1. Fill in the multiplication table for the group S_3. (You don't need to show the details of computation)

   Solution:

S_3	id	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
id	id	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1 2)	(1 2)	id	(1 3 2)	(123)	(2 3)	(1 3)
(1 3)	(1 3)	(1 2 3)	id	(1 3 2)	(1 2)	(2 3)
(2 3)	(2 3)	(1 3 2)	(1 2 3)	id	(1 3)	(1 2)
(1 2 3)	(1 2 3)	(1 3)	(2 3)	(1 2)	(1 3 2)	id
(1 3 2)	(1 3 2)	(2 3)	(1 2)	(1 3)	id	(1 2 3)

2. G is a group and $x \in G$. Define $C(x) = \{g \in G | gx = xg\}$. Prove $C(x)$ is a subgroup of G.

   Solution:

   For any $a, b \in C(x)$: $ax = xa$, $a^{-1}(ax)a^{-1} = a^{-1}(xa)a^{-1}$, $xa^{-1} = a^{-1}x$

   It follows $(a^{-1}b)x = a^{-1}(bx) = a^{-1}(xb) = (xa^{-1})b = x(a^{-1}b)$, so $a^{-1}b \in C(x)$, $C(x)$ is a subgroup of G.

3. H and K are subgroups of G. Prove that $H \cup K$ is a subgroup of G if and only if $H \subseteq K$ or $K \subseteq H$.

   Solution:

   If $H \subseteq K$ or $K \subseteq H$, then $H \cap K = K$ or $H \cap K = H$, so $H \cap K$ is a subgroup of G.

   If $H \not\subset K$ and $K \not\subset H$, then there exists $h \in H \setminus K$ and $k \in K \setminus H$. Suppose $H \cup K$ is a subgroup of G, then $hk \in H \cup K$. If $hk \in H$, then $k = h^{-1}(hk) \in H$, contradiction; if $hk \in K$, then $h = (hk)k^{-1} \in K$, contradiction. So $H \cup K$ is not a subgroup of G.

4. G is a group, $g \in G$ and $|g|$ is an odd number. Prove there exists $k \in \mathbb{Z}$ such that $g = g^{2k}$.

   Solution: $|g|$ is odd, so $|g|$ and 2 are relatively prime, which implies the existence of $k, l \in \mathbb{Z}$ such that $2k + |g|l = 1$. So:

$$g = g^1 = g^{2k+|g|l} = g^{2k}(g^{|g|})^l = g^{2k}1 = g^{2k}$$

5. a and b are nonzero integers.

   (i). Show that there exists nonzero $m \in \mathbb{Z}$ such that $m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$. (This m is defined to be the **least common multiple** of a and b)

   (ii). Prove m is divisible by both a and b.

   (iii). If n is an integer divisible by both a and b, then m divides n.

   (iv). If d is the greatest common divisor of a and b, prove $ab = dm$.

   Solution: (i). Since $a\mathbb{Z}$ and $b\mathbb{Z}$ are subgroups of $\mathbb{Z}$, by Question 1, their intersection $a\mathbb{Z} \cap b\mathbb{Z}$ is also a subgroup of $\mathbb{Z}$, so it is of the form $m\mathbb{Z}$ for some $m \in \mathbb{Z}$. Note that a, b are nonzero, ab is a nonzero number such that $ab \in a\mathbb{Z} \cap b\mathbb{Z}$, so $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z} \neq \{0\}$, we see $m \neq 0$.

   (ii). $m \in m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$, so $m \in a\mathbb{Z}$ and $m \in b\mathbb{Z}$, which implies a divides m and b divides m.

   (iii). If n is divisible by both a and b, then $n \in a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$, so n is divisible by m.

   (iv). it suffices to show $ab|md$ and $md|ab$.

   Since d is the greatest common divisor of a, b, we get $\frac{b}{d}$ and $\frac{a}{d}$ are integers. Observe that $\frac{ab}{d} = a\frac{b}{d} = b\frac{a}{d}$, this implies $\frac{ab}{d}$ is divisible by both a and b, By (iii), $m|\frac{ab}{d}$, i.e. $md|ab$.

   Next consider $\frac{ab}{m}$. since ab is divisible by both a and b, by (iii), $m|ab$, so $\frac{ab}{m}$ is an integer. $a = \frac{ab}{m}\frac{m}{b}$ and $b = \frac{ab}{m}\frac{m}{a}$, and by (ii), $\frac{m}{a}$ and $\frac{m}{b}$ are also integers, we see $\frac{ab}{m}$ divides both a and b. By the property of greatest common divisor, we get $\frac{ab}{m}|d$, i.e. $ab|md$

6. G is a group, $g \in G$. Prove $|g| = |xgx^{-1}|$ for any $x \in G$.

   Solution: For any $k \in \mathbb{N}$, $(xgx^{-1})^k = xg^kx^{-1}$. This implies

   $$g^k = 1 \iff (xgx^{-1})^k$$

   Since the order of an element is the smallest positive power to which the element is identity, we conclude $|g| = |xgx^{-1}|$.

7. x is an element of order n in a group G. k is an integer such that the greatest common divisor of k and n is d. Prove $< x^k > = < x >$ if and only if $d = 1$

   Solution: If $d > 1$, then we see $(x^k)^{\frac{n}{d}} = x^{\frac{kn}{d}} = (x^n)^{\frac{k}{d}} = 1$, so by the definition of $|x^k|$, $| < x^k > | = |x^k| \leq \frac{n}{d} < n = | < x > |$, $< x^k > \neq < x >$.

If $d = 1$, it suffices to prove $x \in < x^k >$, which implies $< x > \subset < x^k >$, and $< x^k > \subset < x >$ is trivial, then we can conclude $< x > = < x^k >$. $d = 1$ implies there exists integers p, q such that $np + kq = 1$. Thus $x = x^{np+kq} = x^{np}x^{kq} = x^{kq} = (x^k)^q$, we see $x \in < x^k >$.