Chapter 6: Cosets and Lagrange's Theorem

5. List the left- and right-cosets of each of the following:

(b) $\langle 3\rangle$ in $U(8)$.

The group $U(8)$ consists of the units in $\mathbb{Z}_8$, that is $U(8) = \{1, 3, 5, 7\}$.

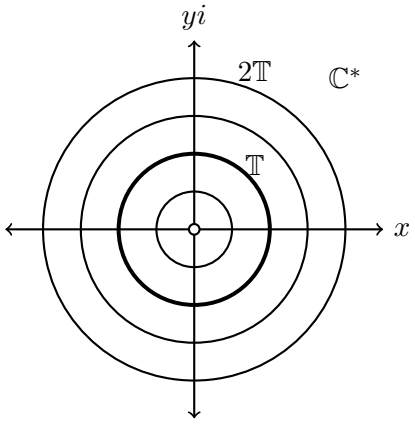
Notice that $\langle 3\rangle = \{3^n : n \in \mathbb{Z}\} = \{1, 3\}$.

Thus the left-cosets of $\langle 3\rangle$ are $\boxed{1\langle 3\rangle = \{1, 3\} \text{ and } 5\langle 3\rangle = \{5, 7\}.}$

Since $U(8)$ is abelian, the right cosets are the same.

(g) $\mathbb{T}$ in $\mathbb{C}^*$.

Since $\mathbb{C}^*$ is abelian, the left cosets will be the same as the right cosets, so it suffices to describe only the left cosets $\omega\mathbb{T}$. Take an element $\omega \in \mathbb{C}^*$, and consider the left coset $\omega\mathbb{T}$. Any element of this coset must have form ωz with $z \in \mathbb{T}$. Notice that $|\omega z| = |\omega| \cdot |z| = |\omega| \cdot 1 = |\omega|$. This means any element of $\omega\mathbb{T}$ is on the circle of radius $|\omega|$ centered at the origin. That is, $\omega\mathbb{T} \subseteq |\omega|\mathbb{T}$, and by Lemma 6.1, $\omega\mathbb{T} = |\omega|\mathbb{T}$. In words, any left coset $\omega\mathbb{T}$ is a circle of radius $|\omega|$ in $\mathbb{C}^*$, centered at the origin. Following is a picture of some left cosets of $\mathbb{T}$.



12 Suppose H is a subgroup of a group G. If $ghg^{-1} \in H$ for every $g \in G$ and $h \in H$, then left cosets are identical to right cosets.

Proof. Let G and H be as stated, and suppose $ghg^{-1} \in H$ for every $g \in G$ and $h \in H$. Given an arbitrary $g \in G$, we need to show that $gH = Hg$.

Thus take an arbitrary $g \in G$. We will show $gH = Hg$ by showing $gH \subseteq Hg$ and $Hg \subseteq gH$.

First we show $gH \subseteq Hg$. Suppose $x \in gH$. This means $x = gh$ for some $h \in H$. Then also $x = ghe = gh(g^{-1}g) = (ghg^{-1})g$. By assumption, $ghg^{-1} = h' \in H$, so the above gives $x = h'g \in Hg$. We have shown $x \in gH$ implies $x \in Hg$, so $gH \subseteq Hg$.

Next we show $Hg \subseteq gH$. Suppose $x \in Hg$. This means $x = hg$ for some $h \in H$. Then also $x = ehg = (gg^{-1})h(g^{-1})^{-1} = g(g^{-1}h(g^{-1})^{-1})$. By assumption, $g^{-1}h(g^{-1})^{-1} = h' \in H$, so the above gives $x = gh' \in gH$. We have shown $x \in Hg$ implies $x \in gH$, so $Hg \subseteq gH$.

It now follows that $gH = Hg$. ■

14 Suppose an element g in a group satisfies $g^n = e$. Show that the order of g divides n.

Proof. Suppose $g^n = e$ and the order of g is k, that is, k is the smallest natural number for which $g^k = e$. We need to show $k|n$.

By the division algorithm, there are integers q and r, with $0 \leq r < k$ for which

$$n = qk + r. \tag{1}$$

Now observe that

$$e = g^n = g^{qk+r} = g^{qk}g^r = (g^k)^q g^r = e^q g^r = eg^r = g^r.$$

Therefore we have shown $e = g^r$. But recall that $0 \leq r < k$, and k is smallest natural number for which $g^k = e$. It follows that $r = 0$. Now Equation (1) gives $n = qk$, so $k|n$. We have now shown that the order of g divides n. ■

18. If $[G : H] = 2$, prove that $gH = Hg$.

Proof. Suppose $[G : H] = 2$, which means are only two left-cosets of H in G. One of these cosets is H (as $H = eH$). Since the left cosets partition G, and there are only two cosets, the other coset besides H must be the set difference $G \setminus H$. **Thus the two left cosets are H and $G \setminus H$.**

By Theorem 6.3, there are also just two right-cosets of H in G. Reasoning as in the previous paragraph, we see that **the two right cosets must be H and $G \setminus H$.**

Now consider two cosets gH and Hg. By the previous paragraph, each one equals either the set H or the set $G \setminus H$. Now g is in both gH and Hg, but g is **not** in both H and $G \setminus H$. It follows that it is impossible for one of gH and Hg to be H and the other to be $G \setminus H$. Therefore either both gH and Hg equal H, or both equal $G \setminus H$. Either way we have $gH = Hg$. ■

21. If G is a group of order p^n, where $n \geq 2$ and p is a prime, show that G must have a proper subgroup H of order p.

Proof. Assume a group G has order p^n, where p is prime and $n \geq 2$. Take a non-identity element $a \in G$. By Lagrange's Theorem, $|\langle a \rangle|$ must divide p^n, so $|\langle a \rangle|$ is one of the numbers $p, p^2, p^3, \ldots, p^n$. Thus $|\langle a \rangle| = p^m$ for some integer m with $1 \leq m \leq n$. Thus

$$\langle a \rangle = \{a^1, a^2, a^3, a^4, \ldots, a^{p^m - 1}, a^{p^m}\},$$

where the final element listed is $a^{p^m} = e$. Thus we have

$$e = a^{p^m} = a^{p^{m-1}p} = \left(a^{p^{m-1}}\right)^p$$

It follows that $a^{p^{m-1}} \in G$ has order p. Therefore $H = \langle a^{p^{m-1}} \rangle$ is a subgroup of G with order p. ■

Chapter 3, #50. If $xy = x^{-1}y^{-1}$ for every $x, y \in G$, then G is abelian.

Proof. Suppose $xy = x^{-1}y^{-1}$ for every $x, y \in G$. Then given any $x \in G$, we can set $y = e$, and get $xe = x^{-1}e^{-1}$, which yields $x = x^{-1}$. Thus $xx = e$ for each $x \in G$.

Now take any $a, b \in G$. By the above, we must have $(ab)(ab) = e$, or $abab = e$. Left-multiply both sides of this by a to get $aabab = a$. Now right-multiply both sides of *this* by b to get $aababb = ab$, which is $(aa)ba(bb) = ab$. Using the fact that $aa = e$ and $bb = e$, this becomes $ba = ab$. It follows that G is abelian. ■