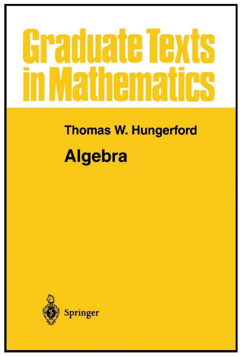
Modern Algebra

Chapter II. The Structure of Groups
II.6. Classification of Finite Groups—Proofs of Theorems



Proposition II.6.1

Proposition II.6.1. Let p and q be primes such that $p > q$.

(i) If $q \nmid p - 1$ then every group of order pq is isomorphic to the cyclic group $\mathbb{Z}_{pq}$.

(ii) If $q \mid p - 1$ then there are (up to isomorphism) exactly two distinct groups of order pq: the cyclic group $\mathbb{Z}_{pq}$ and a nonabelian group K generated by elements c and d such that these elements have orders $|c| = p$ and $|d| = q$. Also $dc = c^s d$ where $s \not\equiv 1 \pmod{p}$ and $s^q \equiv 1 \pmod{p}$. This nonabelian group is called a *metacyclic group* (see Exercise II.6.2).

Proof. In both cases, the only abelian group of order pq is (up to isomorphism) $\mathbb{Z}_{pq} \cong \mathbb{Z}_p \oplus \mathbb{Z}_q$ by Theorem II.2.6 and Lemma II.2.3. By Cauchy's Theorem (Theorem II.5.2), G contains elements a and b with orders $|a| = p$ and $|b| = q$. Furthermore, $S = \langle a \rangle$ is normal in G by Corollary II.4.10, so the quotient group G/S exists and is of order $|G/S| = |G|/|S| = q$ by Lagrange's Theorem (Corollary I.4.6).

Proposition II.6.1 (continued 1)

Proof (continued). Since q is prime, G/S is cyclic (Exercise I.4.3(iii)). Now coset bS is of order q in group G/S. (Notice that $b \notin \langle a \rangle = S$ or else $\langle a \rangle \cap \langle b \rangle \neq \{e\}$ and we would have a subgroup of G of an order different from 1, p, q, and pq, contradicting Lagrange's Theorem. Since the order of element bS must divide $|G/S| = q$ and the order of bS is not 1, then the order of bS must be q.) So $G/S = \langle bS \rangle$. Now the cosets of S partition group G, so every $g \in G$ is in some $b^i S$ and since $S = \langle a \rangle$ then $g = b^i a^j$ for some $i, j \geq 0$. That is, $G = \langle a, b \rangle$. The number of Sylow q-subgroups is $kq + 1$ for some $k \geq 0$ and divides $|G| = pq$ by the Third Sylow Theorem (Theorem II.5.10). So there are either 1 or p Sylow q-subgroups of G. If there is one such subgroup, which must be the case if $q \nmid (p-1)$ (since $q \nmid (p-1)$ and $(kq+1) \mid (pq)$ imply that either $kq + 1 = 1$, $kq + 1 = p$, or $kq + 1 = q$; if $kq + 1 = 1$ then $k = 0$; for $k \geq 1$, we cannot have $kq + 1 = q$; if $kq + 1 = p$ then $kq = p - 1$ and $q \mid (p-1)$; so if $q \nmid (p-1)$ then $k = 0$ and there is one Sylow q-subgroup) then this unique Sylow q-subgroup $\langle b \rangle$ is a normal subgroup by Corollary II.5.8(iii).

Proposition II.6.1 (continued 2)

Proof (continued). As described above, $\langle a \rangle \cap \langle b \rangle = \{e\}$. By Theorem I.3.2, $S = \langle a \rangle \cong \mathbb{Z}_p$ and $\langle b \rangle \cong \mathbb{Z}_q$ and these are normal subgroups of G by the above arguments. So the hypotheses of Theorem I.8.6 are satisfied and G is the weak direct product of $\langle a \rangle$ and $\langle b \rangle$. Since for finite products, the weak direct product and direct product coincide, then we can also say that G is the direct product of $\langle a \rangle$ and $\langle b \rangle$. Now define $f_1 : \langle a \rangle \to \mathbb{Z}_p$ such that $f_1(a) = \overline{1}$ and define $f_2 : \langle b \rangle \to \mathbb{Z}_q$ such that $f_2(b) = \overline{1}$. Then f_1 and f_2 are isomorphisms and f mapping $\langle a \rangle \times \langle b \rangle$ to $\mathbb{Z}_p \oplus \mathbb{Z}_q$ defined as $f = f_1 \times f_2$ is an isomorphism by Theorem I.8.10. By Exercise I.8.5, since p and q are relatively prime, then $\mathbb{Z}_p \oplus \mathbb{Z}_q \cong \mathbb{Z}_{pq}$. Hence

