Math 3101 HW # 3

Mario L. Gutierrez Abed

Section 5

(#36)

a) Complete the following table to give the group $\mathbb{Z}_6$ of 6 elements.

$\mathbb{Z}_6+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

.

b) Compute the subgroups $\langle 0\rangle$, $\langle 1\rangle$, $\langle 2\rangle$, $\langle 3\rangle$, $\langle 4\rangle$, and $\langle 5\rangle$ of the group $\mathbb{Z}_6$ given in part a).

Solution:

- $\langle 0\rangle = \{0^n : n \in \mathbb{Z}\} = \{n \cdot 0 : n \in \mathbb{Z}\} = \{0\}$.
- $\langle 1\rangle = \{1^n : n \in \mathbb{Z}\} = \{n \cdot 1 : n \in \mathbb{Z}\} = \{1, 2, 3, 4, 5, 0\} = \mathbb{Z}_6$.
- $\langle 2\rangle = \{2^n : n \in \mathbb{Z}\} = \{n \cdot 2 : n \in \mathbb{Z}\} = \{2, 4, 0\}$.
- $\langle 3\rangle = \{3^n : n \in \mathbb{Z}\} = \{n \cdot 3 : n \in \mathbb{Z}\} = \{3, 0\}$.
- $\langle 4\rangle = \{4^n : n \in \mathbb{Z}\} = \{n \cdot 4 : n \in \mathbb{Z}\} = \{4, 2, 0\} = \langle 2\rangle$.
- $\langle 5\rangle = \{5^n : n \in \mathbb{Z}\} = \{n \cdot 5 : n \in \mathbb{Z}\} = \{5, 4, 3, 2, 1, 0\} = \langle 1\rangle = \mathbb{Z}_6$.

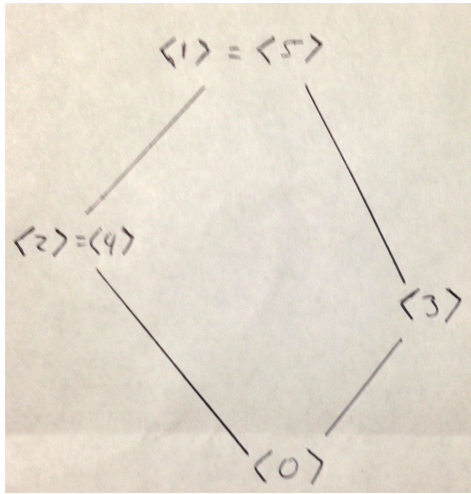
c) Which elements are generators for the group $\mathbb{Z}_6$ of part a)?

Solution:

The generators of $\mathbb{Z}_6$ are the nonzero elements $a \in \mathbb{Z}_6$ such that $\gcd(a, 6) = 1$. The only elements in $\mathbb{Z}_6$ that are relatively prime to 6 are 1 and 5, hence these are the generators.

d) Give the subgroup diagram for the part b) subgroups of $\mathbb{Z}_6$. (We will see later that these are all the subgroups of $\mathbb{Z}_6$.)

Solution:



(#40) Show by means of an example that it is possible for the quadratic equation $x^2 = e$ to have more than two solutions in some group G with identity e.

Solution:
Take the Klein 4-group for example ($V = \{a, b, c, e\}$ with the property $a^2 = b^2 = c^2 = e$), where the equation $x^2 = e$ has all four elements of the group as solutions, i.e. $x = a, x = b, x = c$.

(#42) Let $\phi : G \longrightarrow G'$ be an isomorphism from a group $\langle G, *\rangle$ to a group $\langle G', *'\rangle$. Prove that if G is cyclic, then G' is also cyclic.

Proof:
Let G be cyclic. Then there exists $a \in G$ such that $G = \langle a \rangle = \{a^n : n \in \mathbb{Z}^+\}$. We claim that $\phi(a)$ is a generator for G'. Now let $b = a^m$ for some $m \in \mathbb{Z}^+$ be any element in G. Since ϕ is an isomorphism, it is onto, thus we are guaranteed the existence of some $b' \in G'$ such that that $b' = \phi(b) = \phi(a^m)$.
But then

$$\begin{aligned}\phi(a^m) &= \phi(\underbrace{a * a * \ldots * a}_{m\text{ times}})\\ &= \underbrace{\phi(a) *' \phi(a) *' \ldots *' \phi(a)}_{m\text{ times}} \quad \text{(by the homomorphic property)}\\ &= [\phi(a)]^m .\end{aligned}$$

Hence we have shown that $G' = \langle \phi(a) \rangle = \{[\phi(a)]^m : a \in G,\ m \in \mathbb{Z}^+\}$, which proves that G' is cyclic. ■

Section 6

In exercises 33-37, either give an example of a group with the property described, or explain why no example exists:

(#33) A finite group that is not cyclic.

Solution:
The Klein 4-group is not cyclic because there is no element $x \in V$ such that $\langle x \rangle = \{a, b, c, e\}$.
That is

$$\langle a \rangle = \{a, e\} \neq \{a, b, c, e\}$$
$$\langle b \rangle = \{b, e\} \neq \{a, b, c, e\}$$
$$\langle c \rangle = \{c, e\} \neq \{a, b, c, e\}$$

(#34) An infinite group that is not cyclic.

