Homework 3

Aleck Zhao

September 23, 2016

Section 1.4: Permutations

6. If σ and τ fix k, show that $\sigma\tau$ and σ^{-1} both fix k.

   Proof. Since σ and τ both fix k, we have $\sigma k = k$ and $\tau k = k$, so that $\sigma\tau k = \sigma(\tau k) = \sigma k = k$, so then $\sigma\tau$ fixes k as well.
   Since $\sigma k = k$, multiplying by σ^{-1} on the left, we have $\sigma^{-1}\sigma k = \sigma^{-1} k \implies k = \sigma^{-1} k$, so σ^{-1} fixes k, as desired. $\square$

12. Let $\sigma = (1 \quad 2 \quad 3)$ and $\tau = (1 \quad 2)$ in S_3.

   (a) Show that $S_3 = \{\varepsilon, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$ and that $\sigma^3 = \varepsilon = \tau^2$ and $\sigma\tau = \tau\sigma^2$.

   Proof. We know that

$$S_3 = \{\varepsilon, (1 \quad 2 \quad 3), (1 \quad 3 \quad 2), (1 \quad 2), (1 \quad 3), (2 \quad 3)\}.$$

   Note that trivially, $\varepsilon, \sigma, \tau$ are in S_3.
   Write

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

   Then we have

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1 \quad 3 \quad 2)$$
$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2 \quad 3)$$
$$\tau\sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1 \quad 3)$$

   Thus S_3 is as desired.
   We have

$$\sigma^3 = \sigma\sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \varepsilon$$
$$\tau^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \varepsilon$$
$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \tau\sigma^2$$

   as desired. $\square$

(b) Use (a) to fill in the multiplication table for S_3.

Solution. The Cayley table is as follows:

S_3	ε	σ	σ^2	τ	$\tau\sigma$	$\tau\sigma^2$
ε	ε	σ	σ^2	τ	$\tau\sigma$	$\tau\sigma^2$
σ	σ	σ^2	ε	$\tau\sigma^2$	τ	$\tau\sigma$
σ^2	σ^2	ε	σ	$\tau\sigma$	$\tau\sigma^2$	τ
τ	τ	$\tau\sigma$	$\tau\sigma^2$	ε	σ	σ^2
$\tau\sigma$	$\tau\sigma$	$\tau\sigma^2$	τ	σ^2	ε	σ
$\tau\sigma^2$	$\tau\sigma^2$	τ	$\tau\sigma$	σ	σ^2	ε

□

16. If $\sigma = (1 \quad 2 \quad 3 \quad \cdots \quad n)$, show that $\sigma^n = \varepsilon$ and that n is the smallest positive integer with this property.

Proof. We may define σ as $\sigma k = (k+1) \pmod n$ whenever $k \in \sigma$. This accounts for looping. Then $\sigma^2 k = \sigma(\sigma k) = (k+2) \pmod n$, and by induction, we have $\sigma^n k = (k+n) \pmod n \equiv k \pmod n$. Thus σ^n fixes k so it is the identity permutation, as desired.

It is the smallest positive integer with this property because $(k+x) \equiv k \pmod n$ is satisfied whenever $n|x$, so $x = n$ is the smallest.

□

Section 2.1: Binary Operations

1. In each case a binary operation $*$ is given on a set M. Decide whether it is commutative or associative, whether a unity exists, and find the units (if there is a unity).

(c) $M = \mathbb{R}; a * b = a + b - ab$

Solution. We have $a + b - ab = b + a - ba$, so $a * b = b * a$ thus $*$ $\boxed{\text{is commutative.}}$
We have

$$a * (b * c) = a * (b + c - bc) = a + b + c - bc - a(b + c - bc) = a + b + c - ab - ac - bc + abc$$
$$(a * b) * c = (a + b - ab) * c = a + b - ab + c - c(a + b - ab) = a + b + c - ab - ac - bc + abc$$