$$G = \langle a \rangle \times \langle b \rangle \cong \mathbb{Z}_p \oplus \mathbb{Z}_q \cong \mathbb{Z}_{pq},$$

and if G has only one Sylow q-subgroup then $G \cong \mathbb{Z}_{pq}$. So (i) holds and (ii) holds in the event that G has only one Sylow q-subgroup.

Proposition II.6.1 (continued 3)

Proof (continued). If the number of Sylow q-subgroups is p (which can only occur if $q \mid (p-1)$, as explained above), then $bab^{-1} = a^r$ for some $a^r \in \langle a \rangle$, since $S = \langle a \rangle \triangleleft G$, where

$$r \not\equiv 1 \,(\text{mod } p) \qquad (*)$$

(for if $r \equiv 1$ (mod p) then $a^r = a$ by Theorem I.3.4(v) and then $bab^{-1} = a$ or $ba = ab$; but then, since every element of G is of the form $b^i a^j$ as explained above, then G would be abelian and so have only one Sylow q-subgroup, not p, a contradiction). Since $bab^{-1} = a^r$, it follows by induction that $b^j ab^{-j} = a^{r^j}$, as we now explain. The result is true for $j = 1$, by hypothesis. Next, $b^j ab^{-j} = a^{r^j}$ implies

$$b^{j+1}ab^{-(j+1)} = b(b^j ab^{-j})b^{-1} = ba^{r^j}b^{-1} = b\underbrace{aa\cdots a}_{r^j \text{ times}}b^{-1} =$$

$$= \underbrace{(bab^{-1})(bab^{-1})\cdots(bab^{-1})}_{r^j \text{ times}} = (a^r)^{r^j} = a^{r^{j+1}} \text{ since } bab^{-1} = a^r.$$

Proposition II.6.1 (continued 4)

Proof (continued). In particular for $j = q$, $b^q ab^{-q} = a = a^{r^q}$ (since $|b| = q$) and by Theorem I.3.4(v)

$$r^q \equiv 1 \,(\text{mod } p). \qquad (**)$$

To complete the proof, we must show that if $q \mid (p-1)$ and G is the nonabelian group described in the previous paragraph, then G is isomorphic to group K in the statement of the theorem. We need two results from number theory. Hungerford references J.E. Schockley's *Introduction to Number Theory* (Holt, Rinehart, and Winston, 1967):
Result 1. The congruence $x^q \equiv 1$ (mod p) has exactly q distinct solutions modulo p. [Shockley, Corollary 6.1, page 67]
Result 2. If r is a solution to $x^q \equiv 1$ (mod p) and k is the least positive integer such that $r^k \equiv q$ (mod p), then $k \mid p$. [Shockley, Theorem 8, page 70]

Proposition II.6.1 (continued 5)

Proof (continued). In our case $r \not\equiv 1$ (mod p) (see $(*)$) and $r^q \equiv 1$ (mod p) (see $(**)$), so the condition $k \mid q$ of Result 2 implies that $k = q$ since q is prime. So the q distinct solutions modulo p to the equation $x^q \equiv 1$ (mod p) of Result 1 are $1, r, r^2, \ldots, r^{q-1}$. Consider *any* $s \in \mathbb{N}$ with $s \equiv r^t$ (mod p) for some t where $1 \le t \le q-1$ (so $s \not\equiv 1$ (mod p) since these powers of r are distinct from Result 1). Also, $s^q \equiv r^{tq} \,(\text{mod } p) \equiv (r^q)^t \,(\text{mod } p) \equiv 1 \,(\text{mod } p)$. Define $b_1 = b^t \in G$. Since the order of b is $|b| = q$ and $1 \le t \le q-1$, then the order of b_1 must be $|b_1| = q$ also (and $\langle b \rangle = \langle b_1 \rangle$ are both subgroups of G of order q). As argued at the beginning of the proof (with b replaced with b_1), $G = \langle a, b_1 \rangle$ and every element of G can be written in the form $b_1^i a^j$, that $|a| = p$, and that $b_1 ab_1^{-1} = a^s$ for *some* $a^s \in \langle a \rangle$ where $s \not\equiv 1$ (mod p) and $s^q \equiv 1$ (mod p) (see $(**)$ above; s here plays the role of r in the argument above).

