GROUPS OF ORDER p^3

KEITH CONRAD

For any prime p, we want to describe the groups of order p^3 up to isomorphism. 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 $\mathbf{Z}/(p) \times \mathbf{Z}/(p) \times \mathbf{Z}/(p)$. 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. The descriptions of these two groups will be different for $p = 2$ and $p \neq 2$, so we will treat these cases separately after the following lemma.

Lemma 1. *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 any group G, if G/Z is cyclic then G is abelian. So G being nonabelian forces has 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 $[G, G] = Z$. □

Theorem 2. *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 $yxy^{-1} \in \langle x \rangle$:

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

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

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

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 $y^2 = x^2$.

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

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

or

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

In the first case $G \cong D_4$ and in the second case $G \cong Q_8$. $\square$

From now on we take $p \neq 2$. The two nonabelian groups of order p^3, up to isomorphism, will turn out to be

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

and

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

where m actually only matters modulo p.[1] 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 $\mathrm{Heis}(\mathbf{Z}/(p))$ from G_p for $p \neq 2$ by counting elements of order p. In $\mathrm{Heis}(\mathbf{Z}/(p))$,

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

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

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

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

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+a' & b+b'+ac' \\ 0 & 1 & c+c' \\ 0 & 0 & 1 \end{pmatrix} \tag{2}$$

and in G_p

$$\begin{pmatrix} 1+pm & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1+pm' & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1+p(m+m') & b+b'+pmb' \\ 0 & 1 \end{pmatrix}. \tag{3}$$

[1] The notation G_p for this group is not standard. I don't know a standard notation for it.

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

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

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

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = y^c x^a [x,y]^b. \tag{4}$$

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

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

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. *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. □

Theorem 4. *For primes $p \neq 2$, a nonabelian group of order p^3 is isomorphic to* $\mathrm{Heis}(\mathbf{Z}/(p))$ *or G_p.*

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

By Lemma 1, we can write $G/Z = \langle \overline{x}, \overline{y} \rangle$ and $Z = \langle z \rangle$. For any $g \in G$, $g \equiv x^i y^j \bmod Z$ 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,

$$x^i y^j = y^j x^i [x,y]^{ij}, \quad y^j x^i = x^i y^j [x,y]^{-ij}. \tag{5}$$

This shows we can move any power of y past any 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 (4).) A product of two such terms is

$$\begin{aligned} y^c x^a [x,y]^b \cdot y^{c'} x^{a'} [x,y]^{b'} &= y^c (x^a y^{c'}) x^{a'} [x,y]^{b+b'} \\ &= y^c (y^{c'} x^a [x,y]^{ac'}) x^{a'} [x,y]^{b+b'} \quad \text{by (5)} \\ &= y^{c+c'} x^{a+a'} [x,y]^{b+b'+ac'}. \end{aligned}$$

Here the exponents are all integers. Comparing this with (2), it appears we have a homomorphism $\mathrm{Heis}(\mathbf{Z}/(p)) \to G$ by

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mapsto y^c x^a [x,y]^b. \tag{6}$$

After all, we just showed multiplication of such triples $y^c x^a [x,y]^b$ behaves like multiplication in $\mathrm{Heis}(\mathbf{Z}/(p))$. But there is a catch: the matrix entries a, b, and c in $\mathrm{Heis}(\mathbf{Z}/(p))$ are integers modulo p, so the "function" (6) from $\mathrm{Heis}(\mathbf{Z}/(p))$ 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 (6). It is a well-defined function $\mathrm{Heis}(\mathbf{Z}/(p)) \to G$ 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 $\mathrm{Heis}(\mathbf{Z}/(p))$ and G have order p^3, so our surjective homomorphism is an isomorphism: $G \cong \mathrm{Heis}(\mathbf{Z}/(p))$.

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 $g = \left(\begin{smallmatrix} 1+p & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $h = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, 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 any $g \in G$, $g^p \in Z$ 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, $(gh)^p = g^p h^p [g,h]^{p(p-1)/2}$ 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

$$[x,y] = (y^p)^k, \tag{7}$$

where $k \not\equiv 0 \bmod p$. Let ℓ be a multiplicative inverse for $k \bmod p$ and raise both sides of (7) to the ℓth power: using Lemma 3,

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

Since $\ell \not\equiv 0 \bmod p$, $\langle x \rangle = \langle x^\ell \rangle$, 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 $y^j x^i [x, y]^k = [x, y]^k y^j x^i = y^{pk+j} x^i$. 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), we have a homomorphism $G_p \to G$ 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: $G \cong G_p$. $\square$

Let's summarize what can be said about 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 16 and 15 groups of order p^4 for $p \neq 2$. This was first determined by Hölder (1893), who also classified the groups of order p^3.