Problem 9.
In each case give a geometric description of the cosets of $H$ in $G$
(b) $G = (\mathbb{C}^*, \cdot)$ and $H = \mathbb{R}^*$

Solution.
The group $(\mathbb{C}^*, \cdot)$ is abelian, so for every $z \in \mathbb{C}^*$ we have $zH = Hz$.
Let $z = x_0 + iy_0 \in \mathbb{C}^*$ be arbitrary, where $x_0, y_0 \in \mathbb{R}$ are such that $x_0^2 + y_0^2 \neq 0$.
Then
$$zH = Hz = \{rz \mid r \in \mathbb{R}, r \neq 0\} = \{rx_0 + iry_0 \mid r \in \mathbb{R}, r \neq 0\}.$$
Thus the coset $Hz$ is exactly the line in $\mathbb{C}$ through the origin and passing through $z$,
with the origin removed from this line.
So the cosets of $H$ in $G$ are lines through the origin with the origin removed from them.
(d) $G = (\mathbb{C}, +)$ and $H = \mathbb{R}$.

Solution.
Let $z = x_0 + iy_0 \in \mathbb{C}$ be arbitrary, where $x_0, y_0 \in \mathbb{R}$. Then, since $G = (\mathbb{C}, +)$ is abelian, we have
$$z + H = H + z = \{(r + x_0) + iy_0 \mid r \in \mathbb{R}\} = \{x + iy_0 \mid x \in \mathbb{R}\}$$
is the horizontal line in $\mathbb{C}$ passing through $z$.
Thus the cosets of $H$ in $G$ are the horizontal lines in $\mathbb{C}$.

Problem 10.
(a) If $G = \langle a \rangle$ and $|a| = 30$, find the index of $\langle a^6 \rangle$ in $G$.

Solution.
We have $|G| = |a| = 30$. Also, $|a^6| = \frac{30}{6} = 5$ and hence $|\langle a^6 \rangle| = 5$. Therefore by Lagrange’s Theorem $[G : \langle a^6 \rangle] = \frac{|G|}{|\langle a^6 \rangle|} = \frac{30}{5} = 6$.
(b) Let $G = \langle a \rangle$, $|a| = n$. If $d|n$, find the index of $\langle a^d \rangle$ in $G$.

Solution.
We have $|G| = |a| = n$. Let $d \geq 1$ be such that $d|n$. Since $d|n$, we know that $|a^d| = n/d$. Therefore $|\langle a^d \rangle| = |a^d| = n/d$. Hence by Lagrange’s Theorem
$$[G : \langle a^d \rangle] = \frac{|G|}{|\langle a^d \rangle|} = \frac{n}{n/d} = d.$$

Problem 12.
Let $G$ be a group and let $g \in G$. In each case show that $G = \langle g \rangle$.
(a) $|G| = 12, g^4 \neq 1, g^6 \neq 1$.

Solution.
We know that $|g||G|$, that is $|g||12$. Hence $|g| \in \{1, 2, 3, 4, 6, 12\}$. Since by assumption $g^4 \neq 1, g^6 \neq 1$, we have $|g| \neq 4$ and $|g| \neq 6$. This also implies that $|g| \neq 2$ since if $|g| = 2$ then $g^2 = 1$ and hence $g^4 = (g^2)^2 = 1$, contrary to our assumption that $g^4 \neq 1$. Similarly, $|g| \neq 3$ since if $|g| = 3$ then $g^3 = 1$ and hence $g^6 = (g^3)^2 = 1$, contrary to our assumptions. Finally, $|g| \neq 1$ since if $|g| = 1$ then $g = 1$ and $g^n = 1$ for every $n \in \mathbb{Z}$, contrary to the fact that $g^4 \neq 1$. Thus $|g| \neq 1,$
\(|g| \neq 2, \, |g| \neq 3, \, |g| \neq 4 \text{ and } |g| \neq 6. \) It follows that \(|g| = 12. \) Hence \(|\langle g \rangle| = |g| = 12\) and since \(|G| = 12\) and \(|\langle g \rangle| \subseteq G\), it follows that \(|\langle g \rangle| = G\).

(c) \(|G| = 60, \, g^{30} \neq 1, \, g^{20} \neq 1 \text{ and } g^{12} \neq 1.\)

\textbf{Solution.} \\
Since \(|g|\|[G|, \text{ that is } |g|\|60 \text{ and } 60 = 2^2 \cdot 3^1 \cdot 5^1, \text{ we know that } |g| \text{ is a divisor of } 60, \text{ that is } |g| = 2^{\alpha_1}3^{\alpha_2}5^{\alpha_3}, \text{ where } 0 \leq \alpha_1 \leq 2, \, 0 \leq \alpha_2 \leq 1, \, 0 \leq \alpha_3 \leq 1. \) \n
We claim that \(|g| = 60. \) Indeed, suppose not and \(|g| < 60. \) Then \(|g| = 2^{\alpha_1}3^{\alpha_2}5^{\alpha_3}, \) where \(0 \leq \alpha_1 \leq 2, \, 0 \leq \alpha_2 \leq 1, \, 0 \leq \alpha_3 \leq 1 \) and where either \(\alpha_1 < 2 \) or \(\alpha_2 < 1 \) or \(\alpha_3 < 1.\)

If \(\alpha_1 < 2 \) then \(30 = \frac{60}{2} \) is an integer multiple of \(|g|, \) that is \(30 = s|g| \) for some integer \(s \geq 1.\) Then \(g^{30} = (g|g|^s) = 1, \) contrary to our assumptions.

