Math 241

Problem Set 5 solution manual

Exercise. A5.1

Lemma 1. Let i, j, k, and l be 4 distinct elements: then we have $(ij)(kl) = (ijk)(jkl)$

proof. $(ij)(kl) = (ij)(jk)(jk)(kl) = (ijk)(jkl)$

Now let $\sigma \in A_n$, then using the fact that S_n is generated by the transpositions we can write σ as a product of an even number of transpositions.

Then: $\sigma = \tau_1.\tau_2....\tau_s$ for some s even.

Then consider each to consecutive transpositions:

$\tau_r\tau_m = (ij)(kl)$:We have two cases:

$$\begin{cases} i,j,k,l \ are \ distinct & then \ \tau_r\tau_m = (ijk)(kjl) \ by \ above \ lemma. \\ i = k(or \ similarly \ i = l \ or \ j = k \ or \ j = l & then \ \tau_r\tau_m = (ij)(kl) = (ij)(il) = (jil). \\ i = k \ j = l(or \ i = l \ j = k) & In \ this \ case \ they \ \ cancel \ each \ other. \end{cases}$$

Then we can join each to consecutive transpositions to get 3 cycles, then σ is the product of 3-cycles.

Section. 10

Exercise. 36

To do this exercise we need to do exercise 29 in section 4 first :

Ex 4:

Let $S = \{x \in G \mid x \neq x^{-1}\}$.

Then the number of elements of S is even, since the elements of S can be paired (x, x^{-1}), so S splits into two parts with same number of elements, and hence number of elements of S is even.

Then $G - S$, contains an even number of elements, but $G - S$ contains e, so it must contain an element $a \neq e$. Now since $a \notin S$ then a must be equal to its inverse, and hence $a^2 = a.a = a.a^{-1} = e$. So a is of order 2. So G contains an element of order 2.

Now back to our Ex:

We have $|G| = 2n$ for some n odd. Then by Ex 4 we know that G contains an element of order 2, call it a. Suppose G contains another element b, with $b \neq a$, and $b \neq e$, such that b is of order 2. It is then easy to verify that $H = \{e, a, b, ab\}$ is a subgroup of G.

We know that e, a, b are three distinct elements, now suppose $ab = a$ this implies that $b = e$ which is not true, similarly we can see that $ab \neq a$, and suppose $ab = e$, this implies that $b = a^{-1}$, which implies that $b = a$ which is not true. So we deduce that the elements of H are all distinct.

Finally by Lagrange we know that $|H|$ divides the order of G. This implies that 4 divides $2n$ $\implies$ 2 divides n, contradiction.

Then we conclude that G contains a unique element a with $a^2 = e$.

Exercise. 41

Let $a + \mathbb{Z}$ be a left coset of $\mathbb{Z}$ in $\mathbb{R}$. Then we can write a as $a = n + l$ for some $n \in \mathbb{Z}$, and $0 \leq l < 1$, then since we know that $a + \mathbb{Z} = \{a + k \mid k \in \mathbb{Z}\}$, $a - n \in a + \mathbb{Z}$, then $l \in a + \mathbb{Z}$, so $a + \mathbb{Z}$ contains an element l, with $0 \leq l < 1$.

Now suppose that we have $0 \leq l_1, l_2 < 1$ with l_1, $l_2 \in a + \mathbb{Z}$, then $l_1 - l_2 \in \mathbb{Z}$, so $l_1 - l_2 = n$ for some $n \in \mathbb{Z}$, but since both l_1, and l_2 are between 0 and 1, then n can only be zero , which implies that $l_1 = l_2$.

Exercise. 42

Consider a left coset $a+ < 2\pi >$ of $< 2\pi >$ in $\mathbb{R}$. The element in this cosets are all of the form $a + 2k\pi$, then for any $r \in a+ < 2\pi >$ $sin(r)$=$sin(a + 2k\pi)$ for some k , so it is equal to $sin(a)$. Then the *sine* function have the same value on all the elements of the cose t $a+ < 2\pi >$.

Exercise. 45

Let $G =< a >$ of order n. Let q be a divisor of n, and $d = \frac{n}{q}$. Now n is the smallest non zero positive integer such that $a^n = e$. Then qd is the smallest non zero positive integer such that $a^{qd} = e$, so q is the smallest non zero positive integer such that $(a^d)^q = e$. Hence a^d is an element of order q in G, which means that $< a^d >$ is a subgroup of order q in G.

Now let H be a subgroup of order q of G, H is cyclic, it is generated by an element x of G. x has the form a^i, then order of $a^i = q$, then $iq = k.n$, for some $k \in \mathbb{Z}$, $\implies i = \frac{k.n}{q} \implies i = k.d$, then $a^i = a^{k.d} = (a^d)^k$ but this implies that $a^i \in < a^d >$, then $< a^i > \subset < a^d >$, but since they have the same cardinal, then they are equal, $\implies H =< a^d >$.