Proposition II.6.1 (continued 6)

Proposition II.6.1. Let p and q be primes such that $p > q$.

(i) If $q \nmid p-1$ then every group of order pq is isomorphic to the cyclic group $\mathbb{Z}_{pq}$.

(ii) If $q \mid p-1$ then there are (up to isomorphism) exactly two distinct groups of order pq: the cyclic group $\mathbb{Z}_{pq}$ and a nonabelian group K generated by elements c and d such that these elements have orders $|c| = p$ and $|d| = q$. Also $dc = c^s d$ where $s \not\equiv 1$ (mod p) and $s^q \equiv 1$ (mod p). This nonabelian group is called a *metacyclic group* (see Exercise II.6.2).

Proof (continued). So CHOOSE $s \in \mathbb{N}$ where $b_1 ab_1^{-1} = a^s$, $s \not\equiv 1$ (mod p) and $s^q \equiv 1$ (mod p). Now $b_1 ab_1^{-1} = a^s$ gives $b_1 a = a^s b_1$. For the isomorphism between $G = \langle a, b_1 \rangle$ and $K = \langle c, d \rangle$, define the mapping $a \mapsto c$ and $b_1 \mapsto d$. □

Corollary II.6.2

Corollary II.6.2. If p is an odd prime, then every group of order $2p$ is isomorphic either to the cyclic group $\mathbb{Z}_{2p}$ or the dihedral group D_p.

Proof. By Proposition II.6.1 with $q = 2$ (in which case $q \mid (p-1)$) there are two distinct groups of order $pq = 2p$, one of which is the cyclic group $\mathbb{Z}_{2p}$. The other group, say G, has parameter s satisfying $s \not\equiv 1 \pmod{p}$ and $s^2 \equiv 1 \pmod{p}$. So $s \equiv -1 \pmod{p}$. Hence $G = \langle c, d \rangle$ where $|d| = 2$, $|c| = p$, and $dc = c^s d$ or $dc = c^{p-1}d = c^{-1}d$. By Theorem I.6.13, $G \cong D_p$ □

Proposition II.6.3

Proposition II.6.3. There are (up to isomorphism) exactly two distinct nonabelian groups of order 8: the quaternion group Q_8 (see Exercise I.2.3) and the dihedral group D_4.

Proof. By Exercise II.6.10, $D_4 \not\cong Q_8$. If a group G of order 8 is nonabelian then it cannot contain an element of order 8 (otherwise it would be cyclic). Nor can such a group have every nonidentity element of order 2 (or else G would be abelian by Exercise I.1.13). Hence G contains an element a of order 4. Now group $\langle a \rangle$ is of index 2, $|G|/|\langle a \rangle| = 2$, and so $\langle a \rangle$ is a normal subgroup by Exercise I.5.1. Choose $b \notin \langle a \rangle$. Then b is in coset $b\langle a \rangle$. So $G = \langle a \rangle \cup b\langle a \rangle$ and $G = \langle a, b \rangle$. Since $b \notin \langle a \rangle$ then $b^2 \notin b\langle a \rangle$. Since G is partitioned into $\langle a \rangle$ and $b\langle a \rangle$, b^2 must be in $\langle a \rangle$. If $b^2 = a$ then $\langle b^2 \rangle = \langle a \rangle$ and coset $b\langle b^2 \rangle$ gives the elements in $G \setminus \langle b^2 \rangle$ and so $\langle b \rangle = G$, a contradiction. Since a is of order 4, $\langle a \rangle = \langle a^3 \rangle$ and a similar contradiction results if $b^2 = a^3$. So it must be that either $b^2 = a^2$ or $b^2 = e$.

