Math 241

Problem Set 3 solution manual

Exercise. A3.1

Let $a, b \in \mathbb{Z}^+$.

a- $a\mathbb{Z}$, and $b\mathbb{Z}$ are both subgroups of $\mathbb{Z}$, so by previous ex (section 5, ex: 54) we have that their intersection is a subgroup of $\mathbb{Z}$.

Consider the element $a.b \neq 0$, $a.b \in a\mathbb{Z}$, and $a.b \in a\mathbb{Z}$, so $a.b \in a\mathbb{Z} \cap b\mathbb{Z}$.

So we have $a\mathbb{Z} \cap b\mathbb{Z}$ is a non-empty subgroup of $\mathbb{Z}$

b- we have $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$, we are required to show that m=LCM(a, b).

$m \in a\mathbb{Z}$ then m is a multiple of a, similarly it is a multiple of b. So m is a common multiple of a and b.

Now let n¿0 be such that n is a common multiple of a and b.

Then $n \in a\mathbb{Z}$ and $n \in b\mathbb{Z}$, $\implies$ $n \in$ $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$ $\implies$ $n < m$ (since both are positive and m is smallest positive integer in $m\mathbb{Z}$).

So m is the smallest common multiple of a and b.

c- Let c be a common multiple of a and b, then $c \in a\mathbb{Z}$, and $c \in b\mathbb{Z}$ $\implies$ $c \in m\mathbb{Z}$ $\implies$ c is a multiple of m.

d- $d = GCD(a, b)$. $a^{'}d = a$ and $b^{'}d = b$.

$GCD(a^{'}, b^{'})$=1 $\implies$ $\exists$ k_1, $K_2 \in \mathbb{Z}$ such that $a^{'}k_1 + b^{'}k_2 = 1$. Now multiply both side by $m = LCM(a, b)$, we get:
$ma^{'}k_1 + mb^{'}k_2 = m$ $(\star)$.

Now notice that since m is the LCM of a, and b then $m = ac_1$, and $m = bc_2$
then replace them in $(\star)$ we get : $m = c_2ba^{'}k_1 + c_1ab^{'}k_2$.
But $ba^{'} - db^{'}a^{'} = ab^{'}$. so we get : $m = da^{'}b^{'}c_2k_1 + da^{'}b^{'}c_1k_2 = da^{'}b^{'}(c_1k_2 + c_2k_1)$.
implies m is a multiple $da^{'}b^{'}$.

On the other hand $da^{'}b^{'} = ab^{'}$, so $da^{'}b^{'}$ is a multiple of a , similarly $da^{'}b^{'}$ is a multiple of b, then by part (c) we get that $da^{'}b^{'}$ is a multiple of m.

But two positive number are multiples of each other only if they are equal, so we get $m = da^{'}b^{'}$.

Finally : multiply by d on both sides of the relation $m = da^{'}b^{'}$ we get $md = a.b$, $\implies$ $m = \frac{ab}{d}$
$\implies$ $LCM(a, b)$=$\frac{ab}{GCD(a,b)}$.

Section. 6

Exercise. 53

G is cyclic $\implies$ G is generated by one element (i.e $G =< g >$ for some $g \in G$).

Let $x \in G$, be such that $x^m = e$, then since $x \in G$ we can write $x = g^i$ for some $i \in \{0, 1, .., n-1\}$.

Then we have $(g^i)^m = e \implies g^{im} = e$, but since g is the generator of G and is of order n, then n is the smallest power of g such that g raised to this power is e, and any other power k such that $g^k = e$ should be a multiple of n.

And from this we deduce that im is a multiple of n, so $im = kn$ for some $k \in \mathbb{Z} \implies i = \frac{kn}{m}$ (note that this fraction is still in $\mathbb{Z}$ since m divides n).

Finally the set of solutions of $x^m = e$ is $\{g^i \mid i = \frac{kn}{m}, k \in \mathbb{Z}\}$=$\{g^{\frac{kn}{m}} \mid k \in \{0, 1, 2..(m-1)\}\}$. Since for $i = \frac{kn}{m}$ with $k > m$, we can write $k = b.m + r$ with $b \in \mathbb{Z}$ and $0 \leq r < m$, then $\frac{kn}{m} = \frac{(b.m+r)n}{m} = b.n + \frac{rn}{m}$, and then $g^i = g^{\frac{r.n}{m}}$ which belong to the set described above.

So the number of solutions of the equation $x^m = e$ is m.

