Kyle Kloberdanz
Math 417

Exercise 3.1.4: Prove that a nonempty set G with an associative operation $*$ is a group if and only if the equations $g * x = h$ and $x * g = h$ have solutions in G for all $g, h \in G$. *Hint: Prove that if $e * g = g$ for some g, then $e * h = h$ for all $h \in G$. Now appeal to Exercise 3.1.3*

Note: you should *not* assume that the same x solves both equations simultaneously. In other words, prove that G is a group if and only if $*$ is an associative operation such that:

for all $g, h \in G$ there exist $x, y \in G$ such that $g * x = h$ and $y * g = h$.

Proof. Recall the definition of a group:

1. The operation * is associative.
2. There is an identity $e \in G$ with the property that $e * g = g * e = g$ for all $g \in G$
3. For all $g \in G$, there exists an inverse $g^{-1} \in G$, with the property that $g * g^{-1} = g^{-1} * g = e$

For 1, we are given in the problem statement that $*$ is associative.

For 2, we will show that the identity exists, and the identity is unique

Let's determine that there is an identity. We will demonstrate a proof by contradiction. We will assume that for any set with no identity that for all $g, h \in G$ there exist $x, y \in G$ such that $g * x = h$ and $y * g = h$. Let's use the set $X = \mathbb{N} \backslash \{0\} = \{1, 2, 3, ...\}$ and the associative operator $+$. We can see that if $g = 1$ and $h = 1$ where $g, h \in X$, then there is no element in X such that $g + x = h$ where $x \in X$. To put another way $1 + x = 1$ if and only if $x = 0$, which is the identity, and because $0 \notin X$, this contradicts the problem statement. Hence the identity must be present in the set for the condition above to hold.

Now let's prove that the identity element is unique for the set G. We will demonstrate this by contradiction. Let's start by assuming that there are two identity elements, $e, e' \in G$ such that $eg = ge = g$ and $e'g = ge' = g$. Now if e is an identity, then $ee' = e'$ but at the same time if e' is also an identity, then $ee' = e$, therefore $e' = ee' = e$, a contradiction that e and e' are different identities, hence the identity $e \in G$ is unique.

By showing that the identity exists and is unique in G, we know that if e is the identity, then $e * g = g$ and $e * h = h$.

For 3, we will demonstrate another proof by contradiction. We will show that the condition in the problem statement cannot hold if there does not exist an inverse. We have already shown that our set must contain the identity. Let

us examine the natural numbers, $\mathbb{N} = \{0, 1, 2, ...\}$. $g, g^{-1} \in N$ if and only if $0 = g + g^{-1}$ for all g. Clearly, the only value for g that satisfies this is when $g = g^{-1} = 0$. For all other values of g, there does not exist a g^{-1} such that $g + g^{-1} = 0$. Hence the inverse must exist in G for the condition in the problem statement to hold.

We have shown that:
For all $g, h \in G$ there exist $x, y \in G$ such that $g * x = h$ and $y * g = h$ $\iff$ $*$ is associative **and** there is an identity $e \in G$ with the property that $e * g = g * e = g$ for all $g \in G$ **and** for all $g \in G$, there exists an inverse $g^{-1} \in G$, with the property that $g * g^{-1} = g^{-1} * g = e$, which is the definition of a group, therefore a nonempty set G with an associative operation $*$ is a group if and only if the equations $g * x = h$ and $x * g = h$ have solutions in G for all $g, h \in G$. □

Exercise 3.2.1: Suppose $n \geq 2$ is an integer and $d, d' > 0$ are two divisors of n. Prove that $\langle [d] \rangle < \langle [d'] \rangle$ if and only if $d' | d$.

