Chapter 4: 6, 12, 13, 28, 30, 35.
Due date: Friday, 10/03

(Exercise numbers correspond to the printed textbook, generated from 2013/08/16 source files.)

6. Find the order of every element in the symmetry group of the square, D_4.

Solution:
In Exercise 5 of Homework 3, we found all eight elements of the group of symmetries of a square, also known as the dihedral group on four letters, denoted D_4.

To identify the elements of this group, we imagined a square with vertices labeled counter-clockwise: 1 in the south-west corner, 2 in the south-east corner, 3 in the north-east corner, and 4 in the north-west corner. The result looks something like this:

$$\begin{bmatrix} 4 & 3 \\ 1 & 2 \end{bmatrix}$$

The universe of this group is $\{e, \mu_1, \mu_2, \mu_3, \mu_4, \rho_1, \rho_2, \rho_3\}$, the elements of which are defined as follows:

- $e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = (\,)$ (the identity)
- $\mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = (2,4)$ (reflection across 45 degree line)
- $\mu_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (1,2)(3,4)$ (reflection across vertical line)
- $\rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1,2,3,4)$ (rotation by 90 degrees)
- $\mu_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = (1,3)$ (reflection across -45 degree line)
- $\rho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (1,3)(2,4)$ (rotation by 180 degrees)
- $\rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = (1,4,3,2)$ (rotation by -90 degrees)
- $\mu_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (1,4)(2,3)$ (reflection across horizontal line)

Since the order of an element x is the smallest positive integer k such that $x^k = e$, we can find the order by simply computing higher powers and stopping when we get to e. However, for the group of symmetries of a square, it's even easier. For example, it's obvious that

a reflection across a line, executed twice, leaves the points in their original position, so reflections have order 2. Rotations of ± 90 degrees have order 4, and 180 degree rotations have order 2.

To summarize, $\mu_1^2 = \mu_2^2 = \mu_3^2 = \mu_4^2 = e$, so the reflections have order 2. As for the rotations, $\rho_1^4 = e = \rho_3^4$, and 4 is the smallest such positive integer, so $|\rho_1| = 4 = |\rho_3|$, whereas $\rho_2^2 = e$, so $|\rho_2| = 2$. We can confirm this answer with just two lines of Sage/Python code. Using the format $(g, |g|)$, the following produces a list of orders of elements $g \in D_4$:

```
G = DihedralGroup(4)
[(x, x.order()) for x in G.list()]
```

From the output, we can read off the order of the elements of this group:

$$[((), 1), ((2,4), 2), ((1,2)(3,4), 2), ((1,2,3,4), 4), ((1,3), 2), ((1,3)(2,4), 2), ((1,4,3,2), 4), ((1,4)(2,3), 2)]$$

12. Find a cyclic group with exactly one generator. Can you find cyclic groups with exactly two generators? Four generators? How about n generators?

Solution: The cyclic group $\mathbb{Z}_2 = \langle \{0, 1\}, +, -, 0 \rangle$ has exactly one generator, namely the element 1. The cyclic group $\mathbb{Z}_3 = \langle \{0, 1, 2\}, +, -, 0 \rangle$ has exactly two generators, namely 1 and 2. Notice that the cyclic group $\mathbb{Z}_4$ still has only two generators. However, in the cyclic group $\mathbb{Z}_5 = \langle \{0, 1, 2, 3, 4\}, +, -, 0 \rangle$, all four non-identity elements are generators, since they are relatively prime to 5. More generally, by the same argument, we see that for any prime p the group $\mathbb{Z}_p = \langle \{0, 1, \ldots, p-1\}, +, -, 0 \rangle$ has $p - 1$ generators. What about 3? What about n?

13. For $n \leq 20$, which groups $U(n)$ are cyclic? Make a conjecture as to what is true in general. Can you prove your conjecture?

Solution: The elements of $U(n)$ are the *multiplicative units* of the set $\{0, 1, 2, \ldots, n-1\}$ with respect to multiplication modulo n. What this means is that, for each $x \in \{0, 1, 2, \ldots, n-1\}$, we have $x \in U(n)$ if and only there exists $y \in \{0, 1, 2, \ldots, n-1\}$ such that $x \cdot y = 1$, where $\cdot$ means multiplication modulo n. As we have seen, $x \in U(n)$ if and only if x and n are relatively prime.

Given n, if we wish to determine whether $U(n)$ is cyclic, the most direct approach would be to first compute $m = |U(n)|$ and then compute the order of each element of $U(n)$ to determine whether there exists $x \in U(n)$ such that $|x| = m$. If such an element exists, then it generates $U(n)$. This is certainly the first approach the student should try in order to gain more familiarity with unit groups.

After generating some examples, to speed things up we could let Python (or Sage or GAP) do the work for us. Some Python and GAP code is given in the appendix below for printing, for each $2 \leq n \leq 20$, those elements in $\{0, 1, 2, \ldots, n-1\}$ that are relatively prime to n. (As remarked above, these are precisely the elements of $U(n)$.)

