

H/wk 6, Solutions to selected problems

Problem 7.

Let $g \in G$ be such that $|g| = 20$.

Compute the orders:

- (a) $|g^2|$;
- (b) $|g^8|$;
- (c) $|g^5|$;
- (d) $|g^3|$;

Solution.

All parts of this problem can be solved by directly using the definition of order of an element (the smallest positive power that is equal to the identity) and the fact that if $|g| = n$ then for $m \in \mathbb{Z}$ we have $g^m = 1$ if and only if m is divisible by n .

Note also, that by part (2) of Theorem 7 in Ch 2.4 we know that if $d \geq 1$ is a divisor of n then $|g^d| = |\langle g^d \rangle| = n/d$.

(a) Since $2|20$, we have $|g^2| = 20/2 = 10$.

(c) Since $5|20$, we have $|g^5| = 20/5 = 4$.

(d) Since $\gcd(3, 20) = 1$, Theorem 6 in Ch 2.4 implies that g^3 is a generator of $\langle g \rangle$, that is $\langle g^3 \rangle = \langle g \rangle$. Therefore $|g^3| = |\langle g^3 \rangle| = |\langle g \rangle| = |g| = 20$.

Alternatively, it is easy to see that the smallest positive integer $m \geq 1$ such that $3m$ is divisible by 20 is $m = 20$ and hence $|g^3| = 20$.

(b) It is not hard to see that the smallest positive integer m such that $8m$ is divisible by 20 is $m = 5$ and hence $|g^8| = 5$.

Here is a more general alternative argument: We claim that $\langle g^8 \rangle = \langle g^4 \rangle$. There is a statement, embedded in the proof of Theorem 7 which says the following: Let $|g| = n$. Then for any $k \geq 1$ if $d = \gcd(k, n)$ then $\langle g^d \rangle = \langle g^k \rangle$ and hence $|g^k| = |\langle g^k \rangle| = |\langle g^d \rangle| = |g^d| = n/d$. If we accept this statement (a proof of which is given below), then since $\gcd(8, 20) = 4$, we have

$$|g^8| = |\langle g^8 \rangle| = |\langle g^4 \rangle| = |g^4| = 20/4 = 5.$$

Claim. Let $g \in G$ have $|g| = n \geq 1$. Let $d = \gcd(k, n)$. Then for any $k \in \mathbb{Z}$ we have $\langle g^k \rangle = \langle g^d \rangle$ and hence $|g^k| = |g^d| = n/k$.

Proof. Since $d|k$ and $k = qd$ for some $q \in \mathbb{Z}$, we have $g^k = (g^d)^q$. Therefore $g^k \in \langle g^d \rangle$ and hence $\langle g^k \rangle \subseteq \langle g^d \rangle$.

Since $d = \gcd(k, n)$, there exist $x, y \in \mathbb{Z}$ such that $d = xk + yn$. Hence

$$g^d = (g^k)^x (g^n)^y = (g^k)^x \in \langle g^k \rangle.$$

and therefore $\langle g^d \rangle \subseteq \langle g^k \rangle$. This implies that $\langle g^d \rangle = \langle g^k \rangle$ as claimed. We also have in this case:

$$|g^k| = |\langle g^k \rangle| = |\langle g^d \rangle| = |g^d| = n/d$$

where the last equality holds by Theorem 7. □

Problem 16. In each case find $H = \langle x, y \rangle \leq G$.

(a) $G = \langle a \rangle$ is cyclic and $x = a^4, y = a^3$.

Solution.

Notice that $a = a^4(a^3)^{-1}$. Hence, by Theorem 8 from Ch 2.4, $a \in H = \langle a^4, a^3 \rangle$. This implies that $\langle a \rangle \leq H \leq G = \langle a \rangle$ and therefore $H = G = \langle a \rangle$.

(b) $G = \langle a \rangle$ is cyclic, $x = a^6$ and $y = a^8$.

Solution.

By Theorem 8 every element of $H = \langle a^6, a^8 \rangle$ is some product of powers of a^8 and a^6 and hence is equal to some even power of a . This implies that $H \subseteq \langle a^2 \rangle$.

On the other hand $a^2 = a^8 \cdot (a^6)^{-1}$ which shows that $a^2 \in H$ and therefore $\langle a^2 \rangle \subseteq H$. Since we have already established that $H \subseteq \langle a^2 \rangle$, it follows that $H = \langle a^2 \rangle$.

(c) $G = \langle a \rangle$ is cyclic, $x = a^m$, $y = a^k$ and $d = \gcd(m, k)$.

Solution.

We claim that $H = \langle a^d \rangle$.

First, since d is a divisor of both m and k , we have $m = qd$, $k = pd$ and $a^m = (a^d)^q$ and $a^k = (a^d)^p$. By Theorem 8 every element of H is a product of some powers of a^m and a^k and hence is a power of a^d . This shows that $H \subseteq \langle a^d \rangle$.

Also, since $d = \gcd(m, k)$, there exist integers u, v such that $d = um + vk$. Then

$$a^d = a^{um+vk} = (a^m)^u (a^k)^v \in H = \langle a^m, a^k \rangle.$$

This $a^d \in H$ and hence $\langle a^d \rangle \subseteq H$. Since we already know that $H \subseteq \langle a^d \rangle$, it follows that $H = \langle a^d \rangle$, as claimed.

(d) $G = S_3$, $x = (1\ 2)$, $y = (2\ 3)$.

Solution.

Note that $H = \langle (1\ 2), (2\ 3) \rangle \subseteq S_3$. We claim that $H = S_3$, so we need to show that $S_3 \subseteq H$.

