

GROUPS OF ORDER p^3

KEITH CONRAD

1. INTRODUCTION

For each prime p , we will describe all groups of order p^3 up to isomorphism. This was done for $p = 2$ by Cayley [3, 4] in 1859 and 1889 and Kempe [8, pp. 38–39, 45] in 1886, and for odd p by Cole and Glover [5, pp. 196–201], Hölder [7, pp. 371–373] and Young [13, pp. 133–139] independently in 1893. The groups were described by them using generators and relations, which sometimes leads to unconvincing arguments that the groups constructed to be of order p^3 really have that order.¹

From the cyclic decomposition of finite abelian groups, there are three abelian groups of order p^3 up to isomorphism: $\mathbf{Z}/(p^3)$, $\mathbf{Z}/(p^2) \times \mathbf{Z}/(p)$, and $\mathbf{Z}/(p) \times \mathbf{Z}/(p) \times \mathbf{Z}/(p)$.² These are nonisomorphic since they have different maximal orders for their elements: p^3 , p^2 , and p respectively. We will show there are two nonabelian groups of order p^3 up to isomorphism. That number is the same for all p , but the actual description of the two nonabelian groups of order p^3 will be different for $p = 2$ and $p \neq 2$, so we will treat these cases separately.

2. GROUPS OF ORDER 8

Theorem 2.1. *A nonabelian group of order 8 is isomorphic to D_4 or to Q_8 .*

The groups D_4 and Q_8 are not isomorphic since there are 5 elements of order 2 in D_4 and only one element of order 2 in Q_8 .

Proof. Let G be nonabelian of order 8. The nonidentity elements in G have order 2 or 4. If $g^2 = 1$ for all $g \in G$ then G is abelian, so some $x \in G$ must have order 4.

Let $y \in G - \langle x \rangle$. The subgroup $\langle x, y \rangle$ properly contains $\langle x \rangle$, so $\langle x, y \rangle = G$. Since G is nonabelian, x and y do not commute.

Since $\langle x \rangle$ has index 2 in G , it is a normal subgroup. Therefore $xyx^{-1} \in \langle x \rangle$:

$$xyx^{-1} \in \{1, x, x^2, x^3\}.$$

Since xyx^{-1} has order 4, $xyx^{-1} = x$ or $xyx^{-1} = x^3 = x^{-1}$. The first option is not possible, since it says x and y commute, but they don't. Therefore

$$xyx^{-1} = x^{-1}.$$

The group $G/\langle x \rangle$ has order 2, so $y^2 \in \langle x \rangle$:

$$y^2 \in \{1, x, x^2, x^3\}.$$

Since y has order 2 or 4, y^2 has order 1 or 2. Thus $y^2 = 1$ or $y^2 = x^2$.

¹The page <https://math.stackexchange.com/questions/1023341> gives a nonobvious description of the trivial group by generators and relations.

²See <https://kconrad.math.uconn.edu/blurbs/grouptheory/finite-abelian.pdf>.

Putting this together, $G = \langle x, y \rangle$ where either

$$(2.1) \quad x^4 = 1, \quad y^2 = 1, \quad yxy^{-1} = x^{-1}$$

or

$$(2.2) \quad x^4 = 1, \quad y^2 = x^2, \quad yxy^{-1} = x^{-1}.$$

The relations in (2.1) resemble D_4 , using $x \leftrightarrow r$ and $y \leftrightarrow s$, while the relations in (2.2) resemble Q_8 using $x \leftrightarrow i$ and $y \leftrightarrow j$. We will construct isomorphisms $D_4 \rightarrow G$ in the first case and $Q_8 \rightarrow G$ in the second case.³

First suppose (2.1) is true. Each element of D_4 has the form $r^m s^n$ for unique $m \in \mathbf{Z}/(4)$ and $n \in \mathbf{Z}/(2)$. Set $f: D_4 \rightarrow G$ by $f(r^m s^n) = x^m y^n$.