thus $*$ $\boxed{\text{is associative.}}$
If a unity i exists, it must satisfy $a * i = i * a = a$ for all a. This means that $a + i - ai = a$, so $i - ai = i(1-a) = 0$ for all a, so $\boxed{\text{0 is a unity.}}$ Since $*$ is commutative this follows in the other direction as well.
Let a be a unit, so that b is its inverse. Then $a * b = a + b - ab = i = 0$. Manipulating this equation, we have

$$\begin{aligned} ab - a - b &= 0 \\ ab - a - b + 1 &= 1 \\ (a-1)(b-1) &= 1 \\ b - 1 &= \frac{1}{a-1} \\ b &= 1 + \frac{1}{a-1} = \frac{a}{a-1} > 0 \end{aligned}$$

thus $\boxed{\text{all elements are units.}}$

□

(g) $M = \mathbb{N}^+; a * b = \gcd(a, b)$

Solution. We have $\gcd(a, b) = \gcd(b, a)$, so $a * b = b * a$ thus $*$ $\boxed{\text{is commutative.}}$
In Homework 2, Section 1.2 #42 we showed that $\gcd(a, b, c) = \gcd(a, \gcd(b, c))$, so it follows that

$$\gcd(a, \gcd(b, c)) = \gcd(a, b, c) = \gcd(\gcd(a, b), c),$$

so $a * (b * c) = (a * b) * c$, thus $*$ $\boxed{\text{is associative.}}$
There does not exist a unity. Suppose there did exist a unity i, then $a * i = \gcd(a, i) = a$ for all $a \in M$. However, this means that i is divisible by every natural number, which is impossible (since 0 is excluded from M). Thus there is $\boxed{\text{no unity.}}$

$\square$

5. Given an alphabet A, call an n-tuple $(a_1, a_2, \cdots, a_n)$ with $a_i \in A$ a word of length n from A and write it as $a_1 a_2 \cdots a_n$. Multiply two words by $(a_1 a_2 \cdots a_n) \cdot (b_1 b_2 \cdots b_m) = a_1 a_2 \cdots a_n b_1 b_2 \cdots b_m$, and call this product juxtaposition. We decree the existence of an empty word λ with no letters. Show that the set W of all words from A is a monoid, noncommutative if $|A| > 1$, and find the units.

Proof. For a set to be a monoid, its binary operation must be associative and it must have a unity. Obviously if we take two words from W and juxtapose them, the result will still be a word in W, so W is closed under juxtaposition.

Let X, Y, Z be words with

$$\begin{aligned} X &= x_1 x_2 \cdots x_i \\ Y &= y_1 y_2 \cdots y_j \\ Z &= z_1 z_2 \cdots z_k \end{aligned}$$

Then

$$\begin{aligned} X \cdot (Y \cdot Z) &= X \cdot (y_1 y_2 \cdots y_j z_1 z_2 \cdots z_k) \\ &= x_1 x_2 \cdots x_i y_1 y_2 \cdots y_j z_1 z_2 \cdots z_k \\ (X \cdot Y) \cdot Z &= (x_1 x_2 \cdots x_i y_1 y_2 \cdots y_j) \cdot Z \\ &= x_1 x_2 \cdots x_i y_1 y_2 \cdots y_j z_1 z_1 \cdots z_k \end{aligned}$$

so juxtaposition is associative.

Now, λ is a unity of W since $X \cdot \lambda = X = \lambda \cdot X$ since we are either appending or inserting an empty word. Thus W is a monoid, as desired.

If $|A| > 1$, then there are at least 2 "letters," say a and b. Then let $X = ab$ and $Y = ba$, so that $X \cdot Y = abba$ but $Y \cdot X = baab$, so $X \cdot Y \neq Y \cdot X$, so W is noncommutative if $|A| > 1$. On the other hand, if $|A| = 1$, then W is commutative, since every word is just a repeating string of a single letter, which when juxtaposed with other words, is just another string of the same letter.

$\square$

11. An element e is called a left unity for an operation if $ex = x$ for all x. If an operation has two left unities, show that it has no right unity.

