Elements of Algebra I: Homework #4

Due on February 7th, 2017

Professor Deepam Patel Section 161

Yao Xiao

Problem 1

1.
a) $GL_n(\mathbb{R})$ it has an inverse because it's an invertible matrix, and also the product of two real numbers is a real number so the product of two real numbers matrix is a real number matrix. The identity matrix is invertible as well
b) it's a sub group, since multiplication of 1,-1 is closed under $\{1, -1\}$, and identity $1 \in \{1, -1\}$, and also $\{1^{-1}, -1^{-1}\}$ is in $\{1, -1\}$
c) it's not a subgroup, since the inverse of positive integer is not positive

Problem 2

a) $Z_2 * Z_2 * Z_2$, since there's no generator
b) $Z_2 * Z_2 = \{(0, 1), (0, 0), (1, 0), (1, 1)\}$ Since no elements to itself will equal to (1,1)

Problem 3

For $k \in \mathbb{Z}_8$, gcd(8, k) = 1, k = 1, 3, 5, 7 For $k \in \mathbb{Z}_{20}$, gcd(20, k) = 1, k = 1, 3, 7, 9, 11, 13, 17, 19

Problem 4

Let the order of ab be n, so

$$(ab)^n = e$$
$$(ab)(ab)(ab)...(ab) = e$$
$$a(ba)(ba)(ba)(ba)....(ba)b = e$$
$$a^{-1}a(ba)(ba)(ba)(ba)....(ba)ba = e$$
$$(ba)^n = e$$

So ba has an order of n too.

Problem 5

We must show that g is close. So assume

$$a, b \in Z, g \in G, g^{-1} \in G$$
$$ag = ga$$
$$bg = gb$$
$$ag^{-1} = g^{-1}a$$
$$bg^{-1} = g^{-1}b$$
$$abgg^{-1} = agbg^{-1} = agg^{-1}b = gag^{-1}b = gg^{-1}ab$$

so ab is close under Z. Let $a \in Z$ n. a has an inverse $a^{-1} \in G$
we want to show that $a^{-1} \in Z$
let $g, g^{-1} \in G$

$$(g^{-1}a^{-1}g)^{-1} = g^{-1}ag = g^{-1}ga = a$$

Which implies $g^{-1}a^{-1}g = a^{-1}$, multiply g^{-1} on the both sides, we get $g^{-1}a^{-1} = a^{-1}g^{-1}$. So $a^{-1} \in Z$

Problem 6

$$|g^k| = \frac{n}{gcd(n,k)}$$
$$gcd(40,k) = 40/10 = 4$$

So all elements in Z40 has a gcd of 4 is the answer, which is 4,12,28,36. Respectively, $x^4, x^{12}, x^{28}, x^{36}$ are the elements of order 10.

Problem 7

We could show that kr=n. So a cyclic group of order n is equal to a group of $\{e^0, e^1, e^2 ... e^{n-1}\}$. We could easily find a subgroup with an order r. $\{e^0, e^k, e^(2k) ... e^{k(r-1)}\}$ We assume there's another group which has an order of r, namely G'. And we could tell that G'=$< k' >$ and k'r=n. But according to division theory, there exists only unique integers q,r such that a=qb+r , so k=k'.

Problem 8

We assume that $d = gcd(n', n) > 1$. Then $k = \frac{n'n}{d}$ is an integer since n/d is an integer, as a result every element of $Z_n * Z_m$ has an order dividing k, and it can't be cyclic because of that.
When $d = gcd(n', n) = 1$, then $k = \frac{n'n}{d} = nn'$, so $< 1, 1 >$ could be the generator of the group so it's cyclic.