f is well-defined. The product $r^m s^n$ determines $m \bmod 4$ and $n \bmod 2$, which makes $x^m y^n$ sensible since $x^4 = 1$ and $y^2 = 1$. Note $f(r) = x$ and $f(s) = y$, which was suggested by (2.1) originally. It remains to show f is a homomorphism and a bijection.

f is a homomorphism. For general elements $g = r^m s^n$ and $g' = r^{m'} s^{n'}$ in D_4 , we want to show $f(gg') = f(g)f(g')$. On the left side, $gg' = r^m s^n r^{m'} s^{n'}$. To rewrite this as a power of r times a power of s , from $srs^{-1} = r^{-1}$ we have $s^n r s^{-n} = r^{(-1)^n}$ for $n \in \mathbf{Z}/(2)$, so (raise both sides to the m' -power) $s^n r^{m'} s^{-n} = r^{(-1)^n m'}$. Thus

$$(2.3) \quad gg' = r^m s^n r^{m'} s^{n'} = r^m r^{(-1)^n m'} s^n s^{n'} = r^{m+(-1)^n m'} s^{n+n'},$$

so $f(gg') = x^{m+(-1)^n m'} y^{n+n'}$. Also

$$(2.4) \quad f(g)f(g') = f(r^m s^n)f(r^{m'} s^{n'}) = x^m y^n x^{m'} y^{n'}.$$

The rewriting of $r^m s^n r^{m'} s^{n'}$ in (2.3) was based only on the relations $srs^{-1} = r^{-1}$ and $s^2 = 1$, so from the similar relations $yxy^{-1} = x^{-1}$ and $y^2 = 1$ in (2.1), the right side of (2.4) is $x^{m+(-1)^n m'} y^{n+n'}$, which is $f(gg')$. So f is a homomorphism.

f is a bijection. Since f is a homomorphism to G and its image includes $x = f(r)$ and $y = f(s)$, the image of f contains $\langle x, y \rangle$, which is all of G . Thus f is onto. Since $|D_4| = |G|$, a surjection $D_4 \rightarrow G$ is a bijection, so f is a bijection.

Now suppose (2.2) is true. We want to build an isomorphism $Q_8 \rightarrow G$ mapping i to x and j to y . Every element of Q_8 looks like $i^m j^n$ where $m, n \in \mathbf{Z}/(4)$. Set $f: Q_8 \rightarrow G$ by $f(i^m j^n) = x^m y^n$.

f is well-defined. A representation of an element of Q_8 as $i^m j^n$ is *not* unique: if $i^m j^n = i^{m'} j^{n'}$ then $i^{m-m'} = j^{n'-n}$, so $m-m' = 2a$ and $n'-n = 2b$ where $a \equiv b \pmod{2}$ (why?). Then $x^{m-m'} = (x^2)^a = (y^2)^a = (y^2)^b = y^{n'-n}$ by the first two relations in (2.2), so $x^m y^n = x^{m'} y^{n'}$.

f is a homomorphism. Since $jij^{-1} = i^{-1}$ and j^2 commutes with i , check $j^n i j^{-n} = i^{(-1)^n}$ for all $n \in \mathbf{Z}/(4)$. This and the first two relations in (2.2) imply $f: Q_8 \rightarrow G$ is a homomorphism for reasons similar to the previous mapping $D_4 \rightarrow G$ being a homomorphism.

f is a bijection. This follows for the same reasons as before, since the image of f includes $f(i) = x$ and $f(j) = y$ and $\langle x, y \rangle = G$. \square

³We map from D_4 or Q_8 to G rather than in the other direction because D_4 and Q_8 are known groups, so it is better to start there.