Proof. Let's start by assuming that $\langle [d] \rangle < \langle [d'] \rangle$. Let $x, n \in \mathbb{Z}$.

$$\langle [d] \rangle < \langle [d'] \rangle \implies [d] \in \langle [d'] \rangle \implies [d] = [d']^x \implies [d]_n = [d']_n^x \implies$$
$$d \equiv d'x \pmod{n} \implies d' | d$$

Working backwards:

$$d' | d \implies d \equiv d'x \pmod{n} \implies [d]_n = [d']_n^x \implies [d] = [d']^x \implies$$
$$[d] \in \langle [d'] \rangle \implies \langle [d] \rangle < \langle [d'] \rangle$$

Because we have shown the implication goes both ways, therefore

$$\langle [d] \rangle < \langle [d'] \rangle \iff d' | d$$

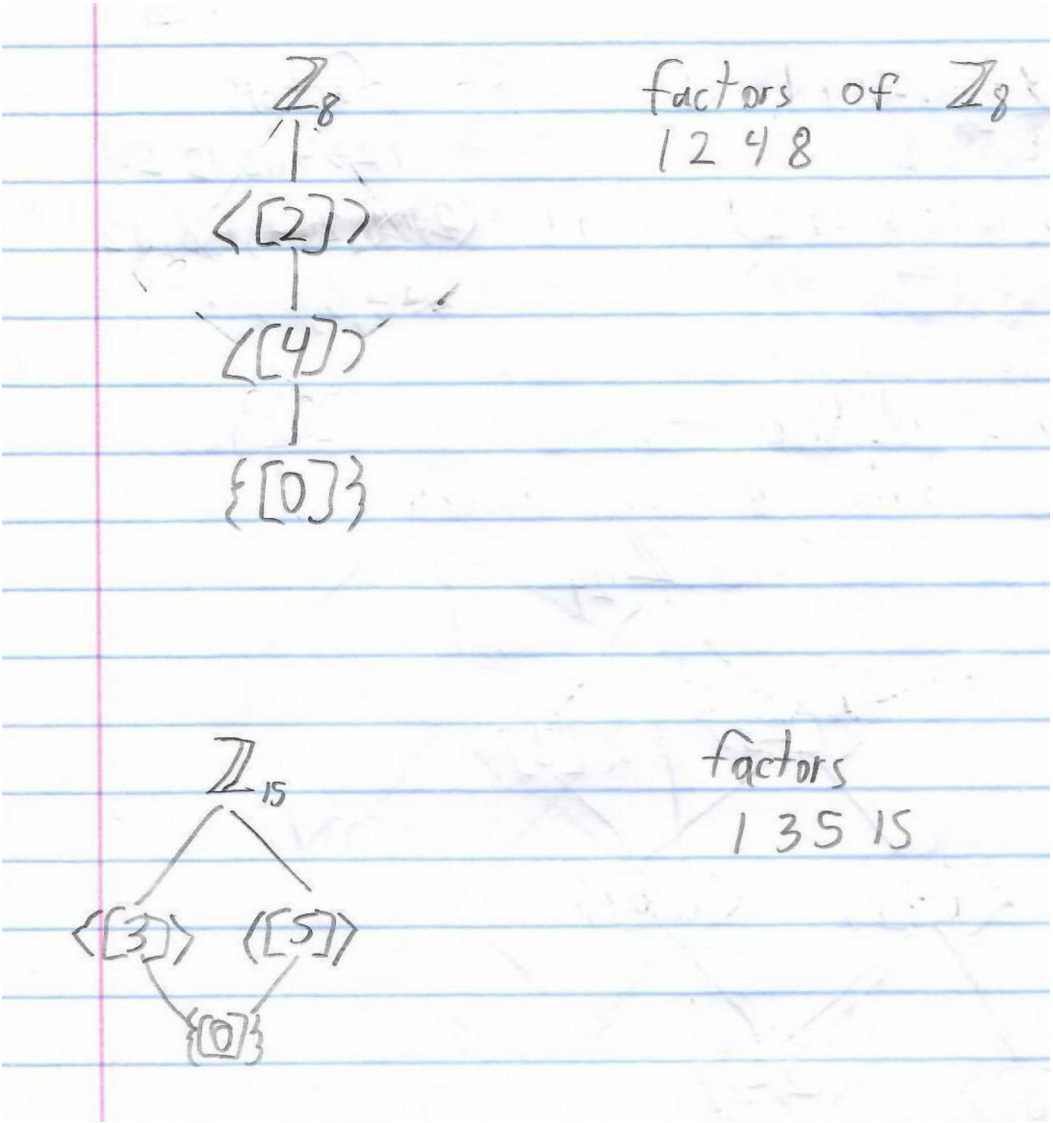
□

Exercise 3.2.2: Prove that the number of elements of order n in $\mathbb{Z}_n$ is exactly $\varphi(n)$, the Euler phi function of n.
Hint: You need to decide which $[a] \in \mathbb{Z}_n$ *generate* $\mathbb{Z}_n$.

Note: The group operation in $\mathbb{Z}_n$ is $+$ (modular addition)

Proof. Recall, an equivalency class $[a]_n = \{a + nk | k \in \mathbb{Z}\}$ Recall that $1 = gcd(a, n) \iff 1 = ma + nk$ where $a, m, k \in \mathbb{Z}$. Because the generator for the integer is $\langle 1 \rangle$, we need to have some a where $a + nk = [a + 1]$. If $gcd(a, n) \neq 1$, then we would be in a situation where there is no a such that $a + nk = [a + 1]$, which would imply that this particular a could not be a generator of $\mathbb{Z}_n$. Hence the only generators of $\mathbb{Z}_n$ are the elements of $\mathbb{Z}_n$ that are relatively prime with n. The cardinality of this set is defined as $\varphi(n)$, therefore the number of elements of order n in $\mathbb{Z}_n$ is exactly $\varphi(n)$, the Euler phi function of n. □

Exercise 3.2.3 Draw the subgroup lattice for the groups $\mathbb{Z}_8, \mathbb{Z}_{15}, \mathbb{Z}_{24}$, and $\mathbb{Z}_{30}$.