Proposition II.6.3 (continued)

Proposition II.6.3. There are (up to isomorphism) exactly two distinct nonabelian groups of order 8: the quaternion group Q_8 (see Exercise I.2.3) and the dihedral group D_4.

Proof (continued). Since $\langle a \rangle$ is normal in G, then $bab^{-1} \in \langle a \rangle$ by Theorem I.5.1(iv). If $bab^{-1} = e$ then $ba = b$ and $a = e$, a contradiction. If $bab^{-1} = a$ then $ab = ba$ and since $G = \langle a, b \rangle$ then G is abelian, a contradiction. If $bab^{-1} = a^2$ then $(bab^{-1})^2 = a^4 = e$ or $ba^2b^{-1} = e$ and $ba^2 = b$ and $a^2 = e$, a contradiction. So it must be that $bab^{-1} = a^3$. So $ba = a^3 b = a^{-1}b$. Hence, we have two cases depending on the value of b^2. In one case we have $|a| = 4$, $b^2 = a^2$, $ba = a^{-1}b$, and so by Exercise I.4.14, $G \cong Q_8$. In the other case, $|a| = 4$, $|b| = 2$ (since $b^2 = e$), $ba = a^{-1}b$ and so by Theorem I.6.13, $G \cong D_4$. □

Proposition II.6.4

Proposition II.6.4. There are (up to isomorphism) exactly three distinct nonabelian groups of order 12: the dihedral group D_6, the alternating group A_4, and a group T generated by elements a and b such that $|a| = 6$, $b^2 = a^3$, and $ba = a^{-1}b$.

Proof. In Exercise II.6.5 it is shown that the group T actually exists and in Exercise II.6.6 it is shown that no two of D_6, A_4, T are isomorphic. If G is a nonabelian group of order 12, then G has a Sylow 3-subgroup P by the First Sylow Theorem (Theorem II.5.7). Then $|P| = 3$ and $[G : P] = |G|/|P| = 4$. By Proposition II.4.8 there is a homomorphism $f : G \to A(S)$ (where $A(S)$ is the group of all permutations of the set of left cosets of P; since there a 4 left cosets of P then $A(S) \cong S_4$) whose kernel K is contained in P. Whence $K = P$ or $K = \{e\}$ (since the kernel is a subgroup by Exercise I.2.9(a) and $|P| = 3$). If $K = \{e\}$ then f is one to one (Theorem I.2.3(i)) and G is isomorphic to a subgroup of order 12 of S_4 (namely $\text{Im}(f) = f[G]$), which must be A_4 by Theorem I.6.8 (and the first possible structure of G is established).

Proposition II.6.4 (continued 1)

Proof (continued). Otherwise $K = P$ and P is normal in G (Theorem I.5.5). In this case, P is the unique Sylow 3-subgroup (since all Sylow p-subgroups of G are conjugates by the Second Sylow Theorem [Theorem II.5.9] and a normal subgroup is self conjugate by Theorem I.5.1(v)). Hence G contains only two elements of order 3 (the two nonidentity elements in P). If c is one of these order 3 elements, then $[G : C_G(c)]$ is the number of conjugates of c (by Corollary II.4.4(i); $C_G(c) = \{g \in G \mid gcg^{-1} = c\}$ is the "centralizer" of c) and every conjugate of c has order 3 (consider $(gcg^{-1})^3$); so $[G : C_G(c)] = 1$ or 2 (either c is self conjugate or c and the other element of G of order 3 are conjugates, respectively). Since $[G : C_G(c)] = |G|/|C_G(c)|$ (Lagrange's Theorem, Corollary I.4.6) then $|C_G(c)| = 12$ or 6 (respectively). In either case there is $d \in C_G(c)$ of order 2 by Cauchy's Theorem (Theorem II.5.2). Since $cd \in C_G(c)$ then $|cd|$ is 1, 2, 3, 4, or 6. Since $d \in C_G(c)$ then $dcd^{-1} = c$ or $dc = cd$. Now if $cd = e$ then $e = e^2 = (cd)^2 = (cd)(dc)$ $= cd^2c = cec = c^2$, a contradiction since $|c| = 3$.