3. THE CASE OF ODD p

From now, $p \neq 2$. We'll show the two nonabelian groups of order p^3 , up to isomorphism, are

$$\text{Heis}(\mathbf{Z}/(p)) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbf{Z}/(p) \right\}$$

and

$$G_p = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a, b \in \mathbf{Z}/(p^2), a \equiv 1 \pmod{p} \right\} = \left\{ \begin{pmatrix} 1 + pm & b \\ 0 & 1 \end{pmatrix} : m, b \in \mathbf{Z}/(p^2) \right\},$$

where m actually only matters modulo p .⁴ These two constructions both make sense at the prime 2, but in that case the two groups are isomorphic to each other, as we'll see below.

We can distinguish between $\text{Heis}(\mathbf{Z}/(p))$ and G_p for $p \neq 2$ by counting elements of order p . In $\text{Heis}(\mathbf{Z}/(p))$,

$$(3.1) \quad \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & na & nb + \frac{n(n-1)}{2}ac \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{pmatrix}$$

for $n \in \mathbf{Z}$, so

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^p = \begin{pmatrix} 1 & 0 & \frac{p(p-1)}{2}ac \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

When $p \neq 2$, $\frac{p(p-1)}{2} \equiv 0 \pmod{p}$, so all nonidentity elements of $\text{Heis}(\mathbf{Z}/(p))$ have order p . On the other hand, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ in G_p has order p^2 since $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$. So $\text{Heis}(\mathbf{Z}/(p)) \not\cong G_p$.

At the prime 2, $\text{Heis}(\mathbf{Z}/(2))$ and G_2 each contain more than one element of order 2, so $\text{Heis}(\mathbf{Z}/(2))$ and G_2 are both isomorphic to D_4 (Theorem 2.1).

Let's look at how matrices combine and decompose in $\text{Heis}(\mathbf{Z}/(p))$ and G_p when $p \neq 2$, since this will inform some of our computations later when we classify the nonabelian group of order p^3 . In $\text{Heis}(\mathbf{Z}/(p))$,

$$(3.2) \quad \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a + a' & b + b' + ac' \\ 0 & 1 & c + c' \\ 0 & 0 & 1 \end{pmatrix}$$

and in G_p

$$(3.3) \quad \begin{pmatrix} 1 + pm & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 + pm' & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 + p(m + m') & b + b' + pm'b' \\ 0 & 1 \end{pmatrix}.$$

In $\text{Heis}(\mathbf{Z}/(p))$,

$$\begin{aligned} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^c \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^a \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^b \quad \text{by (3.1)} \end{aligned}$$

⁴The notation G_p for this group is not standard. I don't know a standard "matrix group" notation for it.

and a particular commutator is

$$\left[\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \right] = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

So if we set

$$x = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } y = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

then

$$(3.4) \quad \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = y^c x^a [x, y]^b.$$

In $G_p \subset \text{Aff}(\mathbf{Z}/(p^2))$,

$$\begin{pmatrix} 1+pm & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1+pm & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^b \begin{pmatrix} 1+p & 0 \\ 0 & 1 \end{pmatrix}^m.$$

If we set

$$x = \begin{pmatrix} 1+p & 0 \\ 0 & 1 \end{pmatrix} \text{ and } y = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

then

$$\begin{pmatrix} 1+pm & b \\ 0 & 1 \end{pmatrix} = y^b x^m$$

and

$$[x, y] = \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix} = y^p.$$

Lemma 3.1. *In a group G , if g and h commute with $[g, h]$ then $[g^m, h^n] = [g, h]^{mn}$ for all m and n in \mathbf{Z} , and $g^n h^n = (gh)^n [g, h]^{\binom{n}{2}}$.*

Proof. Exercise. □

Lemma 3.2. *Let p be prime and G be a nonabelian group of order p^3 with center Z . Then $|Z| = p$, $G/Z \cong (\mathbf{Z}/(p)) \times (\mathbf{Z}/(p))$, and $[G, G] = Z$.*

Proof. Since G is a nontrivial group of p -power order, its center is nontrivial. Therefore $|Z| = p, p^2$, or p^3 . Since G is nonabelian, $|Z| \neq p^3$. For a group G , if G/Z is cyclic then G is abelian. So G being nonabelian forces G/Z to be noncyclic. Therefore $|G/Z| \neq p$, so $|Z| \neq p^2$. The only choice left is $|Z| = p$, so G/Z has order p^2 .