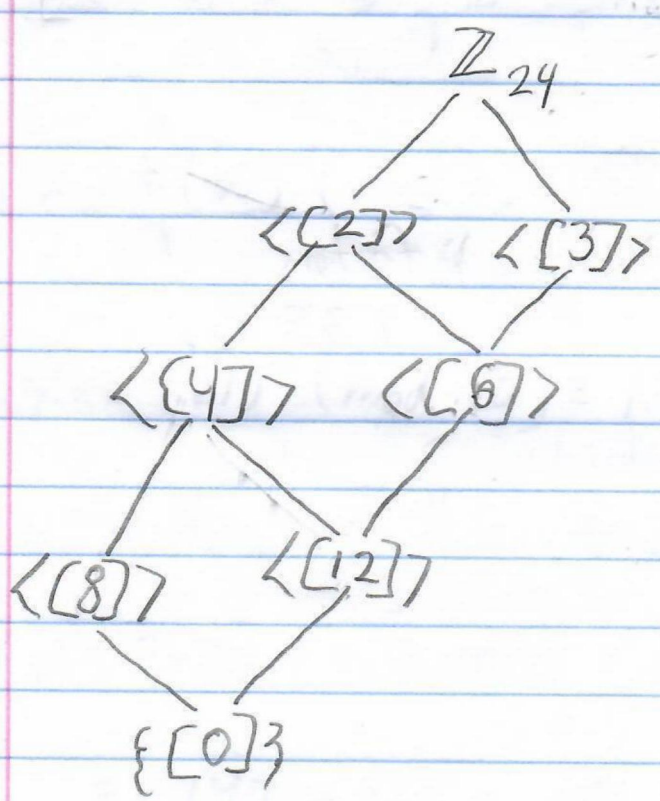


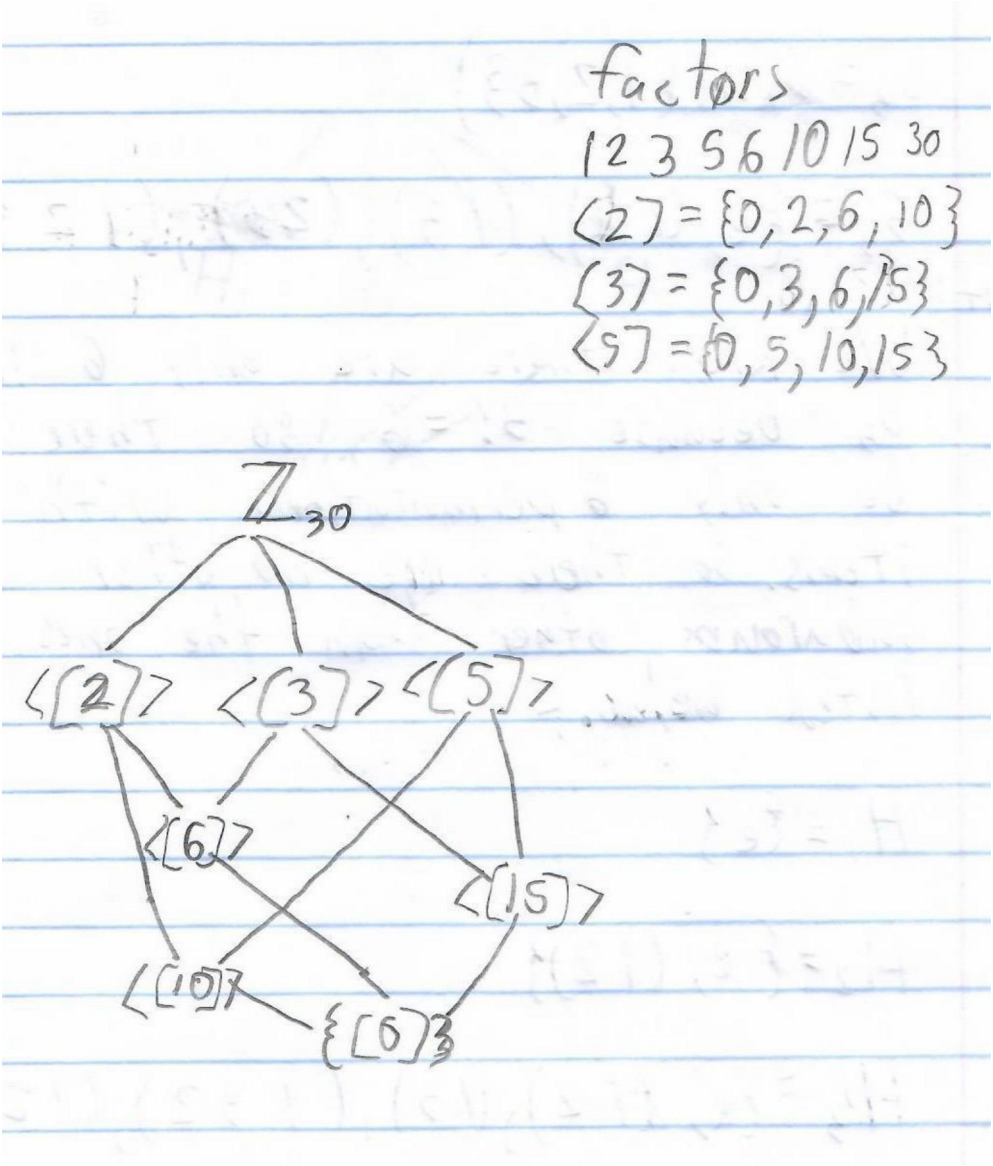
factors

1 2 3 4 6 8 12 24

$\langle 2 \rangle = 0, 2, 4, 6, 8, 12$

$\langle 3 \rangle = 0, 3, 6, 12$





Exercise 3.2.4 Draw the subgroup lattice for S_3 (a group with respect to composition $\circ$). You will need to find all the subgroups $H < S_3$ by hand (because we don't yet have any theorems that tell us what the subgroups of S_3 are). *Hint: There are exactly 6 subgroups, but you should verify this by proving that there are no other subgroups than the ones you have listed.*

To start, we will find the subgroups.