After a fair amount of calculation (or using the programs given in the appendix below), we find that $U(n)$ is cyclic when $n \in \{2, 3, 4, 5, 6, 7, 9, 10, 11, 13, 14, 17, 18, 19\}$, and not

cyclic when $n \in \{8, 12, 15, 16, 20\}$. Here is a list of conjectures we might arrive at after contemplating our computational results:

(a) The group $U(4n)$ is not cyclic for $n \geq 2$.
(b) The group $U(n)$ is cyclic for n prime.
(c) The group $U(n)$ is cyclic for $n = 2p$ where p is a prime.
(d) If n is an odd number such that $U(n)$ is cyclic, then $U(2n)$ is cyclic also.
(e) If p and q are odd primes, then $U(pq)$ is not cyclic.

We do not yet have enough tools at our disposal to prove all of these, but we can certainly prove the first. (Some students, especially those who took a course in number theory, can probably prove the second.)

To prove the first conjecture, we need a little lemma from *Cyclic Group Supplement* that we quote here without proof.[1]

Lemma. *A cyclic group contains at most one element of order 2.*

Proof of (a): To prove the first conjecture above, we show that for $n \geq 2$ the group $U(4n)$ has two elements of order 2, hence, by the lemma, cannot be cyclic.

The group $U(4n)$ contains those elements of the set $\mathbb{Z}_{4n} = \{0, 1, \ldots, 4n-1\}$ that are relatively prime to $4n$. The element $2n-1$ belongs to $\mathbb{Z}_{4n}$ and is, in fact, relatively prime to $4n$, so $2n-1 \in U(4n)$. To see this, use the Euclidean Algorithm (page 25 of the text):

$$\begin{aligned} 4n &= (2n-1) \cdot 2 + 2 \\ 2n-1 &= 2 \cdot (n-1) + 1 \\ n-1 &= 1 \cdot (n-1) + 0 \end{aligned}$$

Arriving at 1 as the first coefficient on the right hand side of the last equation in the Euclidean Algorithm shows that $\gcd(4n, 2n-1) = 1$. By a similar argument, $4n-1 \in U(4n)$.

Now,

$$\begin{aligned} (2n-1)^2 &= 4n^2 - 4n + 1 \equiv 1 \pmod{4n}, \\ (4n-1)^2 &= 16n^2 - 8n + 1 \equiv 1 \pmod{4n}, \end{aligned}$$

so $2n-1$ and $4n-1$ are two distinct involutions of $U(n)$. By the lemma, then, $U(4n)$ is not cyclic.

28. Let a be an element in a group G. What is a generator for the subgroup $\langle a^m \rangle \cap \langle a^n \rangle$?

Solution: If m divides n, then $\langle a^n \rangle \leq \langle a^m \rangle$, so $\langle a^m \rangle \cap \langle a^n \rangle = \langle a^n \rangle$ and a^n is a generator. Similarly, if n divides m, then $\langle a^m \rangle \leq \langle a^n \rangle$, so $\langle a^m \rangle \cap \langle a^n \rangle = \langle a^m \rangle$ and a^m is a generator. Since these two cases are easily dispensed with, let's require of m and n that neither one divides the other.

An element x of $\langle a^m \rangle \cap \langle a^n \rangle$ must have the form $x = a^{mj} = a^{nk}$. So every element is a^t, where t is a common multiple of m and n. It is only natural, then, to suspect that the

[1] The statement and proof of this lemma are provided in the document CyclicgroupSupplement.pdf which resides in the misc directory of our GitHub repository.

generator of this subgroup should be the element a^ℓ, where ℓ is the *least* common multiple of m and n. This heuristic reasoning leads us to the statement that we wish to prove.

Claim: If $\ell = \text{lcm}(m, n)$, then a^ℓ generates $\langle a^m \rangle \cap \langle a^n \rangle$.

Proof. Let x be an arbitrary non-identity element of $\langle a^m \rangle \cap \langle a^n \rangle$. We will show that $x = a^{\ell d}$ for some d, which will prove that a^ℓ generates $\langle a^m \rangle \cap \langle a^n \rangle$.

As noted above, $x = a^{mj} = a^{nk}$, for some positive integers j and k. We can assume that j and k are the least positive integers with these properties. Then $mj = nk = t$, so $x = a^t$, where t is a common multiple of m and n. Since ℓ is the least common multiple, we have $\ell | t$, so there exists d such that $\ell d = t$. Therefore, $x = a^t = a^{\ell d}$. □

30. Suppose that G is a group and let a, $b \in G$. Prove that if $|a| = m$ and $|b| = n$ with $\gcd(m, n) = 1$, then $\langle a \rangle \cap \langle b \rangle = \{e\}$.