Up to isomorphism the only groups of order p^2 are $\mathbf{Z}/(p^2)$ and $\mathbf{Z}/(p) \times \mathbf{Z}/(p)$. Since G/Z is noncyclic, $G/Z \cong \mathbf{Z}/(p) \times \mathbf{Z}/(p)$.

Since G/Z is abelian, we have $[G, G] \subset Z$. Because $|Z| = p$ and $[G, G]$ is nontrivial, necessarily $[G, G] = Z$. □

Remark 3.3. Although it won't be necessary below, Lemma 3.2 implies for all primes p , including $p = 2$, that a nonabelian group G of order p^3 has $p^2 + p - 1$ conjugacy classes. To start, G has p conjugacy classes of size 1 since those are the elements of the center Z and $|Z| = p$. Next, if $g \in G - Z$ then its conjugacy class has order $|G|/|Z(g)| = p^3/|Z(g)|$, where $Z(g) = \{x \in G : xg = gx\}$ is the centralizer of g . Since $Z(g)$ is a subgroup of G containing Z and g and $Z(g) \neq G$, $|Z(g)| = p^2$. Thus $|G|/|Z(g)| = p^3/p^2 = p$, so all conjugacy classes

of size greater than 1 have size p . Conjugate elements of G are equal in G/Z (since G/Z is abelian) and each coset in G/Z has size p , so for each $g \in G - Z$, its conjugacy class in G must be the coset gZ .

Collecting the $p^3 - p$ noncentral elements of G into disjoint conjugacy classes each of size p , the number of such conjugacy classes is $(p^3 - p)/p = p^2 - 1$, so the total number of conjugacy classes in G is $p + (p^2 - 1) = p^2 + p - 1$: p of size 1 and $p^2 - 1$ of size p .

Theorem 3.4. *For $p \neq 2$, a nonabelian group of order p^3 is isomorphic to $\text{Heis}(\mathbf{Z}/(p))$ or G_p .*

Proof. Let G be a nonabelian group of order p^3 . Each $g \neq 1$ in G has order p or p^2 .

By Lemma 3.2, we can write $G/Z = \langle \bar{x}, \bar{y} \rangle$ and $Z = \langle z \rangle$. For $g \in G$, $g \equiv x^i y^j \pmod{Z}$ for some integers i and j , so $g = x^i y^j z^k = z^k x^i y^j$ for some $k \in \mathbf{Z}$. If x and y commute then G is abelian (since z^k commutes with x and y), which is a contradiction. Thus x and y do not commute. Therefore $[x, y] = xyx^{-1}y^{-1} \in Z$ is nontrivial, so $Z = \langle [x, y] \rangle$. Therefore we can use $[x, y]$ for z , showing $G = \langle x, y \rangle$.

Let's see what the product of two elements of G looks like. Using Lemma 3.1,

$$(3.5) \quad x^i y^j = y^j x^i [x, y]^{ij}, \quad y^j x^i = x^i y^j [x, y]^{-ij}.$$

This shows we can move every power of y past every power of x on either side, at the cost of introducing a (commuting) power of $[x, y]$. So every element of $G = \langle x, y \rangle$ has the form $y^j x^i [x, y]^k$. (We write in this order because of (3.4).) A product of two such terms is

$$\begin{aligned} y^c x^a [x, y]^b \cdot y^{c'} x^{a'} [x, y]^{b'} &= y^c (x^a y^{c'}) x^{a'} [x, y]^{b+b'} \\ &= y^c (y^{c'} x^a [x, y]^{ac'}) x^{a'} [x, y]^{b+b'} \quad \text{by (3.5)} \\ &= y^{c+c'} x^{a+a'} [x, y]^{b+b'+ac'}. \end{aligned}$$