If \(\alpha_2 < 1, \) then \(20 = \frac{60}{3} \) is an integer multiple of \(|g|, \) that is \(20 = s|g| \) for some integer \(s \geq 1.\) Then \(g^{20} = (g|g|^s) = 1, \) contrary to our assumptions.

If \(\alpha_3 < 1, \) then \(12 = \frac{60}{5} \) is an integer multiple of \(|g|, \) that is \(12 = s|g| \) for some integer \(s \geq 1.\) Then \(g^{12} = (g|g|^s) = 1, \) contrary to our assumptions.

Thus \(|g| = 60 as claimed. \) Therefore \(|\langle g \rangle| = |g| = 60 = |G| \) and hence \(|\langle g \rangle| = G, \) as required.

(d) Generalize.

\textbf{Solution.} \\
Let \(|G| = n \geq 2, \) let \(n = p_1^{m_1} \cdots p_k^{m_k}, \) where \(m_i \geq 1, \) be the prime factorization of \(n. \) Suppose that \(g^{n/p_i} \neq 1 \) for each \(i = 1, \ldots, k. \) Then \(G = \langle g \rangle.\)

\textbf{Proof.} We know that \(|g|\|[G|, \) that is

\[ |g| = |g| |G| = p_1^{m_1} \cdots p_k^{m_k}. \]

Therefore \(|g| = p_1^{m_1} \cdots p_k^{m_k} \) where \(0 \leq \alpha_i \leq m_i \) for \(i = 1, \ldots, k. \) We claim that \(|g| = n. \) Indeed, suppose not and \(|g| < n. \)

Then \(|g| = p_1^{m_1} \cdots p_k^{m_k} \) where \(0 \leq \alpha_i \leq m_i \) for \(i = 1, \ldots, k \) and \(\alpha_j < m_j \) for some \(j \in \{1, \ldots, k\} \) such that \(0 \leq \alpha_j < m_j. \)

Then \(\frac{n}{p_j} = p_1^{m_1} \cdots p_{j-1}^{m_{j-1}} p_j^{m_j-1} p_{j+1} \cdots p_k^{m_k} \) is an integer multiple of \(|g|, \) that is \(\frac{n}{p_j} = s|g| \) for some integer \(s \geq 1.\) Hence \(g^{n/p_j} = (g|g|^s) = 1, \) contrary to our assumptions.

Thus indeed \(|g| = n. \) Therefore \(|\langle g \rangle| = |g| = n = |G| \) and hence \(G = \langle g \rangle, \) as claimed.

\square

\textbf{Problem 13.} \\
Let \(K = \{e, (1 \, 2)(3 \, 4), (1 \, 3)(2 \, 4), (1 \, 4)(2 \, 3)\} \subseteq A_4\) and let \(H\) be a subgroup of \(A_4\) containing \(K. \) If \(H\) contains a 3-cycle, prove that \(H = A_4. \)

\textbf{Solution.} \\
Recall that \(|A_4| = 1 \cdot 4! = 12 \) and, obviously, \(|K| = 4. \) Hence by Lagrange’s theorem, \(|A_4 : K| = \frac{|A_4|}{|K|} = \frac{12}{4} = 3. \) Since \(K \leq H \leq A_4\) and the index \(|A_4 : K| = 3\) is a prime, Example 6 in Ch. 2.6 implies that either \(H = K\) or \(H = A_4. \) Since \(H\) contains some 3-cycle, we have \(H \neq K. \) Therefore \(H = A_4. \)

\textbf{Problem 17.}
Let \( |G| = p^2 \), where \( p \) is a prime. Prove that every proper subgroup of \( G \) is cyclic.

**Solution.**

Let \( H \leq G \) be a proper subgroup, that is a subgroup such that \( H \neq \{1\} \) and \( H \neq G \). Thus \( 1 < |H| < p^2 \). By Lagrange’s Theorem \( |H|||G| \), that is \( |H||p^2| \). Since \( p \) is a prime, the only positive divisor of \( p^2 \) different from 1 and \( p^2 \) is \( p \). Hence \( |H| = p \). Therefore by Corollary 3 in Ch. 2.6 the group \( H \) is cyclic.