Exercise. 46

Consider the group $\mathbb{Z}_n$, we know that for each d such that d divides n we have a unique subgroup of order d in $\mathbb{Z}_n$.

Now since each subgroup of $\mathbb{Z}_n$ is by itself a cyclic group of order d, then we that the number of generators of this subgroup is $\phi(d)$.

Hence since every element of $\mathbb{Z}_n$ generats some subgroup of order d dividing n , we can deduce that $\sum_{d \backslash n} \phi(d)$ counts each element of $\mathbb{Z}_n$ once, and Hence $n = \sum_{d \backslash n} \phi(d)$.

Section. 20

Exercise. 3

The generators of the multiplicative group $\mathbb{Z}_{17}$ are: 3, 5, 6, 7, 10, 11, 12, 14.

To find them you need to find first a generator, say you found 3, then since it is a cyclic group you know that all the generators are only 3^n, where n is coprime with 16 the order of the multiplicative group $\mathbb{Z}_{17}$

Exercise. 4

Notice that $3^{47} = (3^{22})^2.3^3$, and we know that $3^{22} = 3^{23-1} \equiv 1 \text{ mod}(23)$ by Fermat's little theorem, then $3^{47} \equiv 3^3 \equiv 27 \equiv 4 \text{ mod } (23)$.

Exercise. 8

We need to find $\phi(p^2)$ where p is prime. Look at all the integers $n < p^2$, suppose that $gcd(n, p^2) \neq 1$, then there exist a common divisor of n and p^2, but any divisor of p^2(and less that p^2) is a divisor of p which can only be p or 1, so we can deduce that p must be a divisor of n, (i.e. n is a multiple of p). Hence the integers $\in \{1, 2, 3..., p^2 - 1\}$ which are not coprime with p^2, are the divisors of p from $1, ..., p^2 - 1$.

Now the divisors of p are $p, 2p, 3p, ..., (p-1)p$ there number is $p - 1$.

Finally we conclude that $\phi(p^2) = p^2 - 1 - (p - 1) = p^2 - p$.

Exercise. 9

We know that the multiples of p,and q (i.e $\{p, 2p, ..., (q-1)p, q, 2q, ..., (p-1)q\}$, there number is $(p - 1) + (q - 1)$) are not coprime with pq.

Now let us prove that they are the only ones. Let n be such that $gcd(n, pq) \neq 1$, then there exist a common divisor of n, and pq call it m, since m divides pq then m must divide p or q, suppose it divides p, them m must be equal to p (since p prime), and hence p divides n, which implies that n is a multiple of p.

Then we deduce that the only elements coprime with pq are the ones which are not a multiple of p or of q, and those multiples form 2 disjoint sets of $\{1, 2, ..., pq - 1\}$.

Hence $\phi(pq) = pq - 1 - (p - 1) - (q - 1) = pq - p - q + 1$.

Exercise. 10

First notice that $7^{1000} = (7^8)^{125}$, and we know that $7^8 \equiv 1 \text{ mod}(24)$ (using Euler's theorem with $n = 24$,$\phi(24) = 8$).

Then $7^{1000} \equiv 1 \text{ mod}(24)$.

Section. 11

Exercise. 1

The elements of the group	The order of each element
(0,0)	1
(1,0)	2
(0,1)	4
(1,1)	4
(1,2)	2
(1,3)	4
(0,2)	2
(0,3)	4

So this group is not cyclic since it doesn't contain any element of order 8.

Exercise. 2

The elements of the group	The order of each element
(0,0)	1
(1,0)	3
(2,0)	3
(0,1)	4
(0,2)	2
(0,3)	4
(1,1)	12
(1,2)	6
(1,3)	12
(2,1)	12
(2,2)	6
(2,3)	12

So this group is cyclic, and it can be generated by (1,1), (1,3), (2,1), and (2,3).

Exercise. 4

We need to find the order of (2,3) in $\mathbb{Z}_6 \times \mathbb{Z}_{15}$, we know that the order of 2 in $\mathbb{Z}_6$ is 3, and the order of 3 in $\mathbb{Z}_{15}$ is 5, then order of (2,3) is $lcm(3,5) = 15$.

Exercise. 5

Similarly we can find the order of (8,10) in $\mathbb{Z}_{12} \times \mathbb{Z}_{18}$. First order of 8 in $\mathbb{Z}_{12} = \frac{12}{gcd(12,8)} = \frac{12}{4} = 3$, and order of 10 in $\mathbb{Z}_{12} = \frac{18}{gcd(18,10)} = 9$, then order of (8,10) is 9.

Exercise. 8

The greatest order in $\mathbb{Z}_n \times \mathbb{Z}_m$ is the order of (1,1), i.e it is the lcm(n,m).
So for $\mathbb{Z}_6 \times \mathbb{Z}_8$, the greatest order is 24.
And for $\mathbb{Z}_{12} \times \mathbb{Z}_{15}$, the greatest order is 60.