Blake Griffith
HW 1: Chapter 2, 1.3, 2.3, 2.4, 3.2,,4.2,4.3,4.4,4.6, 4.10 &
Pre-Lecture Problems: Chapter 2, 2.1, 3.1,4.5, 4.7
M373K
Due 09/10, 2013

Exercise (1.3). *Let $\mathbb{N}$ denote the set $\{1, 2, 3, \ldots\}$ of natural numbers, and let $s : \mathbb{N} \to \mathbb{N}$ be the shift map, defined by $s(n) = n + 1$. Prove that s has no right inverse, but it has infinitely many left inverses.*

right inverse

Suppose that s has a right inverse r. Then by definition $\forall n \in \mathbb{N}$ we have $s \circ r(n) = n$. However if we take the case $n = 1$ we see:

$$\begin{aligned} s \circ r(1) &= 1 \\ s(r(1)) &= 1 \\ r(1) + 1 &= 1 \\ r(1) &= 0 \end{aligned}$$

But this means $s(r(1)) = s(0)$ which is undefined because $s : \mathbb{N} \to \mathbb{N}$ and $0 \notin \mathbb{N}$. So the right inverse cannot exist.

left inverse

Suppose s has a left inverse l. For any $n \in \mathbb{N}$ we must have $l : \mathbb{N} \to \mathbb{N}$ and

$$\begin{aligned} l \circ s(n) &= n \\ l(s(n)) &= n \\ l(n + 1) &= n \end{aligned}$$

But the range of $s(n)$ is $\{2, 3, \dots\}$ so our requirements on $l \circ s(n)$ only require l be a map from $\{2, 3, \dots\} \to \mathbb{N}$ so we are free to define $l(1)$ to be any of the infinite natural numbers. So there are infinite left inverses of s.

Exercise (2.3)**.** *Let x, y, z and w be the elements of a group G.*

(a) Solve for y, given that $xyz^{-1}w = 1$.

(b) Suppose that $xyz = 1$. Does it follow that $yzx = 1$? Does it follow that $yxz = 1$?

Proof.

(a)

$$\begin{aligned} xyz^{-1}w &= 1 \\ x^{-1}xyz^{-1}w &= x^{-1} \\ yz^{-1}w &= x^{-1} \\ yz^{-1}ww^{-1} &= x^{-1}w^{-1} \\ yz^{-1} &= x^{-1}w^{-1} \\ yz^{-1}z &= x^{-1}w^{-1}z \\ y &= x^{-1}w^{-1}z \end{aligned}$$

(b)

For $yzx = yxz = 1$ we would need $xz = zx$ but x, z communitivity is not implied by the stated conditions. So it does not follow that $yxz = 1$.

□

Exercise (2.4)**.** *In which of the following cases is H a subgroup of G?*

(a) $G = GL_n(\mathbb{C})$ and $H = GL_n(\mathbb{R})$.

(b) $G = \mathbb{R}^\times$ and $H = \{1, -1\}$.

(c) $G = \mathbb{Z}^+$ and H is the set of positive integers.

(d) $G = \mathbb{R}^\times$ and H is the set of positive reals.

(e) $G = GL_2(\mathbb{R})$ and H is the set of matrices $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ with $a \neq 0$.

Proof.

(a)

Yes. We have closure since $GL_n(\mathbb{C}) \subset GL_n(\mathbb{R})$ and $GL_n(\mathbb{R})$ is closed under the matrix product. We have the identity element since $I \in GL_n(\mathbb{R})$. And we have inverses since all elements of $GL_n(\mathbb{R})$ are invertible by definition and contained in $GL_n(\mathbb{R})$.

(b)

Yes. H is closed under multiplication. The identity element $1 \in H$. And finally 1 and -1 are each their own inverse element.

(c)

No. The element 644228 is in H but its inverse, -644228, is not in H.

(d)

Yes. H is closed since for any $a, b \in \mathbb{R}_{>0}$ we have $ab > 0$. Inverses are in H because if we consider some $a \in \mathbb{R}_{>0}$. Then its inverse is $1/a$ which is also in $\mathbb{R}$. Finally $R_{>0}$ contains the multiplicative identity element 1.

(e)

Yes. We have closure because.

$$\begin{aligned} A &= \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \\ AA &= \begin{pmatrix} a^2 & 0 \\ 0 & 0 \end{pmatrix} \\ AAA &= \begin{pmatrix} a^3 & 0 \\ 0 & 0 \end{pmatrix} \\ &\cdots \end{aligned}$$

And so on... So the H is closed under the matrix product. We have the identity element. Which is the case where $a = 1$.

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

And

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

And finally H contains the inverses of all its elements which are of the form:

$$AA^{-1} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1/a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

□

Exercise (3.2)**.** *Prove that if a and b are positive integers whose sum is a prime p, their greatest common divisor is* 1*.*

Proof. Let $a + b = c$ where c is prime and define $\gcd(a, b) = d$ where d is the biggest number that divides a and b. Now since d divides a and b, it must divide c. Because we could Rewrite $a + b = c$ as

$$\underbrace{(d+\cdots+d)}_{\text{a}}+\underbrace{(d+\cdots+d)}_{\text{b}}=\underbrace{(d+\cdots+d)}_{\text{c}}$$

However since c is prime its only divisors are c and 1. So d is either c or 1. But we can rule out $d = c$ since $d \leq a$ and $d \leq b$ and $a + b = c$. Therefore $d = 1$.