Here the exponents are all integers. Comparing this with (3.2), it appears we have a homomorphism $\text{Heis}(\mathbf{Z}/(p)) \rightarrow G$ by

$$(3.6) \quad \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mapsto y^c x^a [x, y]^b.$$

After all, we just showed multiplication of such triples $y^c x^a [x, y]^b$ behaves like multiplication in $\text{Heis}(\mathbf{Z}/(p))$. But there is a catch: the matrix entries a , b , and c in $\text{Heis}(\mathbf{Z}/(p))$ are integers modulo p , so the “function” (3.6) from $\text{Heis}(\mathbf{Z}/(p))$ to G is only well-defined if x , y , and $[x, y]$ all have p -th power 1 (so exponents on them only matter mod p). Since $[x, y]$ is in the center of G , a subgroup of order p , its exponents only matter modulo p . But maybe x or y could have order p^2 .

Well, if x and y both have order p , then there is no problem with (3.6). It is a well-defined function $\text{Heis}(\mathbf{Z}/(p)) \rightarrow G$ that is a homomorphism. Since its image contains x and y , the image contains $\langle x, y \rangle = G$, so the function is onto. Both $\text{Heis}(\mathbf{Z}/(p))$ and G have order p^3 , so our surjective homomorphism is an isomorphism: $G \cong \text{Heis}(\mathbf{Z}/(p))$.

What happens if x or y has order p^2 ? In this case we anticipate that $G \cong G_p$. In G_p , two generators are $g = \begin{pmatrix} 1+p & 0 \\ 0 & 1 \end{pmatrix}$ and $h = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, where g has order p , h has order p^2 , and $[g, h] = h^p$. We want to show our abstract G also has a pair of generators like this.

Starting with $G = \langle x, y \rangle$ where x or y has order p^2 , without loss of generality let y have order p^2 . It may or may not be the case that x has order p . To show we can change generators to make x have order p , we will look at the p -th power function on G . For all

$g \in G$, $g^p \in Z$ since $G/Z \cong \mathbf{Z}/(p) \times \mathbf{Z}/(p)$. Moreover, the p -th power function on G is a *homomorphism*: by Lemma 3.1, $(gh)^p = g^p h^p [g, h]^{p(p-1)/2}$ and $[g, h]^p = 1$ since $[G, G] = Z$ has order p , so

$$(gh)^p = g^p h^p.$$

Since y^p has order p and $y^p \in Z$, $Z = \langle y^p \rangle$. Therefore $x^p = (y^p)^r$ for some $r \in \mathbf{Z}$, and since the p -th power function on G is a homomorphism we get $(xy^{-r})^p = 1$, with $xy^{-r} \neq 1$ since $x \notin \langle y \rangle$. So xy^{-r} has order p and $G = \langle x, y \rangle = \langle xy^{-r}, y \rangle$. We now rename xy^{-r} as x , so $G = \langle x, y \rangle$ where x has order p and y has order p^2 .

We are not guaranteed that $[x, y] = y^p$, which is one of the relations for the two generators of G_p . How can we force this relation to occur? Well, since $[x, y]$ is a nontrivial element of $[G, G] = Z$, $Z = \langle [x, y] \rangle = \langle y^p \rangle$, so

$$(3.7) \quad [x, y] = (y^p)^k,$$

where $k \not\equiv 0 \pmod{p}$. Let ℓ be a multiplicative inverse for $k \pmod{p}$ and raise both sides of (3.7) to the ℓ th power: using Lemma 3.1,

$$[x, y]^\ell = (y^{p^\ell})^\ell \implies [x^\ell, y] = y^p.$$

Since $\ell \not\equiv 0 \pmod{p}$, $\langle x \rangle = \langle x^\ell \rangle$, so we can rename x^ℓ as x : now $G = \langle x, y \rangle$ where x has order p , y has order p^2 , and $[x, y] = y^p$.