Recall, any subgroup will have the following properties:

1. Each group will contain the identity, e
2. For all $g, h \in H$, $g * h \in H$
3. For all $g \in H$, $g^{-1} \in H$

Hence, each of the subgroups we find for S_3 must also have these properties. To put this in plain English, each group we find will include the identity, it will include the product of every other member of the group, and it will also include the inverse of every member of the group.

Recall from section 1.3 on permutations that $S_n = Sym(1..n)$, so we can use this definition to write S_3 as $Sym(\{1, 2, 3\})$.

We can expand out these symmetries into the set

$$S_3 = \{e, (2\ 3), (1\ 2), (1\ 2\ 3), (1\ 3\ 2), (1\ 3)\}$$

As we can see, there are six elements in this set, which if we remember back to probability and statistics classes, this makes sense because the number of permutations of 3 distinct items is $3! = 3 \times 2 \times 1 = 6$ permutations.

We can also employ the powerful CAS system, Sage Mathematics, to automate this task.

```
sage: G = SymmetricGroup(3)
sage: {i for i in G}
{(), (2,3), (1,2), (1,2,3), (1,3,2), (1,3)}
```

We will now find each of the subgroups, H, of this symmetry set.

Let's begin with $H_1 = \{e\}$, the set that only contains the inverse. Let's verify the three properties listed above. Notice that for the sake of brevity, I will exclude repeats when verifying below. For example, I show that $e \circ e = e \in H_1$, therefore we know that this will hold for H_1 through H_6, and therefore does not need to be shown each time.

1. $e \in H_1$
2. $e \circ e = e \in H_1$
3. $e \circ e = e \in H_1$

Let $H_2 = \{e, (2\ 3)\}$.

1. $e \in H_2$
2. $$e \circ (2\ 3) = (2\ 3) \circ e = (2\ 3) \in H_2$$
   And
   $$(2\ 3) \circ (2\ 3) = e \in H_2$$
3. $(2\ 3) \circ (2\ 3) = e \in H_2$

Let $H_3 = \{e, (1\ 2)\}$.

1. $e \in H_3$

2.
$$e \circ (1\ 2) = (1\ 2) \circ e = (1\ 2) \in H_3$$
And
$$(1\ 2) \circ (1\ 2) = e \in H_3$$

3. $(1\ 2) \circ (1\ 2) = e \in H_3$

Let $H_4 = \{e, (1\ 3)\}$.

1. $e \in H_4$
2.
$$e \circ (1\ 3) = (1\ 3) \circ e = (1\ 3) \in H_4$$
And
$$(1\ 3) \circ (1\ 3) = e \in H_4$$

3. $(1\ 3) \circ (1\ 3) = e \in H_4$

Let $H_5 = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$.

1. $e \in H_5$
2.
$$e \circ (1\ 2\ 3) = (1\ 2\ 3) \circ e = (1\ 2\ 3) \in H_5$$
And
$$e \circ (1\ 3\ 2) = (1\ 3\ 2) \circ e = (1\ 3\ 2) \in H_5$$
And
$$(1\ 3\ 2) \circ (1\ 2\ 3) = e \in H_5$$
And
$$(1\ 2\ 3) \circ (1\ 3\ 2) = e \in H_5$$
And
$$(1\ 2\ 3) \circ (1\ 2\ 3) = (3\ 1\ 2) \in H_5$$
And
$$(1\ 3\ 2) \circ (1\ 3\ 2) = (1\ 2\ 3) \in H_5$$
3.
$$(1\ 3\ 2) \circ (1\ 2\ 3) = e \in H_5$$
And
$$(1\ 2\ 3) \circ (1\ 3\ 2) = e \in H_5$$

Now the for this beast, $H_6 = \{e, (2\ 3), (1\ 2), (1\ 2\ 3), (1\ 3\ 2), (1\ 3)\}$

To satisfy property 1, we see that $e \in H_6$.
We arrive at H_6 by the procedure below.