Exercise. 56

a- Let $H =< h >$ and $K =< k >$ be two cyclic subgroups of G generated by h of order r, and k of order s respectively.

Note that since G is commutative $(ab)^n = (ab)(ab)...(ab) = (a.....a)(b.....b) = a^n b^n$.

We need to find a subgroup of G of order rs.

Consider the subgroup L generated by the element hk (i.e $L =< hk >$).

L is a cyclic subgroup of G of order equal the order of the element hk.

We know that $(hk)^{rs} = h^{rs}k^{rs} = (h^r)^s(k^s)^r = e$, in order to have order of hk equal rs we must prove that rs is the smallest positive integer i such that $(hk)^i = e$.

Let n be such that $(hk)^n = e$, we will show that $n \geq rs$. $(hk)^n = h^n k^n = e \implies h^n = k^{-n} \implies h^n \in < k >$, and $h^n = k^{s-n}$.

Let j be the order of h^n, since $h^n \in < k >$, j is equal to $\frac{s}{GCD((s-n),s)} \implies j$ divides s, similarly j divides $r \implies j = 1$, since r and s are relatively prime. So $h^n = e \implies n$ is a multiple of r.

In a similar way we can prove that n is a multiple of s.

Finally since r and s are relatively prime, there LCM is rs (by A3.1) and then $n \in rs\mathbb{Z}$, $\implies n \geq rs$.

So the order of hk is rs.

b- Now we have the same elements given above but this time r and s are not relatively prime.

Factorize r and s into powers of primes. That is write $r = p_1^{e_1}....p_t^{e_t}$ and $s = p_1^{f_1}....p_t^{f_t}$ where the e_i, f_i are ≥ 0.

Then the $lcm(r, s) = \Pi p_i^{c_i}$ where $c_i = max(e_i, f_i)$.

Then we choose the following elements according to the following:

$$\begin{cases} if \quad c_i = e_i \quad let \quad\ a_i = x^{(\prod\limits_{j \neq i} p_j^{e_j})}. \\ if \quad c_i = f_i \quad let \quad a_i = y^{(\prod\limits_{j \neq i} p_j^{f_j})}. \end{cases}$$

Note that the order of each a_i is $p_i^{c_i}$

Then the elements a_i have their orders pair wise relatively prime, so repeating part a) successively we get that Πa_i is of order $\Pi p_i^{c_i} = lcm(r,s)$. For example :

Suppose

$r = 2^3 3^2 5 = 2^3 3^2 5^1 11^0$,

$s = 2^2 3^7 11 = 2^2 3^7 5^0 11^1$,

so $lcm(r,s) = 2^3 3^7 5^1 11^1$.

Then since x has order r, we define

$x' = x^{(3^2 5)}$ which has order 2^3

$y' = y^{(2^2 11)}$ which has order 3^7

$x'' = x^{(2^3 3^2)}$ which has order 5

$y'' = y^{(2^2 3^7)}$ which has order 11.

Note that we have separated the powers of the primes $2, 3, 5, 11$ that occur. These powers are pair wise relatively prime. Now by repeated application of part a, we obtain that $x'y'x''y''$ has order $2^3 3^7 511 = lcm(r,s)$.

Section. 8

Exercise. 1

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix}$$

Exercise. 4

$$\sigma^{-1}\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 6 & 2 & 4 & 3 \end{pmatrix}$$

Exercise. 5

$$\sigma^{-1}\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 5 & 4 & 3 \end{pmatrix}$$

τ=(1243)(56).
$\sigma^{-1}\tau{-}1$=(1263)(45).

Exercise. 6

σ=(134562), $\implies$ σ is a cycle of order 6, then the order of σ is 6.

Exercise. 7
τ=(14)(23), so τ is the product of two disjoint transpositions, so the order τ is 2.

Exercise. 8

$$\sigma^{100} = (\sigma^6)^{16}.\sigma^4 = \sigma^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 1 & 3 & 4 \end{pmatrix}$$

Exercise. 16

$\{\sigma \in S_4 \mid \sigma(3) = 3\}$.

Note that this set contains all the permutations of {1,2,3,4} which keep the element 3 untouched, so it is like we are permuting the three elements 1,2,4. Then the number of elements of this set is 3!=6.

Exercise. 21

a- Applying the matrices to the vector $\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$ we get all the possible permutations of the columns of this vector.

Moreover, the product of two matrices is the compositions of two permutation of the columns of the vector which is again a permutation.

Then this set of matrices form a group under matrix multiplication, where the identity element is I_3.

b- This group of matrices is isomorphic to S_3 since it is permuting the 3 columns of a vector, similar to S_3 which permutes the three elements of a set.

