Classification of Groups of Small Order

Michael Van Opstall

Abstract

In this paper, all groups of order less than 31 except those of orders 16 and 24 are classified.

Theorem 0.1. *There are two groups, one cyclic and one dihedral, of order $2p$ for every prime p.*

Proof. Suppose G is a nonabelian group of order $2p$. Then by the first Sylow theorem, G has a subgroup H of order p, which has index 2 in G and is hence normal. Since H has prime order, it is cyclic and has a generator a. Now G also has an element b of order 2 by Cauchy's theorem, and a and b generate all of G since their orders are relatively prime and their product is the order of the group. Now since H is normal in G, $bab \in H$, so $bab = a^k$ for some k. Now $(ba)^2 = baba = a^{k+1}$. Now $|ba| = 1$, 2, p, or $2p$. Clearly $|ba| \neq 1$, and $|ba| \neq 2p$ or else ba would generate G and G would be cyclic. Since bab is a power of a, $(ba)^p = ba^m$ for some m, so ba doesn't have order p either. Now $|ba| = 2 \Rightarrow ba = a^{-1}b$, so $G = \langle a, b | a^p = b^2 = 1, ba = a^{-1}b \rangle$, which is the presentation for the dihedral group of order $2p$.

Lemma 0.2. *If $G/Z(G)$ is cyclic, G is abelian.*

Proof. Cosets have the form $xZ(G)$, $x^2Z(G)$, etc. Take two elements of G, x^iy and x^jz, where $y, z \in Z(G)$. Then $(x^iy)(x^jz) = x^i(yx^j)z = x^j(yx^i)z = x^jzx^iy$, so G is abelian.

Lemma 0.3. *The center of a p-group is nontrivial.*

Proof. By the class equation, $p^n = |Z(G)| + \sum[G : C(x)]$. Now $p|p^n$ and $p|[G : C(c)]$ for all $c \notin Z(G)$, so $p||Z(G)|$ since $1 \in Z(G)$, so $|Z(G)| \neq 0$.

Theorem 0.4. *Any group of order p^2 is abelian.*

Proof. Let $|G| = p^2$. Then $|Z(G)| = p$ or $|Z(G)| = p^2$ by Lagrange and the previous lemma. If $|Z(G)| = p^2$ then G is abelian. Otherwise, $G/Z(G)$ is of prime order and hence cyclic, so G is abelian.

The previous theorems classify together with the well-known fact that every group of prime order is cyclic classify the groups of order 1,2,3,4,5,6,7,9,10,11,13,14,17,19,22,23,25,29, and 31. We now tackle the others on a case by case basis, proving the general classification of groups of order p^3 when we get to 27.

Theorem 0.5. *There are 5 groups of order 8.*

Proof. By the structure theorem, there are 3 abelian groups of order 8: $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, and $\mathbb{Z}_8$. Assume G is a nonabelian group of order 8. Then G must have an element of order 4, because if it has an element of order 8, it is cyclic, and if every element has order 2, then it is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Call such an element a. Now $\langle a \rangle$ is a subgroup of G of index 2, and is hence normal, and $G/\langle a \rangle \cong \mathbb{Z}_2$, so we have for any other $b \in G$ but not in $\langle a \rangle$, $b^2 \in \langle a \rangle$ and $bab^{-1} \in \langle a \rangle$. Since b is not in $\langle a \rangle$ and $\langle a \rangle$ has index 2 in G, a and b generate G. If $bab^{-1} = 1$, then $a = 1$; if $bab^{-1} = a$, then $ab = ba$ (and G would be abelian since its generators commute), and if $bab^{-1} = a^2$, then $a^2 = 1$, also impossible, so $bab^{-1} = a^{-1}$. Now $b^2 = a \Rightarrow a^{-1}bb = \Rightarrow bab = 1 \Rightarrow ba = b^{-1} \Rightarrow b^2a = a^2 = 1$, a contradiction, and similarly for $b^2 = a^3$, hence the only two possibilities for G are $\langle a, b | a^4 = b^2 = 1, ba = a^{-1}b \rangle$ and $\langle a, b | a^4 = 1, b^2 = a^2, ba = a^{-1}b \rangle$.