Proposition II.6.4 (continued 2)

Proof (continued). Next, $(cd)^2 = (cd)(cd) = (cd)(dc) = cd^2c = cec$ $= c^2 \neq e$ since $|c| = 3$. Also $(cd)^3 = (cd)(cd)(cd) = (cd)(dc)(cd)$ $= cd^2c^2d = cec^2d = c^3d = d \neq e$. Similarly, $(cd)^4 = (cd)^3(cd)$ $= d(cd) = d(dc) = d^2c = ec = c \neq e$. Also, $(cd)^6 = (cd)^3(cd)^3 = (d)(d) = d^2 = e$. Hence $|cd| = 6$.

Let $a = cd$. Then, as in the proof of Proposition II.6.3, $\langle a \rangle$ is normal in G since $|G/\langle a \rangle| = 2$; there is $b \in G$ such that $b \notin \langle a \rangle$, $b \neq e$, $b^2 \in \langle a \rangle$. Since $\langle a \rangle$ is normal, $bab^{-1} \in \langle a \rangle$. We now consider the value of bab^{-1}.

- If $bab^{-1} = e$ then $ba = b$ and $a = e$, contradiction.
- If $bab^{-1} = a$ then $ba = ab$ and G is abelian ($G = \langle a, b \rangle$ since $G = \langle a \rangle \cup b\langle a \rangle$), a contradiction.
- If $bab^{-1} = a^2$ then $(bab^{-1})^3 = (a^2)^3 = a^6 = e$ and $ba^3b^{-1} = e$ or $ba^3 = b$ or $a^3 = e$, a contradiction.
- If $bab^{-1} = a^3$ then $(bab^{-1})^2 = (a^3)^2$ or $ba^2b^{-1} = a^6 = e$ or $ba^2b^{-1} = e$ and $ba^2 = b$ or $a^2 = e$, a contradiction.

Proposition II.6.4 (continued 3)

Proof (continued).

- If $bab^{-1} = a^4$ then $(bab^{-1})^3 = (a^4)^3 = a^{12} = e$ or $ba^3b^{-1} = e$ and $ba^3 = b$ or $a^3 = e$, a contradiction.

So it must be that $bab^{-1} = a^5 = a^{-1}$. That is $ba = a^{-1}b$ or $aba = b$.

We now consider the possible values of $b^2 \in \langle a \rangle$ in terms of powers of a.

- If $b^2 = a^2$ then, since $aba = b$, we have $(aba)^2 = b^2$ or $(aba)(aba) = b^2$ or $aba^2ba = b^2$ or $abb^2ba = b^2$ or $ab^4a = b^2$ or $ab^4a = a^2$ or $b^4 = e$ or $a^4 = e$, a contradiction since $|a| = 6$.
- If $b^2 = a^4 = a^{-2}$ then, since $aba = b$ or $b = a^{-1}ba^{-1}$, we have $b^2 = (a^{-1}ba^{-1})(a^{-1}ba^{-1}) = a^{-1}ba^{-2}ba^{-1} = a^{-1}b^4a^{-1}$ or (since $b^2 = a^4$) $a^4 = a^{-1}b^4a^{-1}$ or $a^6 = b^4$ or $e = b^4$ or $e = a^8 = a^2$, a contradiction since $|a| = 6$.

Proposition II.6.4 (continued 4)

Proof (continued).

- If $b^2 = a$ then $b^{12} = a^6 = e$. Then $b^6 = a^3 \neq e$, $b^4 = a^2 \neq e$, and $b^3 = ab \neq e$ since $b \neq a^{-1}$ (or else $b \in \langle a \rangle$) and so $G = \langle b \rangle$ which implies that G is cyclic and hence abelian, a contradiction.
- If $b^2 = a^5$ then $b^{12} = a^{30} = e$ (and $b^6 = a^{15} = a^3 \neq e$, $b^4 = a^{10} = a^4 \neq e$, and $b^3 = b^2b = a^5b \neq e$ since $b \neq a$, or else $b \in \langle a \rangle$). Then $G = \langle b \rangle$ which implies that G is cyclic and hence abelian, a contradiction.

Therefore, the only possibilities are:

(i) $|a| = 6$, $b^2 = e$, $ba = a^{-1}b$, where $G \cong D_6$ by Theorem I.6.13;

(ii) $|a| = 6$, $b^2 = a^3$, $ba = a^{-1}b$, whence $G \cong T$ by Exercise II.6.5(b).

So the other two possible structures of G are established. □