Math 241

Problem Set 2 solution manual

Exercise. A2.1
Required to show that x and axa^{-1} have the same order.

Lemma.
- $(axa^{-1})^n = a.x^n.a^{-1}$.
- $aba^{-1} = 1 \Leftrightarrow b = 1$

proof. -we have : $(a.x.a^{-1})^n = (a.x.a^{-1}).(a.x.a^{-1})....(a.x.a^{-1}) = a.x.(a^{-1}.a).x.(a^{-1}.a)....(a^{-1}.a).x.a^{-1}$
$= a.x^n.a^{-1} = a.e.a^{-1} = e$
-$(aba^{-1}) = 1 \Leftrightarrow ab = a \Leftrightarrow b = a^{-1}a \Leftrightarrow b = 1$.

- Case 1 :x has a finite order
  Using the above lemma we conclude that:
  $\{n \mid (axa^{-1})^n = e\} = \{n \mid x^n = e\}$. Since the order of x is the smallest positive integer n such that $x^n = e$, we conclude that x and axa^{-1} have the same order.
- Case 2 : order of x is infinite.
  $< x >= \{ \ x^n \quad n \in \mathbb{N} \ \}$.
  Suppose that $a.x.a^{-1}$ have a finite order. $\implies$ there exists $n \in \mathbb{N}$ such that $(a.x.a^{-1})^n = e$.
  but this implies that $x^n = e$ which contradicts the fact that x has an infinite order.

Exercise. A2.2
Note That in this exercise $(a, b)^n$ is just $(a, b) + (a, b) + ... + (a, b)$ n-times.
Consider the element $(1, 1) \in \mathbb{Z}_3 \times \mathbb{Z}_4$.
$(1, 1)^{12} = (12, 12) = (0, 0)$. We still need to show that 12 is the least integer $n \in \mathbb{N}$ such that $(1, 1)^n = (0, 0)$.
Let $n \in \mathbb{N}^*$ be such that $(1, 1)^n = (0, 0)$.
$\implies$ $(n, n) = (0, 0)$
$\implies$ $n = 0$ in $\mathbb{Z}_3$, and $n = 0$ in $\mathbb{Z}_4$.
$\implies$ n is a common multiple of 3 and 4, but the smallest positive common multiple of 3 and 4 is 12, so n must be greater than or equal 12.
Hence the order of $(1, 1)$ is 12 .

Section. 4 :

Exercise. 32:
G is a group such that $x \star x = e$ for all $x \in G$, where e is the identity element of G.
Notice that $x \star x = e \implies x = x^{-1}$ for all $x \in G$.
$\implies$ $(a \star b) \star (a \star b) = e$
$\implies$ $(a \star b) \star (a \star b) \star (b^{-1} \star a^{-1}) = b^{-1} \star a^{-1}$
$\implies$ $(a \star b) \star a \star (b \star b^{-1}) \star a^{-1} = b^{-1} \star a^{-1}$
$\implies$ $(a \star b) \star (a \star a^{-1}) = b^{-1} \star a^{-1}$
$\implies$ $(a \star b) = b^{-1} \star a^{-1} = b \star a$

OR you can do the following:

Lemma. $(ab)^{-1} = b^{-1}a^{-1}$.

proof. $ab.(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a.1.a^{-1} = 1$.

Now the solution would be like: $(a \star b) \star (a \star b) = e \implies (a \star b) \star (a \star b) \star (a \star b)^{-1} = (a \star b)^{-1}$ $(a \star b) = b^{-1} \star a^{-1} = b \star a$

Exercise. 33:
We proceed by induction on n.
Base step: For $n = 1$ $(a \star b)^1 = a^1 \star b^1$. so it is true for $n = 1$.

Inductive step: suppose it is true for n, then we have $(a \star b)^n = a^n \star b^n$.
Required to show that $(a \star b)^{n+1} = a^{n+1} \star b^{n+1}$
$(a \star b)^{n+1} = (a \star b)^n \star (a \star b)$
$= a^n \star b^n \star (a \star b)$
$= a^n \star b^n \star (b \star a)$
$= a^n \star (b^n \star b) \star a)$
$= a^n \star (b^{n+1} \star a)$
$= (a^n \star a) \star b^{n+1})$
$= a^{n+1} \star b^{n+1}$.
So it is true for $n + 1$. Finally by induction we have it true for all n.

Exercise. 37:
G is a group. Given $a \star b \star c = e$, e being the identity of G, and a, b and $c \in G$.
$a \star b \star c = e \implies a \star (b \star c) = e$ which implies that $b \star c = a^{-1}$.
Then $b \star c \star a = (b \star c) \star a = e$.

Section. 5 :
For exercises 22, 23, 24, 33, and 34 we have:
The subgroup generated by any element $a \in GL(2, \mathbb{R})$ or $\in GL(4, \mathbb{R})$ is $\{ \ a^n \mid n \in \mathbb{Z} \ \}$.

Exercise. 22: $a = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$.
Note that:
$a^2 = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.
and consequently any power of a is either a or the identity element. So the subgroup generated by a contains only a and I_2. then $< a >= \{I_2, a\}$.

Exercise. 23:
$a = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.
Note that:
$a^2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$.
Let us prove that $a^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$.
For $n = 2$ it is true (proved above).
Suppose true for n, and let us prove it for $n + 1$.
$a^{n+1} = a^n.a = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & n+1 \\ 0 & 1 \end{bmatrix}$. The above result is also true for $n < 0$,since
$a^{-1} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$, and we proceed again by induction.
So $< a >= \{ \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \mid n \in \mathbb{Z} \}$.