Because $[x, y]$ commutes with x and y and $G = \langle x, y \rangle$, every element of G has the form $y^j x^i [x, y]^k = [x, y]^k y^j x^i = y^{p^{k+j}} x^i$. Let's see how such products multiply:

$$\begin{aligned} y^b x^m \cdot y^{b'} x^{m'} &= y^b (x^m y^{b'}) x^{m'} \\ &= y^b (y^{b'} x^m [x, y]^{mb'}) x^{m'} \\ &= y^{b+b'} x^m (y^p)^{mb'} x^{m'} \\ &= y^{b+b'+pmb'} x^{m+m'}. \end{aligned}$$

Comparing this with (3.3), we have a homomorphism $G_p \rightarrow G$ by

$$\begin{pmatrix} 1+pm & b \\ 0 & 1 \end{pmatrix} \mapsto y^b x^m.$$

(This function is well-defined since on the left side m matters mod p and b matters mod p^2 while $x^p = 1$ and $y^{p^2} = 1$.) This homomorphism is onto since x and y are in the image, so it is an isomorphism since G_p and G have equal order: $G \cong G_p$. \square

4. NONISOMORPHIC GROUPS WITH THE SAME SUBGROUP LATTICE

When $p = 2$, the five groups of order 8 have different subgroup lattices. This is almost entirely explained by counting subgroups of order 2 (equivalently, counting elements of order 2): 1 for $\mathbf{Z}/(8)$, 3 for $\mathbf{Z}/(2) \times \mathbf{Z}/(4)$, 7 for $(\mathbf{Z}/(2))^3$, 5 for D_4 , and 1 for Q_8 . While the count is the same for $\mathbf{Z}/(8)$ and Q_8 , these groups have different numbers of subgroups of order 4: 1 for $\mathbf{Z}/(8)$ and 3 for Q_8 .

For $p \neq 2$, we'll show the subgroup lattices of G_p and $\mathbf{Z}/(p) \times \mathbf{Z}/(p^2)$ are the same.

Theorem 4.1. *For odd prime p , both G_p and $\mathbf{Z}/(p) \times \mathbf{Z}/(p^2)$ have the same subgroup lattice:*

- $p + 1$ subgroups of order p and $p + 1$ subgroups of order p^2 ,

- a unique subgroup H_0 of order p^2 that contains all subgroups of order p ,
- a unique subgroup K_0 of order p that is contained in all subgroups of order p^2 ,
- each subgroup of order p^2 besides H_0 contains K_0 as its only subgroup of order p ,
- each subgroup of order p besides K_0 has H_0 as the only subgroup of order p^2 containing it.

Figure 1 is the subgroup lattice for G_3 . It reflects all 5 properties of Theorem 4.1.

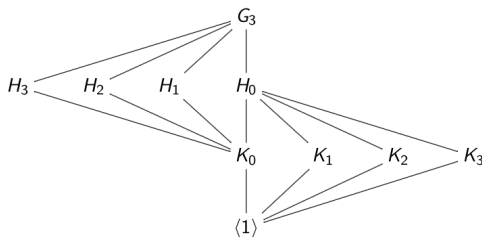


FIGURE 1. Subgroup lattice for G_3 .

Theorem 4.1 is false for $p = 2$: $G_2 \cong D_4$ has 5 subgroups of order 2 and 3 subgroups of order 4 while $\mathbf{Z}/(2) \times \mathbf{Z}/(4)$ has 3 subgroups of order 2 and 3 subgroups of order 4. All nonisomorphic groups of order 8 have different subgroup lattices.