Solution: Let x be an arbitrary element of $\langle a \rangle \cap \langle b \rangle$. We will show that $x = e$. Indeed, x belongs to both of the cyclic subgroups $\langle a \rangle$ and $\langle b \rangle$ and, from Exercise 38 below, we know that the order of an element of a cyclic group divides the order of the group. Thus, $|x|$ is a common divisor of m and n, so $\gcd(m, n) = 1$ implies $|x| = 1$. Therefore, $x = e$. □

35. Prove that the subgroups of $\mathbb{Z}$ are exactly $n\mathbb{Z}$ for $n = 0, 1, 2, \ldots$.

Solution: In lecture we proved Theorem 4.3 which states that every subgroup of a cyclic group is cyclic. Certainly $\mathbb{Z}$ is cyclic, since it is generated by 1. Take an arbitrary subgroup $H \leq \mathbb{Z}$. Then H is cyclic, so $H = \langle n \rangle$ for some n. That is, $H = \{nk : k \in \mathbb{Z}\} = n\mathbb{Z}$. Conversely, if n is any number in $\{0, 1, 2, \ldots\}$, then the set $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ is closed under integer addition, additive inverse, and contains 0, so $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$. □

38. Prove that the order of an element in a cyclic group G must divide the order of the group.

Solution: Let $G = \langle a \rangle$ be a cyclic group. We can assume G is finite (otherwise the statement in this exercise wouldn't make sense), so suppose $|G| = |a| = n$. Let $x \in G$ be an arbitrary element and suppose $|x| = m$. We wish to show that m divides n. As usual, we employ the Division Algorithm, which says there exist integers q and r such that $n = qm + r$, where $0 \leq r < m$. The goal is to show $r = 0$, since, if we accomplish this, then we will have shown $n = qm$, that is, m divides n.

Since a generates the group, there is some integer $0 < j < n$ such that $a^j = x$. Therefore, $x^n = a^{jn} = a^{nj} = e^j = e$, so,

$$e = x^n = x^{qm+r} = x^{qm}x^r = x^{mq}x^r = e^q x^r = ex^r = x^r.$$

That is, $x^r = e$. But the order of x is m, which is the least positive integer such that $x^m = e$. This and $0 \leq r < m$ together imply $r = 0$. □

Appendix A. Computing with the Dihedral Group

In Exercise 6, we wanted the elements of the dihedral group on four letters, and the order of each element. Using the format $(g, |g|)$, the following produces a list of orders of elements $g \in D_4$:

```
G = DihedralGroup(4)
[(x, x.order()) for x in G.list()]
```

From the output, we can read off the order of the elements of this group:

$$[((),1),((2,4),2),((1,2)(3,4),2),((1,2,3,4),4),((1,3),2),((1,3)(2,4),2),((1,4,3,2),4),((1,4)(2,3),2)]$$

Appendix B. Computing with the Unit Group

Exercise 13 concerns the unit group $U(n)$, for $2 \leq n \leq 20$. With a few lines of Python, we can compute, for each $2 \leq n \leq 20$, those elements in $\{0, 1, 2, \ldots, n-1\}$ that are relatively prime to n. (As remarked above, these are precisely the elements of $U(n)$.)

```
for k in range(2,21):
    print "U("+str(k)+"):",
    order=0
    for j in range(k):
        if (gcd(j,k)==1):
            order = order + 1
            print j, ",",
    print " |U(" + str(k) + ")| =", order, "\n"
```

This produces the following output:

```
U(2): 1,  |U(2)| = 1
U(3): 1, 2,  |U(3)| = 2
U(4): 1, 3,  |U(4)| = 2
U(5): 1, 2, 3, 4,  |U(5)| = 4
U(6): 1, 5,  |U(6)| = 2
U(7): 1, 2, 3, 4, 5, 6,  |U(7)| = 6
U(8): 1, 3, 5, 7,  |U(8)| = 4
U(9): 1, 2, 4, 5, 7, 8,  |U(9)| = 6
U(10): 1, 3, 7, 9,  |U(10)| = 4
U(11): 1, 2, 3, 4, 5, 6, 7, 8, 9, 10,  |U(11)| = 10
U(12): 1, 5, 7, 11,  |U(12)| = 4
U(13): 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12,  |U(13)| = 12
U(14): 1, 3, 5, 9, 11, 13,  |U(14)| = 6
U(15): 1, 2, 4, 7, 8, 11, 13, 14,  |U(15)| = 8
U(16): 1, 3, 5, 7, 9, 11, 13, 15,  |U(16)| = 8
U(17): 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16,  |U(17)| = 16
U(18): 1, 5, 7, 11, 13, 17,  |U(18)| = 6
U(19): 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18,  |U(19)| = 18
U(20): 1, 3, 7, 9, 11, 13, 17, 19,  |U(20)| = 8
```

We may also use GAP commands to find the "structure description" of the group $U(n)$, as follows:

```
%gap
for k in [2..20] do
    G:= Units(Integers mod k);
    Print("U(",k,"): ", StructureDescription(G), "\n");
od;
```

The output is:

```
U(2): 1
U(3): C2
U(4): C2
U(5): C4
U(6): C2
U(7): C6
U(8): C2 x C2
U(9): C6
U(10): C4
U(11): C10
U(12): C2 x C2
U(13): C12
U(14): C6
U(15): C4 x C2
U(16): C4 x C2
U(17): C16
U(18): C6
U(19): C18
U(20): C4 x C2
```

(Here `C2` denotes the 2-element cyclic group, and `C2 x C2` is the direct product of `C2` with itself.)