Theorem 0.6. *There are 5 groups of order 12*

Proof. By the structure theorem, there are 2 abelian groups of order 12: $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ and $\mathbb{Z}_{12}$. Suppose G is a nonabelian group of order 12. Then G has a Sylow 3-subgroup P. Let $\phi : G \to S_4$ be the homomorphism induced by

left translation on the set of left cosets of P. Now $\ker\phi \leq P$, so if $\ker\phi = 1$, ϕ is injective and G is isomorphic to a subgroup of order 12 in S_4 which must be A_4.

Otherwise, $P = \ker\phi$, so P is a normal subgroup of G and hence unique. Thus there are 2 elements of order 3 in G, so if c is one of them, the number of conjugates of c, $[G:C(c)] = 1$ or 2, so $|C(c)| = 6$ or 12, and either way, by Cauchy's theorem there is an element of order 2 in $C(c)$ which commutes with c, so their product a is an element of order 6 and hence generates a normal cyclic subgroup of index 2, so as before, if b is an element not in $\langle a\rangle$, a and b generate G and $b^2 = a^j$ and $bab^{-1} = a^k$. Then k must be relatively prime to 6, and k cannot be 0 or 1 or else a is the identity or G is abelian. Hence $bab^{-1} = a^{-1} \Rightarrow ba = a^{-1}b$. Now $b^2 = a^j \Rightarrow a^{-1}b^2 = a^{j-1} \Rightarrow bab = a^{j-1} \Rightarrow \cdots \Rightarrow a^k b^2 = 1 \Rightarrow a^{2k} = 1$, so $k = 0$ or $k = 3$, so the two possibilities for G are $\langle a,b|a^6 = b^2 = 1, ba = a^{-1}b\rangle$ and $\langle a,b|a^6 = 1, b^2 = a^3, ba = a^{-1}b\rangle$.

Theorem 0.7. *There is one group of order 15.*

Proof. By the third Sylow theorem, if $|G| = 15$, then G has unique (and hence normal) Sylow subgroups of orders 3 and 5. The intersection of these normal subgroups is the identity and their union generates G, so G is isomorphic to their direct product, which is the cyclic group of order 15.

Theorem 0.8. *There are 5 groups of order 18.*

Proof. Let $|G| = 18$. By the first Sylow theorem, there is a subgroup H of G of order 9, which is of index 2, and hence normal and unique.

If $H \cong \mathbb{Z}_9$, then there is an a which generates H. As usual, picking a b of order 2 not in H, a and b generate G. Now $bab = a^k$ for some k since b has order 2 and $\langle a\rangle$ is normal. Now $bab = a^k \Rightarrow a = ba^k b \Rightarrow a = a^k ba^{k-1}b \Rightarrow \cdots \Rightarrow a^{k^2} = a$ so $k = 1$ or $k = -1$, so the cyclic and dihedral groups are the only possibilities.

Now suppose $H \cong \mathbb{Z}_3 \times \mathbb{Z}_3$ and let a be a non-identity element of H. Let c be an element of order 2. Now since H is normal, conjugation by c induces an automorphism of H. There are three possibilities for the image of a. The image is either a itself, another element, call it b which along with a generates H, or a^{-1}. In the case $cac = b$, we get the commutation relation $cbc = a$ automatically, so our group is $\langle a,b,c|a^3 = b^3 = c^2 = 1, ab = ba, cac = b\rangle$. If conjugation by c does not switch generators, then either $cac = a$ and $cbc = b$ and we have $G \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$, or $cac = a^{-1}$ and $cbc = b^{-1}$. Hence the last possibility for G is $\langle a,b,c|a^3 = b^3 = c^2 = 1, ab = ba, cac = a^{-1}, cbc = b^{-1}\rangle$.

