Chapter 3: Groups

43. Prove that the intersection of two subgroups of a group is also a subgroup.

Proof. Suppose H and K are two subgroups of a group G. In what follows, we use Proposition 3.9 to show that $H \cap K$ is a subgroup of G.

1. Since H is a subgroup of G, we must have $e \in H$, by definition of a subgroup. For the same reason $e \in K$. Therefore, $e \in H \cap K$, by definition of intersection.
2. Suppose $h_1, h_2 \in H \cap K$. Then $h_1, h_2 \in H$ and $h_1, h_2 \in K$ by definition of intersection. But then we have $h_1h_2 \in H$ and $h_1h_2 \in K$ since H and K are subgroups (and are closed under the group operation). Thus $h_1h_2 \in H \cap K$ by definition of intersection.

   We've now shown that whenever h_1 and h_2 are in $H \cap K$, the product h_1h_2 is also in $H \cap K$.
3. Suppose $h \in H \cap K$. Then $h \in H$ and $h \in K$, by definition of intersection. Therefore $h^{-1} \in H$ and $h^{-1} \in K$ because H and K are subgroups. Consequently $h^{-1} \in H \cap K$.

   We've now shown that whenever h is in $H \cap K$, the inverse h^{-1} is also in $H \cap K$.

Observations 1–3 above combined with Proposition 3.9 prove that $H \cap K$ is a subgroup of G.

Chapter 4: Cyclic Groups

4. (b) $H = \left\{ \begin{pmatrix} 0 & \frac{1}{3} \\ 3 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$

(d) $H = \left\{ \dots \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \dots \right\} = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in \mathbb{Z} \right\}$

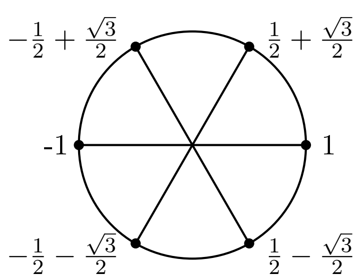
5. Find the order of every element in $\mathbb{Z}_{18}$.

The following table is made with the aid of Theorem 4.6. Since $a = 1$ is a generator of $\mathbb{Z}_{18}$ the theorem asserts that any $b = k \cdot a = k \cdot 1 = k \in \mathbb{Z}_{18}$ has order $\frac{18}{\gcd(k,18)}$.

element	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
order	1	18	9	6	9	18	3	18	9	2	9	18	3	18	9	6	9	18

20. List and graph the sixth roots of unity.

They are as follows: 1, $\quad \frac{1}{2} + \frac{\sqrt{3}}{2}, \quad -\frac{1}{2} + \frac{\sqrt{3}}{2}, \quad -1, \quad -\frac{1}{2} - \frac{\sqrt{3}}{2}, \quad \frac{1}{2} - \frac{\sqrt{3}}{2}$



The generators are $\frac{1}{2} + \frac{\sqrt{3}}{2}$ and $\frac{1}{2} - \frac{\sqrt{3}}{2}$. These are also the primitive sixth roots of unity.

23. Suppose $a, b \in G$. Prove the following statements.

(a) The order of a is the same as the order of a^{-1}.
Proof. Since we know that $(a^n)^{-1} = a^{-n} = (a^{-1})^n$, if follows that $a^n = e$ if and only if $(a^n)^{-1} = e^{-1}$, if and only if $(a^{-1})^n = e$. Thus the smallest n for which $a^n = e$ equals the smallest n for which $(a^{-1})^n = e$. Hence the order of a is the same as that of a^{-1}.

(b) For all $g \in G$, $|a| = |g^{-1}ag|$.
Proof. It suffices to show that $a^n = e$ if and only if $(g^{-1}ag)^n = e$, for then the smallest n for which $a^n = e$ equals the smallest n for which $(g^{-1}ag)^n = e$, so a and $g^{-1}ag$ have the same orders.

Suppose $a^n = e$. Then

$$(g^{-1}ag)^n = \underbrace{(g^{-1}ag)(g^{-1}ag)\cdots(g^{-1}ag)}_{g^{-1}ag \;\; n \text{ times}} = g^{-1}\underbrace{aaa\cdots a}_{a\ n \text{ times}}g = g^{-1}a^n g = g^{-1}eg = g^{-1}g = e.$$

Conversely suppose $(g^{-1}ag)^n = e$. This means

$$e = (g^{-1}ag)^n = \underbrace{(g^{-1}ag)(g^{-1}ag)\cdots(g^{-1}ag)}_{g^{-1}ag \;\; n \text{ times}} = g^{-1}\underbrace{aaa\cdots a}_{a\ n \text{ times}}g = g^{-1}a^n g.$$

Thus we have $e = g^{-1}a^n g$. Left-multiply both sides of this by g and you get $g = a^n g$. Now right-multiply both sides of this by g^{-1} and we have $e = a^n$.
The above has shown that $a^n = e$ if and only if $(g^{-1}ag)^n = e$, so it follows that $|a| = |g^{-1}ag|$.

(c) The order of ab is the same as the order of ba.
Proof. We will show that $(ab)^n = e$ if and only if $(ba)^n = e$, for then it follows that the smallest n for which $(ab)^n = e$ equals the smallest n for which $(ba)^n = e$, hence $|ab| = |ba|$.
Suppose $(ab)^n = e$, so

$$\underbrace{ab\,ab\,ab\,ab\cdots ab}_{ab\ n \text{ times}} = e.$$

Left-multiply both sides of this by a^{-1}, and you get $bababab\cdots ab = a^{-1}$. Now right-multiply both sides of this by a, and we get

$$\underbrace{ba\,ba\,ba\,ba\cdots ba}_{ba\ n \text{ times}} = e.$$

This means $(ba)^n = e$. Now we've shown that $(ab)^n = e$ implies $(ba)^n = e$. Reversing this process, we see that $(ba)^n = e$ implies $(ab)^n = e$.

Thus we've shown $(ab)^n = e$ if and only if $(ba)^n = e$. Therefore ab and ba have the same order.

24. Let p and q be distinct primes. How many generators does $\mathbb{Z}_{pq}$ have?

By Corollary 4.7, the generators of $\mathbb{Z}_{pq}$ are the integers r for which $1 \leq r < pq$ and $\gcd(r, pq) = 1$.

Therefore, the elements $r \in \mathbb{Z}_{pq}$ that are *not* generators are those r for which $0 \leq r < pq$ and $\gcd(r, pq) \neq 1$. This happens if and only if r and pq have a common factor other than 1. But the only factors of pq between 1 and pq are p and q. Thus for r not to be a generator, it must be a multiple of p or q.

Thus the following values of r are the only ones for which r is not a generator:

$$\begin{array}{cccccc} 0 & p & 2p & 3p & 4p & \ldots(q-1)p \\ & q & 2q & 3q & 4q & \ldots(p-1)q \end{array}$$

There are $1 + (q-1) + (p-1)$ such values. In other words, $\mathbb{Z}_{pq}$ has exactly $1 + (q-1) + (p-1)$ elements that are *not* generators. The other elements *are* generators.

Thus $\mathbb{Z}_{pq}$ has $pq - (1 + (q-1) + (p-1)) = \boxed{(p-1)(q-1) \text{ generators.}}$