So one can simply find an isomorphism between them.

Exercise. 46

Consider σ_1 and $\sigma_2 \in S_n$, since $n \geq 3$ we can consider three distinct elements denote them by 1,2,3. Now let σ_1=(123), and $\sigma_2 = (13)$.

Then $\sigma_1\sigma_2(1) = 1$, but $\sigma_2\sigma_1(1) = 2$, so they don't commute $\implies$ S_n is not abelian

Section. 9

Exercise. 7

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 3 & 5 & 8 & 6 & 2 & 7 \end{pmatrix}$$

Exercise. 13

a- σ=(1 4 5 7), we can easily notice that σ^4=id , then the order of σ=4.

b- The order of a cycle of length m is m.

c- σ=(4 5)(2 3 7) , then σ^6=id , so the order of σ=4.

τ=(1 4)(3 5 7 8), then τ^8=id , so the order of τ=8.

d- for exercise 10: the order is 6, for exercise 11 order is 6, and for exercise 12 order is 8.

e- Any permutation expressed as the product of disjoint cycles has its order the lcm of the length of those cycles.

Exercise. 39

Lemma 1.

Let $(a_1a_2...a_m)$ with $m \leq n$ be a cycle, and let f be any permutation in S_n. Then $f^r(a_1a_2...a_m)f^{-r} = (f^r(a_1)f^r(a_2)...f^r(a_m))$.

Proof:

We prove it by induction on r: basic step: for r=1: $\sigma_1 = f(a_1a_2...a_m)f^{-1}$, and $\sigma_2 = (f(a_1)f(a_2)...f(a_m))$ let x be any number between 1 and n , we have 2 cases:

there exist a_i such that $x = f(a_i)$ then we get $\sigma_1(x) = \sigma_1(f(a_i)) = f(a_{i+1})$, and $\sigma_2(f(a_i)) = f(a_{i+1})$, so they are equal.

Or there exist no a_i such that $x = f(a_i)$ then $f^{-1}(x) \notin \{a_i \mid i = 1, ..., m\}$, so we get $\sigma_1(x) = x$, and $\sigma_2(x) = x$.

Hence σ_1 and σ_2 are equal for all $x \in \{1, ..., n\}$.

Inductive step: Suppose it is true up to $r - 1$, and let us prove it for r .

$\sigma_1 = f^r(a_1a_2...a_m)f^{-r}$, and $\sigma_2 = (f^r(a_1)f^r(a_2)...f^r(a_m))$.

Then $\sigma_1 = f^r(a_1a_2...a_m)f^{-r} = f.f^{r-1}(a_1a_2...a_m)f^{-(r-1)}f^{-1} = f(f^{r-1}(a_1)f^{r-1}(a_2)...f^{r-1}(a_m))f^{-1} = (f^r(a_1)f^r(a_2)...f^r(a_m)) = \sigma_2$, where in the last step we use the same argument as for the base step but for the cycle $(f^{r-1}(a_1)f^{r-1}(a_2)...f^{r-1}(a_m))$.

then we now have : $f^r(a_1a_2...a_m)f^{-r} = (f^r(a_1)f^r(a_2)...f^r(a_m))$

Lemma 2.

The transposition (i j)=(i k)(j k)(i k) for any k not equal to i and j, and hence we can deduce that any transposition can be written as the product of adjacent transpositions.

Proof:

easily one can check $(ij) = (ik)(jk)(ik)$, and now to deduce the second part of the lemma we can do it by induction on the difference between i, and j in (ij):

Base step: if $|i - j| = 1$, we are done since (ij) will be an adajcent transposition.

Inductive step step: suppose it is true for $|i - j| = k - 1$ $(k < n)$, let us prove it for $|i - j| = k$

Without loss of generality we can assume $i > j$, then write $(i\ j)$=$(i\ i+1)(j\ i+1)(i\ i+1)$, now by given of induction we can write $(j\ i+1)$ as the product of adjacent transpositions (since $|j - i + 1| = k - 1$) , so (ij) can be written as the product of adjacent transpositions.

Now the exercise :

From lemma 1 , we can easily deduce that $(12...n)^r(12)(12...n)^{n-r}$ will generate all adjacent transpositions. (Notice that $(12...n)^{n-r} = (12...n)^{-r}$ since $(12...n)$ is of order n)

Then from lemma 2 and from the fact that any permutation can be written as the product of transpositions, then any permutation can be expressed as the product of the two elements given by the exercise.