Theorem 0.9. *There are 5 groups of order 20.*

Proof. By the structure theorem, there are 2 abelian groups of order 20: $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5$ and $\mathbb{Z}_{20}$. Let G be a nonabelian group of order 20. Then G has a unique Sylow 5-subgroup H. Hence given an element c of order 5, there are at most 4 conjugates of it, so $[G:C(c)] = 1$, 2, or 4. Suppose $[G:C(c)] = 1$ or 2 so G has an element a of order 10 by the argument used in the classification of groups of order 12. Now $\langle a\rangle$ has index 2 in G, so taking an element b not in H, we have as usual $b^2 = a^j$ and $bab^{-1} = a^k$. Clearly k must be relatively prime with 10. If $bab^{-1} = a^3$, then $ba = a^3 b$. From this it follows that $b^2 = a^j \Rightarrow b^2 ab^{-1} = a^{j+1}b^{-1} \Rightarrow ba^3 = a^{j+1}b^{-1} \Rightarrow ba^3 b = a^{j+1} \Rightarrow a^9 + 1b^2 = a^{j+1} \Rightarrow a^{9+j} = a^{1+j}$, a contradiction. A similar argument eliminates $k = 7$, so we get our familiar relation $ba = a^{-1}b$. Our standard argument here also yields that $b^2 = 1$ or $b^2 = a^5$, so two possibilities for G are $\langle a,b|a^{10} = b^2 = 1, ba = a^{-1}b\rangle$ and $\langle a,b|a^{10} = 1, b^2 = a^5, ba = a^{-1}b\rangle$.

Now suppose G has no element of order 10. Now if every element not of order 5 in G has order 2, then there are 9 Sylow 2-subgroups, each one abelian. Now two of these must intersect in a non-identity element (since each contains three elements of order 2), so if a is a nonidentity element in two of these subgroups, $|C(a)| > 4$, so $|C(a)| = 10$ or 20, so we must have an element of order 4 if there are no elements of order 10. Take an element a of order 5 and an element b of order 4 to generate G. Now $\langle a\rangle$ is normal in G, so $bab^{-1} = a^k$ for some k ($ba = a^k b$). But now $b^4 = 1 \Rightarrow b^4 ab^{-1} = ab^{-1} \Rightarrow b^3 a^k = ab^{-1} \Rightarrow a^{3k} = a$, so $k = 2$ and our group is $\langle a,b|a^5 = b^4 = 1, ba = a^2 b\rangle$.

Theorem 0.10. *There are 2 groups of order 21.*

Proof. Let $|G| = 21$. Then G has a unique Sylow 7-subgroup $\langle a\rangle$. Now there are 1 or 7 Sylow 3-subgroups. If there is a unique Sylow 3-subgroup, the standard argument used in the classification of groups of order 15 holds to show that $G \cong \mathbb{Z}_{21}$.

Otherwise suppose there are 7 Sylow 3-subgroups. Let b be an element of order 3 so a and b generate G. As usual we have $ba = a^k b$ by the normality of $\langle a\rangle$. Using our usual strategy we deduce that $a^{k^3} = a$, so $k = 2$ or $k = 4$, both of which give isomorphic groups, namely the group $\langle a,b|a^7 = b^3 = 1, ba = a^{-1}b\rangle$.

Lemma 0.11. *The center of a nonabelian group G of order p^3 is cyclic of order p.*

Proof. By Lagrange, the center has order 1, p, p^2, or p^3. Since G is not abelian, the center of G does not have order p^3. By an earlier lemma, the center of a p-group is nontrivial. If the center has order p^2, then $|G/Z(G)| = p$, so $G/Z(G)$ is cyclic, which implies that G is abelian by an earlier lemma.

Theorem 0.12. *There are 5 groups of order p^3, where p is prime.*

Proof. By the structure theorem, there are 3 abelian groups of order p^3. Suppose G is a nonabelian group of order p^3. There are two cases.

First, suppose every nonidentity element has order p. We know that $Z(G)$ is cyclic and $G/Z(G)$ is noncyclic of order p^2. Let a and b be such that $aZ(G)$ and $bZ(G)$ generate $G/Z(G)$. Let c be a generator of $Z(G)$. We will prove inductively that every element of $Z(G)$ is a commutator of the form $a^iba^{-i}b^{-1}$. First,

$$aba^{-1}b^{-1}Z(G) = aZ(G)bZ(G)a^{-1}Z(G)b^{-1}Z(G),$$

and since $G/Z(G)$ has order p^2, it is abelian, so

$$aZ(G)bZ(G)a^{-1}Z(G)b^{-1}Z(G) = aZ(G)a^{-1}Z(G)bZ(G)b^{-1}Z(G) = Z(G)$$

so $aba^{-1}b^{-1} \in Z(G)$, so for some k, $aba^{-1}b^{-1} = c^k$. Now suppose $a^iba^{-i}b^{-1} = c^{ki}$ by way of induction. Then

$$a^{i+1}ba^{-i-1}b^{-1} = aa^iba^{-i}a^{-1}b^{-1} = ac^{ki}ba^{-1}b^{-1} = c^{ki}aba^{-1}b^{-1} = c^{k(i+1)}$$