□

Exercise (4.2)**.** *An nth root of unity is a complex number z such that $z^n = 1$.*

(a) Prove that nth roots if unity form a cyclic subgroup of $\mathbb{C}^\times$ of order n.

(b) Determine the product of all the nth roots of unity.

Proof. (a)

If z is an nth root of unity. Such that $z^n = 1$. Then we can generate then cyclic group $< z >$ with powers of it up to $n - 1$

$$< z >= \{z^0, z^1, z^2, \dots z^{n-1}\}$$

This is closed because any product in $< z >$ can be written $z^i z^j = z^{qn+r}$ where q is some integer, and $0 < r < n$. By the division algorithm. So we can write $z^{i+j} = z^{qn+r} = z^{qn}z^r = z^r$ and z^r is in $< z >$.

The identity element 1 is contained in $< z >$.

And each elements inverse can be taken as $(z^i)^{-1} = z^{n-i}$.

(b)

First lets consider the form of the nth root of unity. We rewrite z as $z = |z|^n \exp(in\theta)$. But $|z|^n$ must be one for $z^n = 1$. Now we rewrite $\exp(in\theta)$ using Euler's formula as $z^n = \exp(in\theta) = 1 = \cos(n\theta) + i\sin(n\theta)$. This requires that $\theta = 2\pi/n$. So we get the nth root of unity in the form $z = \exp i2\pi/n$.

If we take the product of all roots of unity up to n we see:

$$\prod_{j=1}^{n} \exp(i2\pi/j) = \exp(i2\pi(\sum_{j=1}^{n} 1/j))$$

But the sum here is a divergent harmonic series... So I don't know what to do.

□

Exercise (4.3)**.** *Let a and b be elements of a group G. Prove that ab and ba have the same order.*

Proof. Let ab be order n, or $(ab)^n = 1$. Then we can rewrite this as:

$$(ab)^n = (ab)_1(ab)_2 \dots (ab)_n = 1$$

We can show this is equivalent to $(ba)^n = 1$ as follows.

$$\begin{aligned} (ab)_1(ab)_2 \dots (ab)_n &= 1 \\ a^{-1}(ab)_1(ab)_2 \dots (ab)_n &= a^{-1} \\ (b)_1(ab)_2 \dots (ab)_n &= a^{-1} \\ (b)_1(ab)_2 \dots (ab)_n a &= a^{-1}a \\ (b)_1(ab)_2 \dots (ab)_n a &= 1 \end{aligned}$$

Now shifting the indices.

$$\begin{aligned} (ba)_1(ba)_2 \dots (ba)_n &= 1 \\ (ba)^n &= 1 \end{aligned}$$

Therefore ba is order n.

□

Exercise (4.4)**.** *Describe all groups G that contain no proper subgroup.*

Proof. For a group to contain no proper subgroup. It either needs to a trivial group itself. Or every element in the group can generate the entire group. Therefore these groups lacking subgroups must be cyclic, because by our definition, a cyclic group can be generated by one element $< x >$.

So we seek a cyclic group G which has no subgroups. First we consider a cyclic G with infinite order. This has infinite subgroups because we can take any element x^i and use it to generate a subgroup $< x^i >$ that will not contain x^{i-1} therefore $< x^i >$ is proper subgroup, so groups with infinite order are ruled out.

For groups with finite order, consider G with order p, and some $x^i \in G$. Then ($i\dot{n} \mod p$) cannot be zero for some $0 < n < p$. Because otherwise, if $(i\dot{n} \mod p) = 0$ then x^i would generate the subgroup $\{(x^i)^0, (x^i)^1, \dots, (x^i)^n\}$ and since $n < p$ this would be a proper subgroup since it contains fewer elements than the parent group.

This requires that p be prime. Otherwise it would have a divisor d and choosing the dth element would yield a subgroup as above.

So the only groups G, without subgroups are cyclic groups with prime orders.

□

Exercise (4.6)**.** *(a) Let G be a cyclic group of order 6. How many of its elements generate G? Answer the same question for cyclic groups of orders 5 and 8.*

(b) Describe the number of elements that generate a cyclic group of arbitrary order n.

Proof. (a)

A group is generated by its elements if the power of the element is coprime with the order of the group.

To see this consider a group G of order n and an element $x^i \in G$ where i is not coprime with n. Then for some $a < n$ we have $ai = n$ so we would only generate the subgroup $\{(x^i)^0, (x^i)^1, \dots (x^i)^a\}$.

So for a group of order 6, there are 2 coprimes: 1 and 5. For order 5 we have 4 coprimes: 1, 2, 3, 4. For order 8 we have 4 coprimes: 1, 3, 5, 7.

(b)

The number of elements which generate a cyclic group of order n is equal to the number of integers coprime with n and less than n.