Proof. Case 1: subgroups of $\mathbf{Z}/(p) \times \mathbf{Z}/(p^2)$. Elements of order 1 or p are (a, b) where $b \in p\mathbf{Z}/(p^2)$, so there are $p^2 - 1$ elements of order p . Different subgroups of order p intersect trivially, so the number of subgroups of order p is $(p^2 - 1)/(p - 1) = p + 1$.

The elements of order 1 or p fill up the subgroup $H_0 := \{(a, b) : b \in p\mathbf{Z}/(p^2)\}$, which has order p^2 and is not cyclic. Since H_0 contains all the subgroups of order p , other subgroups of order p^2 must have an element of order p^2 and are therefore cyclic. Elements of order p^2 are (a, b) where $b \in (\mathbf{Z}/(p^2))^\times$, and the subgroup $\langle(a, b)\rangle$ has a generator of the form $(c, 1)$. As c varies in $\mathbf{Z}/(p)$, the p subgroups $\langle(c, 1)\rangle$ have order p^2 and are distinct, so the number of subgroups of order p^2 is $p + 1$.

In each cyclic subgroup $\langle(c, 1)\rangle$ of order p^2 , the subgroup of order p is $K_0 = \langle p(c, 1) \rangle = \langle(p, 0)\rangle$, which is independent of c . So K_0 is the only subgroup of order p in subgroups of order p^2 besides H_0 .

Case 2: subgroups of G_p . Check by induction that for integers $n \geq 0$,

$$\begin{pmatrix} 1 + pm & b \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 + npm & (n + \frac{n(n-1)}{2}pm)b \\ 0 & 1 \end{pmatrix}$$

Since p is odd, $p(p-1)/2$ is divisible by p , so

$$\begin{pmatrix} 1 + pm & b \\ 0 & 1 \end{pmatrix}^p = \begin{pmatrix} 1 & pb \\ 0 & 1 \end{pmatrix}.$$

Therefore $\begin{pmatrix} 1+pm & b \\ 0 & 1 \end{pmatrix}^p$ is trivial if and only if $b \in p\mathbf{Z}/(p^2)$. Writing $b \equiv p\ell \pmod{p^2}$,

$$\begin{pmatrix} 1 + pm & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 + pm & p\ell \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & p\ell \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 + pm & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}^\ell \begin{pmatrix} 1 + p & 0 \\ 0 & 1 \end{pmatrix}^m$$

for $\ell, m \in \mathbf{Z}/(p)$. So there are $p^2 - 1$ elements of order p .

Check $\begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1+p & 0 \\ 0 & 1 \end{pmatrix}$ commute, so the elements of G_p with order p are the nontrivial elements of the subgroup $H_0 := \langle \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1+p & 0 \\ 0 & 1 \end{pmatrix} \rangle$, which has order p^2 and is not cyclic. A subgroup of G_p with order p^2 besides H_0 must have an element of order p^2 , so subgroups of order p^2 besides H_0 are cyclic. Elements of G_p with order p^2 are $\begin{pmatrix} 1+pm & b \\ 0 & 1 \end{pmatrix}$ where $b \in (\mathbf{Z}/(p^2))^\times$ and $\langle \begin{pmatrix} 1+pm & b \\ 0 & 1 \end{pmatrix} \rangle$ has a generator of the form $\begin{pmatrix} 1+pc & 1 \\ 0 & 1 \end{pmatrix}$ for $c \in \mathbf{Z}/(p)$. These subgroups for different c are distinct, so the number of subgroups of order p^2 is $p + 1$. In $\langle \begin{pmatrix} 1+pc & 1 \\ 0 & 1 \end{pmatrix} \rangle$, the subgroup of order p is $K_0 = \langle \begin{pmatrix} 1+pc & 1 \\ 0 & 1 \end{pmatrix}^p \rangle = \langle \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix} \rangle$, which is independent of c . Therefore K_0 is the only subgroup of G_p with order p that is contained in subgroups of order p^2 other than H_0 . \square

5. COUNTING p -GROUPS BEYOND ORDER p^3

Let's summarize what is known about the count of groups of small p -power order.