Hence by changing generators of $Z(G)$ if necessary, we can assume $z = xyx^{-1}y^{-1}$, so the only possible group is $\langle a,b,c|a^p = b^p = c^p = 1, ac = ca, bc = cb, c = aba^{-1}b^{-1}\rangle$. In the second case, G is generated by elements a and b of order p^2 and p respectively. Now if the center of G is not inside $\langle a\rangle$, then a commutes with more than p^2 elements (everything in $Z(G)$ plus the p^2 elements in $\langle a\rangle$ itself). Hence a would commute with everything, b in particular, so G would be abelian. Hence $Z(G) < \langle a\rangle$, so $Z(G) = \langle a^p\rangle$, the unique subgroup of order p in $\langle a\rangle$. We can choose b such that $aZ(G)$ and $bZ(G)$ generate $G/Z(G)$, so as in the first case, $bab^{-1}a^{-1} \in Z(G)$, so for some k

$$bab^{-1}a^{-1} = a^{kp} \Rightarrow bab^{-1} = a^{kp+1}$$

so we can take G to be $\langle a,b|a^{p^2} = b^p = 1, bab^{-1} = a^{p+1}\rangle$.

For the readers amusement, we provide another delightful fact about groups of order p^3.

Theorem 0.13. *There are $p^2 + p - 1$ conjugacy classes in a group G of order p^3.*

Proof. The center has order p by the above lemma. Hence by the class equation,

$$p^3 = p + \sum[G : C(c)]$$

with the sum taken over conjugacy classes with more than 1 element (and hence p or p^2 elements). No conjugacy class has p^2 elements, however, or for some $a \in G$ we would have $[G : C(a)] = p^2$, so $|C(a)| = p$. However, $C(a)$ has at least p elements, since it contains $Z(G)$ which has order p. Since a is not in $Z(G)$ (or else it would be in a conjugacy class by itself), a also generates a cyclic subgroup of order p or p^2, so a commutes with all these elements in addition to the central elements. Hence every other conjugacy class has p elements, so $p^3 = p + kp$ for some k, that is $p^2 = 1 + k$, so the number of conjugacy classes with p elements is $p^2 - 1$. The total number of conjugacy classes is all of these classes plus the p single element classes for central elements of G.

Theorem 0.14. *There are 4 groups of order 28.*

Proof. This proof is almost identical to the proof for groups of order 20, except we always have an element of order 14 here. For we have a unique Sylow 7-subgroup, so an element c of order 7 has at most 6 conjugates, so $[G : C(c)]$ =1, 2, or 4. If it is 4, however, we can choose another element of order 7 such that $[G : C(c)] = 1$ or 2. As before we get two abelian groups, a dihedral group, and a generalized quaternion group.

Theorem 0.15. *There are 4 groups of order 30.*

Proof. By the structure theorem, there is only one abelian group of order 30. Now G has 1 or 10 Sylow 3-subgroups and 1 or 6 Sylow 5-subgroups. If it has 10 Sylow 3-subgroups and 6 Sylow 5-subgroups, it has 45 elements, so it must have a unique Sylow 3- or 5-subgroup. If there is a unique Sylow 3-subgroup, let c be an element of order 3 so $|C(c)| = 15$ or 30. If $|C(c)| = 15$, then $C(c)$ is generated by an element of order 15. Otherwise we have an element of order 5 commuting with an element of order 3 to get our element of order 15. If there is a unique Sylow 5-subgroup, then $|C(c)| = 10$, 15, or 30. This similarly gives us an element of order 15. Now using our usual techniques, we get three possible groups: $\langle a,b|a^{15} = b^2 = 1, ba = a^4b\rangle$, $\langle a,b|a^{15} = b^2 = 1, ba = a^{11}b\rangle$, and $\langle a,b|a^{15} = b^2 = 1, ba = a^{-1}b\rangle$.