□

Exercise (4.10)**.** *Show by an example that the product of elements of finite order in a group need not have finite order. What if the group is abelian? HINT: Think about* 2×2 *matrices.*

Proof. Consider two matrices which are inverses of themselves:

$$A = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}, A^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
$$B = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}, B^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

So $< A >$ and $< B >$ are finite order. But the product $< AB >$ is not.

$$\begin{aligned} AB = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \\ (AB)^2 &= \begin{pmatrix} 1 & 0 \\ -4 & 1 \end{pmatrix} \\ (AB)^3 &= \begin{pmatrix} 1 & 0 \\ -8 & 1 \end{pmatrix} \end{aligned}$$

And so on.. So the order of $< AB >$ is infinite.

If we consider two elements of finite order in an Abellian group, it must be true that

$$(ab)^l = \underbrace{(ab)(ab)\dots(ab)}_{l \text{ times}} = \underbrace{(a\dots a)}_{l \text{ times}}\underbrace{(b\dots b)}_{l \text{ times}} = a^l b^l$$

So if a is order n and b is order m, ab is at most order mn.

□

Pre-Lecture Problems

Exercise (2.1)**.** *Make a multiplication table for the symmetric group* S_3*.*

Using the same notation as on page 42 of the textbook. with rows $\circ$ columns:

	1	x	x^2	y	xy	x^2y
1	1	x	x^2	y	xy	x^2y
x	x	x^2	1	xy	x^2y	y
x^2	x^2	1	x	x^2y	y	xy
y	y	x^2y	xy	x	x^2	x
xy	xy	y	x^2y	x^2	1	x^2
x^2y	x^2y	xy	y	1	x	1

Exercise (3.1)**.** *Let $a = 123$ and $b = 321$. Compute $d = gcd(a, b)$ and express d as an integer combination $ra + sb$.*

Applying the Euclidean Algorithm

$$
\begin{aligned}
321 &= 2 \cdot 123 + 75 \\
123 &= 1 \cdot 75 + 48 \\
75 &= 1 \cdot 48 + 27 \\
48 &= 1 \cdot 27 + 21 \\
27 &= 1 \cdot 21 + 6 \\
21 &= 4 \cdot 6 + 3 \\
6 &= 2 \cdot \boxed{3}
\end{aligned}
$$

Now we work backwards to find the desired r and s.

$$
\begin{aligned}
3 &= 21 - 3 \cdot 6 \\
3 &= 21 - 3(27 - 21) & &= 4 \cdot 21 - 3 \cdot 27 \\
3 &= -3 \cdot 27 + 4(48 - 27) & &= 4 \cdot 48 - 7 \cdot 27 \\
3 &= 4 \cdot 48 - 7(75 - 48) & &= -7 \cdot 75 + 11 \cdot 48 \\
3 &= -7 \cdot 75 + 11(123 - 75) & &= 11 \cdot 123 - 18 \cdot 75 \\
3 &= 11 \cdot 123 - 18(321 - 2 \cdot 123) \\
3 &= \boxed{47} \cdot 123 - \boxed{18} \cdot 321
\end{aligned}
$$

Exercise (4.5)**.** *Prove that every subgroup of a cyclic group is cyclic. Do this by working with exponents and use the description of the subgroups of $\mathbb{Z}^+$.*

Proof. Suppose G is a cyclic group and H is a subgroup of G. If H is the identity element or equal to G we are done since these are cyclic. If H is a proper subgroup of G, then each element of H must be of the form x^i since every element in G has this form.

So we can choose the element with lowest positive power, m. So $x^m \in H$.

and we choose some other arbitrary element $a = x^n$ of H.

But by the division algorithm we can write $n = qm + r$ for some integer q and $0 \leq r < m$. Since $m \leq n$.

So we can write $x^n = x^{qm+r} = (x^m)^q x^r$. But we required that $0 \leq r < m$ and m be the smallest positive power in H. So $r = 0$ and $x^r = 0$. So now we have $x^n = (x^m)^q$ and x^m to any power is in H since it must be closed. So any arbitrary element of H can be written as a power of x. So $< x >= H$.

□

Exercise (4.7)**.** *Let x and y be elements of a group G. Assume that each of the elements x, y and xy has order 2. Prove that the set $H = \{1, x, y, xy\}$ is a subgroup of G and that it has order 4.*

Proof. For H to be a subgroup of G it must be closed, contain the identity element, and contain each element's inverse. The latter two requirements are easily demonstrated:

- identity: The set contains 1. So we have the identity element.
- inverses: We are given that each element is order 2. Therefore $1^2 = x^2 = y^2 = (xy)^2 = 1$. So each element is its own inverse.

The requirement of closure can be demonstrated by showing that the Cayley table only contains elements which are inside the set. Note that $yx = 1 \cdot yx = (xy)(xy)(yx) = xyx(yy)x = xy(xx) = xy$.

	1	x	y	xy
1	1	x	y	xy
x	x	1	xy	y
y	y	xy	y	x
xy	xy	y	x	1

We have shown H is a subgroup. Now we can say it is order 4 because it only has 4 elements.

$\square$