**Problem 20.** Show that \( |Z_n^*| \) is even for \( n \geq 3 \).

**Solution.**

Since \( n \geq 3 \), we have \(-1 \neq 1 \) in \( Z_n \). We also have \((-1)^2 = 1 \). Therefore the element \(-1 \) has order 2 in \( Z_n^* \). Hence by Corollary 2 in Ch. 2.6, we have \( 2|Z_n^*| \), that is \( |Z_n^*| \) is even.

**Problem 25.**

(a) In \( D_n \) show that \( a^kba^k = b \) for all \( k \in \mathbb{Z} \).

**Solution.**

We have \( aba = b \) in \( D_n \). This implies that \( ab = ba^{-1} \). Therefore, inductively, we have \( a^kba = ba^{-k} = b \) for every \( k \geq 1 \). Thus for \( k \geq 1 \) we have

\[
a^kba^k = ba^{-k}a^k = b,
\]
as required. By pre- and post-multiplying this equality by \( a^{-k} \), it follows that that \( b = a^{-k}ba^{-k} \) for every \( k \geq 1 \). Finally, for \( k = 0 \) it is obvious that \( a^0ba^0 = b \). Thus the equality \( a^kba^k = b \) holds for all \( k \in \mathbb{Z} \).

(b) In \( D_n \) show that \( |ba^k| = 2 \) for all \( k \in \mathbb{Z} \).

**Solution.**

Let \( k \in \mathbb{Z} \) be arbitrary.

Using the result of part (a), we have

\[
(ba^k)^2 = ba^kba^k = bb = 1
\]
since \( |b| = 2 \).

Note also that, since \( |a| = n \), if \( k \equiv j \mod n \) and \( 0 \leq j \leq n - 1 \) then \( a^k = a^j \) and hence \( ba^k = ba^j \). By definition of \( D_n \) we have \( ba^j \neq 1 \). Thus \( (ba^k)^2 \neq 1 \) but \( (ba^k)^2 = 1 \). Therefore \( |ba^k| = 2 \), as required.

**Problem 26.**

If \( n \geq 3 \), show that \( Z(D_n) = \{1\} \) when \( n \) is odd and that \( Z(D_n) = \{1, a^m\} \) when \( n = 2m \) is even.

**Solution.**

Recall that

\[
D_n = \{1, a, a^2, \ldots, a^{n-1}, b, ba, \ldots, ba^{n-1}\},
\]

where \( |a| = n \), \( |b| = 2 \) and \( aba = b \). The last equation gives us \( ab = ba^{-1} \), and hence \( ab^i = ba^{-i} \) for every \( i \geq 1 \), the fact that we will repeatedly use below.

We first show that if \( n \geq 3 \) then for \( j = 0, 1, \ldots, n - 1 \) we have \( ba^j \notin Z(D_n) \). Indeed, let \( 0 \leq j \leq n - 1 \). Then we have:

\[
ba^j(a(ba^j))^{-1} = ba^jaa^{-j}b^{-1} = bab^{-1} = a^{-1}bb^{-1} = a^{-1}.
\]

If \( n \geq 3 \), then since \( |a| = n \), we have \( a \neq a^{-1} \), so that \( ba^j(a(ba^j))^{-1} \neq a \) and hence \( ba^j \notin Z(D_n) \).
Thus we have established that $Z(D_n) \subseteq \{1, a, a^2, \ldots, a^{n-1}\}$. Clearly $1 \in Z(D_n)$.

Suppose now that $a^i \in Z(D_n)$ for some $1 \leq i \leq n - 1$. Then $a^i ba^{-i} = b$ and hence

$$b = a^i ba^{-i} = ba^{-i}a^{-i} = ba^{-2i}$$

which yields $a^{2i} = 1$, that is $n|2i$. Recall that $1 \leq i \leq n - 1$. If $n \geq 3$ is odd then there does not exist $i \in \{1, 2, \ldots, n - 1\}$ such that $n|2i$. Hence for odd $n \geq 3$ we have $Z(D_n) = \{1\}$, as required.

Suppose now that $n = 2m \geq 3$ is even, so that $n \geq 4$ and $m \geq 2$. Then there is a unique $i \in \{1, 2, \ldots, n - 1\}$ such that $n|2i$, namely $i = n/2 = m$. Thus for even $n = 2m \geq 3$ we have $Z(D_n) \subseteq \{1, a^m\}$.

It remains to verify that in this case we do in fact have $a^m \in Z(D_n)$. It is obvious that $a^m a^j a^{-m} = a^j$ for every $0 \leq j \leq n - 1$. Apart from powers of $a$, the only other elements of $D_n$ have the form $ba^j$, $0 \leq j \leq n$. We have

$$a^m ba^j a^{-m} = ba^{-m}a^j a^{-m} = ba^{j-2m} = ba^{j-n} = ba^j,$$

where the last equality holds since $|a| = n$. Thus $a^m$ commutes with every element of $D_n$. Therefore for $n = 2m \geq 3$ even, we have $Z(D_n) = \{1, a^m\}$, as claimed.