Ex. 2 chap. 4

a) \(<5>\) in \(\mathbb{Z}_{12}: \{5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7, 0\}\)

so order 12.

In fact 5 and 12 are coprime so we know that 5 is a generator of \(\mathbb{Z}_{12}\).

b) Infinite order
c) Infinite order
d) \(<-i>\) in \(\mathbb{C}^*:\{<-i, -1, i, 1\}\) so order 4.
e) \(<72>\) in \(\mathbb{Z}_{240}\)\): can be computed by hand, but it is better to observe

\[\gcd(72, 240) = \gcd(72, 8 \times 3^2) = \gcd(72, 16 \times 5 \times 3) = \gcd(2^3 \times 3^2, 2^4 \times 5 \times 3) = 2^3 \times 3 = 24\]

so \(\gcd(72, 240) = 2^3 \times 3 = 24\)

and \(\frac{240}{24} = 10\) So order 10.

f) \(<312>\) in \(\mathbb{Z}_{471}\): by hand?...

Find the factors of \(471 = 3 \times 157\) and 157 is prime

\[312 = 3 \times 104\]

so \(\gcd(312, 471) = 3\) and \(\frac{471}{3} = 157\) so order 157.

Ex. 24 chap. 4

Generators of \(\mathbb{Z}_{pq}\) \[\leftrightarrow\] numbers so \(0 \leq n \leq pq - 1\) such that \(\gcd(n, pq) = 1\).

For \(n\) to be a generator, we need \(\gcd(n, pq) \neq 1\),

so \(n\) is a multiple of \(p\) or a multiple of \(q\).

There are \(q\) multiples of \(p\): \(0, p, 2p, \ldots, (q-1)p\)

and \(p\) multiples of \(q\): \(0, q, 2q, \ldots, (p-1)q\)

\(0\) is counted twice.
So \((p+q-1)\) elements between 0 and \(pq-1\) are not coprime. 

Hence there are \(pq - (p+q-1) = pq - p - q + 1\) generators.

**Ex. 37 chap. 4.** If \(G = \mathbb{Z}/k\mathbb{Z}\), it is clear that \(G\) is cyclic, so assume \(G\) has at least two elements.

Let \(g\) be in \(G\), with \(g \neq e\).

Consider \(<g>\). It is a subgroup. By assumption, it is not proper, non-trivial, so \(G = <g>\), and thus \(G\) is cyclic.

**Ex. 38 chap. 4.** This follows from the fact that \(G\) if \(|G| = n\), and \(G = <g>\), we have \(|g^k| = \frac{n}{\gcd(n,k)}\) which divides \(n\).

(for any \(k\))

**Ex. 12 chap. 4.** \(\mathbb{Z}/4\mathbb{Z}\) is a cyclic group with one generator.

\(\mathbb{Z}/4\mathbb{Z}\) has two generators: 1 and 3.

\(\mathbb{Z}/5\mathbb{Z}\) has four generators: 1, 2, 3, 4.

\(\mathbb{Z}/n\mathbb{Z}\) has \(\varphi(n)\) generators, where \(\varphi(n)\) is the number of elements \(k < n, k \perp n\) which are coprime with \(n\).

For any \(p\) prime, we get \(p-1\) generators.

In general, it is a complicated formula.
Ex. 17 chap 5  Done in class.

Take (12) and (23), they don't commute.

Ex. 18 chap 5  The previous example does not work because (12), (23) are not in An.

However, we now have a cycle (1234) and another (234)

\[
(123)(234) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \\
(234)(123) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}
\]

so they don't commute.