We have $(1\ 2)(2\ 3)(1\ 2) = (1\ 3)$ and therefore $(1\ 3) \in H$ by Theorem 8.

Recall that by the results of Ch. 1.4, every element of S_3 can be written as a product of transpositions. There are only three transpositions in S_3 , namely $(1\ 2)$, $(2\ 3)$ and $(1\ 3)$ and they all belong to H . Therefore every permutation in S_3 belongs to H , and hence $H = S_3$.

Alternatively, we can explicitly see that $\epsilon = (1\ 2)(1\ 2)$, $(1\ 2)(2\ 3) = (1\ 2\ 3)$ and $(2\ 3)(1\ 2) = (3\ 2\ 1)$ which implies that $\epsilon \in H$, $(1\ 2\ 3) \in H$ and $(3\ 2\ 1) \in H$. Thus every element of S_3 belongs to H and hence $H = S_3$.

(e) $G = \langle a \rangle \times \langle b \rangle$ where $|a| = |b| = 4$ and $x = (a^3, b)$, $y = (a, b)$.

Solution.

We need to find $H = \langle (a^3, b), (a, b) \rangle$.

Consider the set

$$G_1 = \{ (a^i, b^j) : i, j \in \mathbb{Z}, \text{ and } i + j \text{ is even} \} = \\ \{ (1, 1), (a, b), (a^2, 1), (1, b^2), (a^2, b^2), (a^3, b), (b^3, a), (a^3, b^3) \} \subseteq G.$$

One can verify directly that $G_1 \leq G$ is a subgroup of G (check that G_1 is closed under multiplication and inversion).

We claim that $H = G_1$.

Since $(a^3, b) \in G_1$, $(a, b) \in G_1$ and G_1 is a subgroup of G , part (2) of Theorem 8 in Ch. 2.4 implies that $H \subseteq G_1$.

We need to establish the opposite inclusion, $G_1 \subseteq H$.

First $(a, b) \in H$ implies $\langle (a, b) \rangle \subseteq H$, so that $(a^2, b^2) \in H$ and $(a^3, b^3) \in H$. Also, $(a^3, b), (a, b) \in H$ implies that $(a^2, 1) = (a^3, b)(a, b)^{-1} \in H$ and $(1, b^2) = (a^4, b^2) = (a^3, b)(a, b) \in H$.

Since $(a^2, 1) \in H$ and $(a, b) \in H$ and H is a subgroup, it follows that $(a^3, b) = (a^2, 1)(a, b) \in H$.

Finally, since $(1, b^2) \in H$ and $(a, b) \in H$ and since H is a subgroup, it follows that $(a, b^3) = (1, b^2)(a, b) \in H$. Finally, $(1, 1) \in H$ since $(1, 1)$ is the identity element in G and since H is a subgroup of G . Thus we have checked that every single element of G_1 belongs to H , so that $G_1 \subseteq H$. Since we already know that $H \subseteq G_1$, it follows that $H = G_1$.

(f) $G = \langle a \rangle \times \langle b \rangle$ where $|a| = 4$, $|b| = 6$ and $x = (a^2, b)$, $y = (a, b^3)$.

Solution.

We claim that $H = G$ in this case. By problem no. 18 in order to prove that $G = H$ it suffices to show that $(a, 1) \in H$ and $(1, b) \in H$.

We have:

Since $(a^2, b) \in H$, it follows that $(a^2, b)^2 = (1, b^2) \in H$.

Since $(1, b^2) \in H$ and $(a, b^3) \in H$, it follows that $(a, b^3)(1, b^2)^{-1} = (a, b) \in H$.

Since $(a^2, b) \in H$ and $(a, b) \in H$ it follows that $(a^2, b)(a, b)^{-1} = (a, 1) \in H$.

Since $(a, 1) \in H$ and $(a^2, b) \in H$, it follows that $(a, 1)^{-2}(a^2, b) = (1, b) \in H$.

Thus indeed $(a, 1), (1, b) \in H$ which, by problem no. 18, implies that $H = G$.

Problem 18.

If $G = \langle g \rangle$ and $H = \langle h \rangle$, show that $G \times H = \langle (g, 1), (1, h) \rangle$.

Solution.

Let $a \in G \times H$ be arbitrary. Then a has the form $a = (g^i, h^j)$ for some $i, j \in \mathbb{Z}$.

We have

$$a = (g^i, h^j) = (a, 1)^i (1, b)^j$$

which implies that $a \in \langle (g, 1), (1, h) \rangle$. Since $a \in G \times H$ was arbitrary, it follows that $G \times H \subseteq \langle (g, 1), (1, h) \rangle$ and hence $G \times H = \langle (g, 1), (1, h) \rangle$.

Problem 25.

Let G and H be cyclic groups with $|G| = m$, $|H| = n$ such that $\gcd(m, n) = 1$. Show that $G \times H$ is cyclic.

Solution.

We have $G = \langle g \rangle$ and $H = \langle h \rangle$ for some $g \in G$ and $h \in H$. Then $|g| = |\langle g \rangle| = m$ and $|h| = |\langle h \rangle| = n$.

Put $a = (g, h)$. Then $|a| = \text{lcm}(|g|, |h|) = \text{lcm}(m, n) = mn$, where the last equality holds since m and n are co-prime.

Therefore $|\langle a \rangle| = |a| = mn = |G \times H|$. Since $\langle a \rangle$ is a subset of size mn in the set $G \times H$ of size mn , it follows that $\langle a \rangle = G \times H$.

Thus $G \times H$ is cyclic, as required.