

1. Find the number of elements of order 7 in a simple group of order 168.

Proof. Any element of order 7 generates a subgroup of order 7. Since $168 = 7 \cdot 24$, a subgroup of order 7 is a 7-Sylow, and thus the number n_7 of subgroups of order 7 divides 24 and is congruent to 1 (mod 7). The only such divisors are 1 and 8. Since the group is simple, this means $n_7 = 8$. The pairwise intersections of these eight subgroups are trivial, and each of the 6 non-identity elements in each group have order 7. Therefore, there are $8 \cdot 6 = 48$ elements of order 7. \square

2. Prove that no group of order 312 is simple.

Proof. 13 divides 312, and the number of 13-Sylows must divide $\frac{312}{13} = 24$ and be congruent to 1 (mod 13). The only such divisor of 24 is 1, thus there is a single, normal 13-Sylow in any group of order 312. \square

3. Using the solvability of groups of order 12, prove that groups of order $588 = 2^2 \cdot 3 \cdot 7^2$ are solvable.

Proof. The number of 7-Sylows must divide 12 and be congruent to 1 (mod 7). The only such divisor is 1, so there is a normal 7-Sylow N of order 49. All groups of order less than 60 are solvable, so N is solvable. G/N has order 12, and so is also solvable. Therefore, G is solvable. \square

4. Suppose that G is a finite group and that $H < G$ is a subgroup of G of prime index. Assume that there is a left coset of H in G , other than H itself, that is also a right coset of H in G . Show that H is a normal subgroup of G .

Proof. There exist $x, y \notin H$ such that $xH = Hy$. So $x \in Hy$, so $x = hy$ for some $h \in H$. But also, $x \in Hx$, so $hy \in Hx \cap Hy$ and thus $Hx = Hy$ because the right cosets partition the group. This gives $xH = Hy = Hx$, therefore x is in the normalizer N of H .

Since H has prime index in G , we must have either $N = H$ or $N = G$. But N contains x , which is not in H by assumption. Therefore $N = G$, so H is normal. \square

- 5a. Let g be an element of the finite group G . Let $\sigma : G \rightarrow G$ be the permutation $x \mapsto gx$. Show that the sign of this permutation is $((-1)^{l+1})^{n/l}$, where l is the order of g and n the order of G .

Proof. Consider the action of $\langle g \rangle$ on G by left translation. The orbits of this action are precisely the orbits of σ . The orbit of a given element $x \in G$ is $\{x, gx, \dots, g^{l-1}x\}$, since if $g^kx = x$ for some $k < l$ then we would have $g^k = e$, a contradiction. So each orbit has size l , and thus there are n/l orbits.

We showed in exercise 33 that the sign of σ is $(-1)^m$, where $m = n - (\text{number of orbits of } \sigma)$. Thus, the sign is $(-1)^{n-n/l} = ((-1)^{(l-1)})^{n/l} = ((-1)^{(l+1)})^{n/l}$. \square

- 5b. Suppose that the 2-Sylow subgroup of G is cyclic and that G has even order. Prove that there are elements of G whose signs (in the sense of part (a)) are -1 and deduce that G has a subgroup of index 2.

Proof. Let 2^k be the highest power of 2 dividing $n = |G|$, and let $\langle g \rangle$ be the cyclic 2-Sylow. We know $k > 0$ because G has even order. The order l of g is then 2^k , and so both $l + 1$ and n/l are odd, thus by part (a) the sign of g is odd.

Therefore, when we embed G into S_n by the left translation action, this element g does not lie within A_n . Since $A_n \subsetneq GA_n \subseteq S_n$, and A_n has index 2, we must have $GA_n = S_n$. Therefore, $(G : G \cap A_n) = (S_n : A_n) = 2$, so $G \cap A_n$ is a subgroup of G of index 2. \square

6. Let G be a group and let $H \leq G$ be a subgroup of G for which the index of H in G is finite. Prove that there is an $n \geq 1$ such that $g^n \in H$ for all $g \in G$.

Proof. We showed in the first homework that a subgroup of finite index contains a normal subgroup of finite index. So there is some $N \leq H$ such that $(G : N) = m$ is finite. So for all $g \in G$, $(gN)^m = g^m N = N$, thus $g^m \in N \subseteq H$. \square

7. Let G be a finite group of order ≥ 3 . Prove that G has an automorphism other than the identity automorphism. (Consider inner automorphisms first. If G is abelian, consider the inversion map $g \mapsto g^{-1}$. Use linear algebra if necessary.)

Proof. Suppose that for all $g \in G$ the automorphism $x \mapsto gxg^{-1}$ is the identity. Then for all $g, x \in G$ we have $gx = xg$, thus G is abelian. Now, suppose also that the inversion map is trivial. Then every element is its own inverse, thus every element has order 2. We know that $G \cong \mathbf{Z}_{q_1} \oplus \cdots \oplus \mathbf{Z}_{q_k}$ where q_1, \dots, q_k are all powers of distinct primes. If any q_i does not equal 2, then the element $1 \cdot i$ (the image of 1 under the inclusion $\mathbf{Z}_{q_i} \hookrightarrow G$) is not its own inverse, a contradiction. So $G \cong \mathbf{Z}_2^k$ for some $k \geq 1$ (since $|G| \geq 3$). So the map that simply switches the 1st and 2nd components is a nontrivial automorphism. \square

8. Let $\{a_1, \dots, a_k\}$ denote the direct sum of cyclic groups of orders a_1, a_2, \dots, a_k . Consider the groups $\{2^2 \cdot 5 \cdot 7, 2^3 \cdot 5^3, 2 \cdot 5^2\}$, $\{2^3 \cdot 5^3 \cdot 7, 2^3 \cdot 5^3\}$, $\{2^2, 2 \cdot 7, 2^3, 5^3, 5^3\}$, $\{2 \cdot 5^3, 2^2 \cdot 5^3, 2^3, 7\}$. Determine all isomorphisms among pairs of groups on this list (they all have order $2^6 5^6 7$).

Proof. We can put each of these groups into their primary decomposition form, and then use the associativity and commutativity of the direct sum to reorder the terms into an ascending order. In order to find the primary decompositions, we use the fact that $\mathbf{Z}_{n \cdot m} \cong \mathbf{Z}_n \oplus \mathbf{Z}_m$ if and only if n and m are relatively prime. Therefore, the groups decompose as

$$\begin{aligned} \{2^2 \cdot 5 \cdot 7, 2^3 \cdot 5^3, 2 \cdot 5^2\} &= \{2^2, 5, 7, 2^3, 5^3, 2, 5^2\} = \{2, 2^2, 2^3, 5, 5^2, 5^3, 7\} \\ \{2^3 \cdot 5^3 \cdot 7, 2^3 \cdot 5^3\} &= \{2^3, 5^3, 7, 2^3, 5^3\} = \{2^3, 2^3, 5^3, 5^3, 7\} \\ \{2^2, 2 \cdot 7, 2^3, 5^3, 5^3\} &= \{2^2, 2, 7, 2^3, 5^3, 5^3\} = \{2, 2^2, 2^3, 5^3, 5^3, 7\} \\ \{2 \cdot 5^3, 2^2 \cdot 5^3, 2^3, 7\} &= \{2, 5^3, 2^2, 5^3, 2^3, 7\} = \{2, 2^2, 2^3, 5^3, 5^3, 7\} \end{aligned}$$

Therefore, only the last two groups are isomorphic. \square