in Part (a).

(c) Find the number of elements of A_6 that have order 4.

Solution: (a) Possible cycle types for elements of S_6 are listed below.

(i) 6: Elements of this type (i.e. 6 cycles) have order 6
(ii) 5,1: Elements of this type have order 5.
(iii) 4,2: Elements of this type have order 4.
(iv) 4,1,1: Elements of this type have order 4.
(v) 3,3: Elements of this type have order 3.
(vi) 3,2,1: Elements of this type have order 6.
(vii) 3,1,1,1: Elements of this type have order 3.

(viii) 2,2,2: Elements of this type have order 2.
(ix) 2,2,1,1: Elements of this type have order 2.
(x) 2,1,1,1,1: Elements of this type have order 2.
(xi) 1,1,1,1,1,1: This is the decomposition type of the identity. The order is 1.

Thus possible orders are 1,2,3,4,5,6.

(b) There is only one element of order 1 (namely the identity).

- Number of elements of order 2: These consist of elements of type 2,2,2, type 2,2,1,1, and type 2,1,1,1,1. The number of elements of type 2,2,2 is
$$\binom{6}{2}\binom{4}{2}\frac{1}{3!} = 15$$
(why?). The number of elements of type 2,2,1,1 is
$$\binom{6}{2}\binom{4}{2}\frac{1}{2} = 45.$$
The number of elements of type 2,1,1,1,1 is $\binom{6}{2} = 15$. Thus the number of elements of order 2 is 75.
- Number of elements of order 3: An element of order 3 is either of type 3,3 or 3,1,1,1. There are
$$\binom{6}{3}2 \cdot 2 \cdot \frac{1}{2} = 20 \cdot 2 = 40$$
elements of type 3,3 (why?). There are $\binom{6}{3} \cdot 2 = 40$ elements of type 3,1,1,1 (why?). Thus in total there are 80 elements of order 3.
- Number of elements of order 4: There are two cycle types elements of which have order 4, namely types 4,2 and 4,1,1. The number of elements of type 4,2 is
$$\binom{6}{4} \cdot 3! = 15 \cdot 3! = 90.$$
The number of elements of order 4,1,1 is also $\binom{6}{4} \cdot 3! = 90$. Thus there are 180 elements of order 4.
- Number of elements of order 5: Elements of order 5 are those of cycle type 5,1. There are
$$\binom{6}{5}4! = 144$$
of them.
- Number of elements of order 6: These are elements of types 6 or 3,2,1. There is $5! = 120$ elements of the former type and
$$\binom{6}{3} \cdot 2 \cdot \binom{3}{2} = 120$$
of the latter type. In total there are 240 elements of order 6.

(Sanity check: 1+75+80+180+144+240=720=6!)

(c) Elements of order 4 in S_6 are those with cycles types 4,2 or 4,1,1. Permutations of the former type are even whereas the ones of the latter type are odd (why?). Thus the elements of

A_6 that have order 4 are the permutations of type 4,2, the number of which is 90 (as calculated in the solution to part (b)).