1. Start with another set, for example H_2. We will see later on that we can start with any of our H sets from above, and this procedure will still work.
2. Append another item from S_3 into H_6.

3. Calculate to composition of that element by each element already in H_6 and append that element into H_6.

4. Repeat step 3 until the composition of every item has been calculated and appended to H_6.

By following the procedure above, we construct H_6, which interestingly enough happens to also be S_3. This procedure will satisfy property 2.

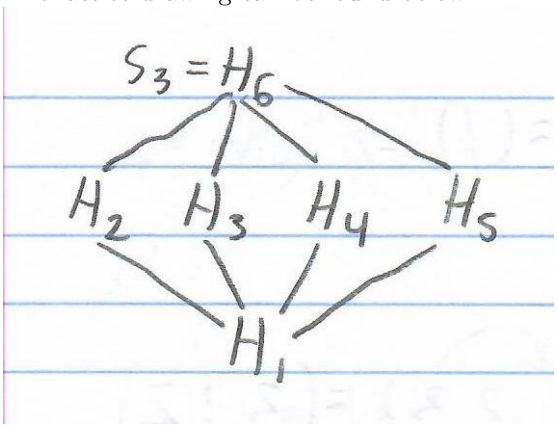
From the calculations for H_1 through H_5, we have already worked out the inverses of each element of H_6, and we can see that for any element of H_6 that the inverse is also present in H_6.

By following this procedure starting with any set H as our starting set, we will construct the same set H_6 each and every time. Therefore, we have shown that there are precisely six subgroups of S_3, because by appending any other element of S_3 to sets H_2 through H_5 and following this procedure, we only ever construct H_6.

Therefore, our six subgroups of S_3 are:

$$H_1 = \{e\}$$
$$H_2 = \{e, (2\ 3)\}$$
$$H_3 = \{e, (1\ 2)\}$$
$$H_4 = \{e, (1\ 3)\}$$
$$H_5 = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$$
$$H_6 = \{e, (2\ 3), (1\ 2), (1\ 2\ 3), (1\ 3\ 2), (1\ 3)\}$$

The lattice drawing can be found below:



Exercise 3.2.5 Prove that if G and H are groups and $K < G$, $J < H$ are subgroups, then $K \times J \subset G \times H$ is a subgroup. Construct an example of a subgroup of $\mathbb{Z}_2 \times \mathbb{Z}_2$ which is **not** of the form $K \times J$ for some $K < \mathbb{Z}_2$ and $J < \mathbb{Z}_2$.

Proof. First we will show that $K \times J \subset G \times H$. Let $k \in K$, $j \in J$, $g \in G$, and $h \in H$. Because $K < G$ and $J < H$, $k \in G$ and $j \in H$ for all k and j, hence for any k, j, g, and h, $(k, j) \subset (g, h)$.

Second, we must show that for all $(k_1, j_1), (k_2, j_2) \in K \times J$ that $(k_1, j_1)(k_2, j_2) \in K \times J$.

$$(k_1, j_1)(k_2, j_2) = (k_1 k_2, j_1 j_2)$$

Because K and J are subgroups, $k_1 k_2 \in K$ and $j_1 j_2 \in J$, hence $(k_1 k_2, j_1 j_2) \in K \times J$.

Third, we must show that for all $(k, j) \in K \times J$ that $(k, j)^{-1} \in K \times J$.

$$(k, j)(k, j)^{-1} = (k, j)(k^{-1}, j^{-1}) = (kk^{-1}, jj^{-1}) = (e, e)$$

Verification:

$$(e, e)(k, j) = (ke, je) = (k, j) = (ek, ej) = (k, j)(e, e)$$

Because K and J are subgroups, $k^{-1} \in K$ and $j^{-1} \in J$. Hence $(k^{-1}, j^{-1}) \in K \times J$, which is the inverse of $K \times J$.

Because of these three reasons, $K \times J \subset G \times H$ is a subgroup, so therefore we can write:

$$K \times J < G \times H$$

□