Exercise. 24: Similarly we can prove by induction that for $a = \begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix}$.
$< a >= \{ \begin{bmatrix} 3^n & 0 \\ 0 & 2^n \end{bmatrix} \mid n \in \mathbb{Z} \}$.

Exercise. 33:

$$a = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

Note that $a^2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$.
So the subgroup generated by a is $< a >= \{ I_4, a \}$.
Note that $a = P_{(1,3)(2,4)}$

Exercise. 34:
$a = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$
we have $a^2 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$.

$$a^3 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

$$a^4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = I_4.$$

This implies that a is of order 4, and the subgroup generated by a is $< a >= \{ I_4, a, a^2, a^3 \}$.
Note that $a = P_{(1324)}$

Exercise. 42:
G is a cyclic group, $\implies \exists\, a \in$ G such that G=$< a >$. ϕ : G $\longrightarrow$ G' is an isomorphism.
Claim: G'=$< \phi(a) >$.

- $\phi(a) \in G' \implies < \phi(a) > \subseteq G'$.
- Let b'$\in G'$. Then since ϕ is an isomorphism $\exists$ an element $b \in$ G such that $\phi(b) = b$'.
  But $b \in G \implies b = a^n$ for some $n \in \mathbb{Z}$.
  $\implies b$'$=\phi(a^n) = (\phi(a))^n$ (since ϕ is a homomorphism)
  $\implies b$'$\in< \phi(a) >$.
  Then the above paragraph shows G'$\subseteq< \phi(a) >$.

So we have G'$=< \phi(a) >$, So G' is cyclic.

Exercise. 51:
G is a group, and a is a fixed element $\in G$.
$H_a = \{ x \in \text{G} \mid xa = ax \}$.
Required to prove H_a subgroup of G.

- $ea = ae$ for e being the identity element of G, then $e \in H_a$.
- suppose x, $y \in H_a$ then $xa = ax$, and $ya = ay$,
  then $(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy)$. So $xy \in H_a$.
- for $x \in H_a$, $ax = xa \implies a = xax^{-1} \implies x^{-1}a = ax^{-1}$. $\implies x^{-1} \in H_a$.

Then H_a is a subgroup of G.

Exercise. 54:
H and K are two subgroups of G , required to show that $H \cap K$ is a subgroup of G.

- $e \in H$
  $e \in K$
  $\implies e \in H \cap K$.

- Let x and $y \in H \cap K$. Then x and $y \in H$ and K
  Then $x.y \in H$, and $x.y \in K$. $\implies x.y \in H \cap K$.

- Let $x \in H \cap K$. Then $x \in H$, and $x \in K$, $\implies x^{-1} \in H$ and $x^{-1} \in K$.
  $\implies x^{-1} \in H \cap K$.

So we have $H \cap K$ a subgroup of G.

Section. 6

Exercise. 18:
The cyclic subgroup generated by 30 in $\mathbb{Z}_{42}$ is of order 7 : -We can either find the elements of $< 30 >$ by successive addition to get that:
$< 30 > =$\{ 0, 30, 18, 6, 36, 24, 12 \}.
-Or we can use the fact that $| < 30 > |=\frac{42}{G.C.D(30,42)} = \frac{42}{6} = 7$.

Exercise. 22:
$\mathbb{Z}_{12}$ is a cyclic group, so all its subgroups are cyclic. So the subgroups of $\mathbb{Z}_{12}$ are $< a >$ for $a \in \mathbb{Z}_{12}$.

- For $a = 1, 5, 7, 11$, we have $G.C.D(a, 12) = 1$, so $< a >=\mathbb{Z}_{12}$.

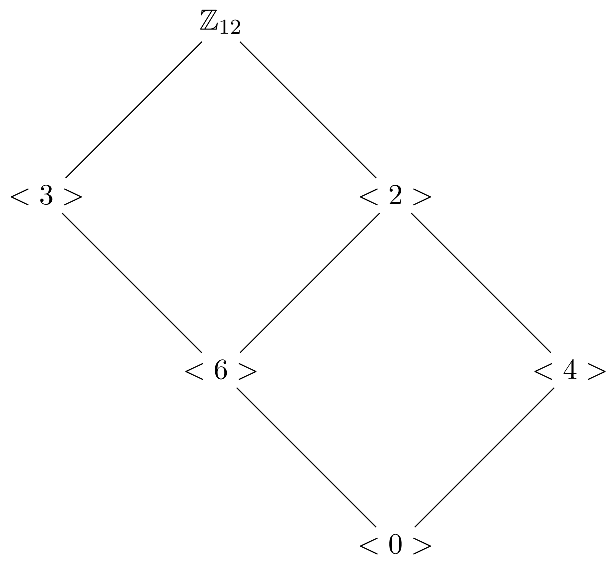
- For $a = 2$, $< 2 >= \{ 0, 2, 4, 6, 8, 10 \} =< 10 >$

- For $a = 3$, $< 3 >= \{ 0, 3, 6, 9 \} =< 9 >$

- For $a = 4$, $< 4 >= \{ 0, 4, 8 \} =< 8 >$

- For $a = 6$, $< 6 >= \{ 0, 6 \}$.

The diagrame of subgroups is:



Exercise. 29:
The subgroups of $\mathbb{Z}_{17}$ are only the cyclic subgroups generated by its elements.
But since for every $a \in \mathbb{Z}_{17}^*$ $GCD(a, 17) = 1$, then $< a >= \mathbb{Z}_{17}$ for all $a \neq 0$. So the only possible orders of subgroups of $\mathbb{Z}_{17}$ are 1, and 17.