Solution:
$\langle \mathbb{R}, + \rangle$ is not cyclic because there's no single element $a \in \mathbb{R}$ such that $\mathbb{R} = \langle a \rangle$. Assume to the contrary that such element a exists. Then $a^m, a^{m+1} \in \mathbb{R}$, where

$$a^m = \underbrace{a + a + \ldots + a}_{m \text{ times}} = m \cdot a$$

and

$$a^{m+1} = \underbrace{a + a + \ldots + a}_{m+1 \text{ times}} = (m+1) \cdot a$$

But since $\mathbb{R}$ is a connected, perfect topological space, it cannot contain any isolated points. Hence, we may pick an ε-neighborhood B_ε that covers a^m and another ε-neighborhood V_ε about a^{m+1}, and we are guaranteed the existence of some $x \in \mathbb{R}$ such that

$$x \in B_\varepsilon \bigcup V_\varepsilon \qquad \text{or} \qquad \sup\{y : y \in B_\varepsilon\} < x < \inf\{y : y \in V_\varepsilon\}.$$

In either case we have that $a^m < x < a^{m+1}$. $(\Rightarrow\Leftarrow)$
This proves that $\langle \mathbb{R}, + \rangle$ is not cyclic.

(#35) A cyclic group having only one generator.

Solution:
$\mathbb{Z}_2 = \{0, 1\}$, where the generator is $\langle 1 \rangle$.

(#36) An infinite cyclic group having four generators.

Solution:
No such example exists. Every infinite cyclic group is isomorphic to $\langle \mathbb{Z}, + \rangle$, which has just two generators (namely 1 and -1). Since isomorphic cyclic groups must have the same number of generators, we have shown that no infinite cyclic group having four generators can possibly exist.

(#37) A finite cyclic group having four generators.

Solution:
$\mathbb{Z}_8$ is such a group. The generators of $\mathbb{Z}_8$ are the nonzero elements $a \in \mathbb{Z}_8$ such that $\gcd(a, 8) = 1$. The elements in $\mathbb{Z}_8$ that are relatively prime to 8 are $1, 3, 5$, and 7, hence these are the generators.

Section 8

In exercises 1-5, compute the indicated product involving the following permutations in S_6:

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

(#1) $\tau\sigma$

Solution:

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

(#2) $\tau^2\sigma$

Solution:

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

(#3) $\mu\sigma^2$

Solution:

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

(#4) $\sigma^{-2}\,\tau$

Solution:

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

(#5) $\sigma^{-1}\,\tau\,\sigma$

Solution:

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

(#18) Consider the symmetric group S_3 (the group of all permutations of a set of three elements). Let $A = \{1,\ 2,\ 3\}$, then we list all 3! permutations of A and assign to each a subscripted Greek letter for a name.
That is, let

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

The multiplication (composition) table for S_3 is given by

$\circ$	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

** Note that this group is not abelian. It turns out that S_3 has minimum order for any nonabelian group. That is, if G is some nonabelian group, then $|G| \geq 6$. **

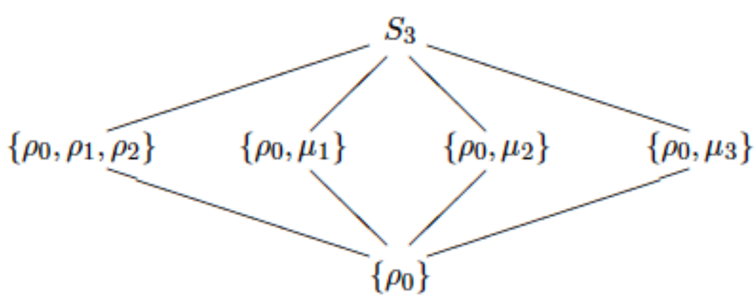
a) Find the cyclic subgroups $\langle\rho_1\rangle$, $\langle\rho_2\rangle$, and $\langle\mu_1\rangle$ of S_3.

Solution:

- $\langle\rho_1\rangle = \{\rho_1^n : n \in \mathbb{Z}\} = \{\rho_1, \rho_2, \rho_0\}$
- $\langle\rho_2\rangle = \{\rho_2^n : n \in \mathbb{Z}\} = \{\rho_2, \rho_1, \rho_0\} = \langle\rho_1\rangle$
- $\langle\mu_1\rangle = \{\mu_1^n : n \in \mathbb{Z}\} = \{\mu_1, \rho_0\}$

b) Find all subgroups, proper and improper of S_3 and give the subgroup diagram for them.

Solution:



(#36) Show by an example that every proper subgroup of a nonabelian group may be abelian.

Solution:

The nonabelian group presented in exercise 18, S_3, is such an example. To see why take each of its proper subgroups

$$\{\rho_0\},\ \{\rho_0, \mu_1\},\ \{\rho_0, \mu_2\},\ \{\rho_0, \mu_3\},\ \{\rho_0, \rho_1, \rho_2\},$$

which are of order 1, 2, 2, 2, and 3, respectively. Since the minimum order for any nonabelian group is 6, we can see that all of the proper subgroups of the nonabelian group S_3 are abelian.