- There is one group of order p up to isomorphism.
- There are two groups of order p^2 up to isomorphism: $\mathbf{Z}/(p^2)$ and $\mathbf{Z}/(p) \times \mathbf{Z}/(p)$.
- There are five groups of order p^3 up to isomorphism, but our explicit description of them is not uniform in p since the case $p = 2$ used a separate treatment.

For groups of order p^4 , the count is no longer uniform in p : there are 14 groups of order 2^4 and 15 groups of order p^4 for $p \neq 2$. This is due to Hölder [7] and Young [13]. A recent account of this result by Adler, Garlow, and Wheland is on the arXiv [1]. For groups of order p^5 , the count depends on $p \bmod 12$ as shown in the table below. This is due to Miller [9] for $p = 2$ and Bagnera [2] for $p > 2$. Tables listing groups of order 32 and 243 are available at Tim Dokchitser's site [6]. The first count of groups of order p^6 is due to Potron [12], with a modern count being made by Newman, O'Brien, and Vaughan-Lee [10]. A count of groups of order p^7 is due to O'Brien and Vaughan-Lee [11].

p	2	3	1 mod 12	5 mod 12	7 mod 12	11 mod 12
Groups of order p^5	51	67	$2p + 71$	$2p + 67$	$2p + 69$	$2p + 65$

REFERENCES

- [1] J. D. Adler, M. Garlow, and E. R. Wheland, "Groups of order p^4 made less difficult." URL <https://arxiv.org/abs/1611.00461>.
- [2] G. Bagnera, "La composizione dei gruppi finiti il cui grado è la quinta potenza di un numero primo," *Ann. Mat. Pura Appl.* **1** (1898), 137–228.
- [3] A. Cayley, "On the theory of groups, as depending on the symbolic equation $\theta^n = 1$, Part III" *Philos. Mag.* **18** (1859), 34–37. URL <https://www.tandfonline.com/doi/abs/10.1080/14786445908642716>.
- [4] A. Cayley, "On the theory of groups," *Amer. J. Math.* **11** (1889), 139–157. URL <https://archive.org/details/details/jstor-2369415>.
- [5] F. N. Cole and J. W. Glover, "On groups whose orders are products of three prime factors," *Amer. J. Math.* **15** (1893), 191–220. URL <https://www.jstor.org/stable/2369839>.
- [6] T. Dokchitser, Group Names, <https://people.maths.bris.ac.uk/~matyd/GroupNames/>.
- [7] O. Hölder, "Die Gruppen der Ordnungen p^3, pq^2, pqr, p^4 ," *Math. Ann.* **43** (1893), 301–412. URL <https://eudml.org/doc/157685>.
- [8] A. B. Kempe, "A memoir on the theory of mathematical form," *Phil. Trans.* **177** (1886), 1–70. URL <https://royalsocietypublishing.org/doi/10.1098/rstl.1886.0002>.
- [9] G. A. Miller, "The regular substitution groups whose order is less than 48," *Quart. J. Math.* **28** (1896), 232–284.

- [10] M. F. Newman, E. A. O'Brien, and M. R. Vaughan-Lee, "Groups and nilpotent Lie rings whose order is the sixth power of a prime," *J. Algebra* **278** (2004), 383–401.
- [11] E. A. O'Brien and M. R. Vaughan-Lee, "The groups of order p^7 for odd prime p ," *J. Algebra* **292** (2005), 243–258.
- [12] M. Potron, "Sur quelques groupes d'ordre p^6 ," Ph.D. thesis, Gauthier-Villars, Paris, 1904.
- [13] J. Young, "On the determination of the groups whose order is a power of a prime," *Amer. J. Math.* **15** (1893), 124–178. URL <https://www.jstor.org/stable/2369564>.