Proof. Let i_1, i_2 be left unities, so that $i_1 \neq i_2$. Then suppose there exists a right unity e. Then we have $e = i_1 e = i_1$ and $e = i_2 e = i_2$, so by the transitive property $i_1 = i_2$, which is a contradiction. Thus there does not exist a right unity, as desired.

$\square$

Section 2.2: Groups

7. Show that the set
$$G = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \middle| a, b, c \in \mathbb{R} \right\}$$
is a group under matrix multiplication.

Proof. A group must satisfy 4 axioms:

1. G is closed under matrix multiplication. Let
$$A = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$
$$X = \begin{bmatrix} 1 & x & y \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$
be in G. Then
$$AX = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & x+a & y+az+b \\ 0 & 1 & z+c \\ 0 & 0 & 1 \end{bmatrix}$$
$$XA = \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+x & b+xc+y \\ 0 & 1 & c+z \\ 0 & 0 & 1 \end{bmatrix}$$
Thus AX and XA are both in G.

2. Matrix multiplication is associative. Let A, X as before, and let $P = \begin{bmatrix} 1 & p & q \\ 0 & 1 & r \\ 0 & 0 & 1 \end{bmatrix}$. Then we have
$$\begin{aligned} A(XP) &= \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \left(\begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & p & q \\ 0 & 1 & r \\ 0 & 0 & 1 \end{bmatrix} \right) = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & p+x & q+xr+y \\ 0 & 1 & r+z \\ 0 & 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & p+x+a & q+xr+y+ar+az+b \\ 0 & 1 & r+z+c \\ 0 & 0 & 1 \end{bmatrix} \\ (AX)P &= \left(\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} \right) \begin{bmatrix} 1 & p & q \\ 0 & 1 & r \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+x & y+az+b \\ 0 & 1 & z+c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & p & q \\ 0 & 1 & r \\ 0 & 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & p+x+a & q+rx+ra+y+az+b \\ 0 & 1 & r+z+c \\ 0 & 0 & 1 \end{bmatrix} \end{aligned}$$
so $A(XP) = (AX)P$, thus the operation is associative.

3. There is a unity element in G. This is
$$I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Let A be as before, then

$$AI = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$
$$IA = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$

Thus I is a unity.

4. Every element of G has an inverse in G. Indeed, if A is as before, then we can find its inverse A^{-1} to be
$$A^{-1} = \begin{bmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{bmatrix}$$
and $A^{-1} \in G$ as well.

Thus G is a group, as desired.

□

16. If $fgh = 1$ in a group G, show that $ghf = 1$. Must $gfh = 1$?

Proof. Since $fgh = f(gh) = 1$, that means that $f^{-1} = gh$. Then $ghf = f^{-1}f = 1$, as desired. It is not necessary that $gfh = 1$, which is not true if f and h don't commute.

□

20. Show that a group G is abelian if $g^2 = 1$ for all $g \in G$. Give an example showing that the converse is false.

Proof. Since $gg = 1$ for all $g \in G$, this means that all elements of g are self-inverses. Consider the product $(gf)(fg) = g(ff)g = gg = 1$. Thus gf and fg are inverses, but since all elements of G are their own inverse, it follows that $gf = fg$, so G is abelian, as desired.

To show the converse is not necessarily true, consider the abelian group $(\mathbb{Z}_3, +)$. Then $\bar{1} + \bar{1} = \bar{2} \neq \bar{0}$, so the condition $g^2 = 1$ does not hold in this case.

□

28. Let a and b be elements of a group G. If $a^n = b^n$ and $a^m = b^m$ where $\gcd(m, n) = 1$, show that $a = b$.

Proof. Since $\gcd(m, n) = 1$, we may find $x, y \in \mathbb{Z}$ such that $xm + yn = 1$. Since $a^n = b^n$, we may raise both sides to the y power, so that $a^{yn} = b^{yn}$, and similarly with the other equation to get $a^{xm} = b^{xm}$. Multiplying the two equations, we have

$$a^{xm+yn} = a = b^{xm+yn} = b,$$

as desired.

□