Groups of order $p^2q$, $p > q$ both prime.

Let $G$ be a group of order $p^2q$, with $p > q$ both prime. Since $1 + kp$ divides $q$ only if $k = 1$, the Sylow $p$-subgroup $S_p$ is normal in $G$. It follows that $G \cong S_p \times qZ_q$ for some $\theta : Z_q \rightarrow \text{Aut}(S_p)$. If $q$ does not divide $p^2 - 1$ then $1 + kq \neq p$ or $p^2$, so $1 + kq$ does not divide $p^2$ unless $k = 0$. In this case, then, $S_q$ too is normal, whence $G$ is abelian, and so isomorphic to $Z_{p^2} \times Z_q$ or to $Z_p \times Z_p \times Z_q$. Thus there is no more to do unless $q|(p^2 - 1)$, which is assumed from now on.

Assume further that $\theta$ is injective, since otherwise $G$ is abelian.

Then check that with $W := \theta(Z_q)$, $G$ is isomorphic to the group of transformations $T_{z,w} : S_p \rightarrow S_p$ ($z \in S_p, w \in W$) where

$$T_{z,w}(x) = wx + z.$$ 

To classify such groups, suppose first that $S_p \cong Z_{p^2}$.

**Lemma 1.** $\text{Aut}(Z_{p^2}) \cong Z_{p^2}^*$ is cyclic, of order $p(p - 1)$.

**Proof.** We have seen the isomorphism before; and $|Z_{p^2}^*| = \phi(p^2) = p(p - 1)$. We also know that $Z_p^*$ is cyclic. Choose $z \in Z_{p^2}^*$ so that its natural image in $Z_p^*$ is a generator. It holds that $z^a \equiv 1 \pmod{p^2} \implies z^a \equiv 1 \pmod{p} \implies (p - 1)|a$. So the order of $z$ is a multiple of $p - 1$, and also is a divisor of $p(p - 1)$, and thus can only be $p - 1$ or $p(p - 1)$. In the latter case, $z$ generates $Z_{p^2}^*$. In the former case, the binomial expansion gives

$$(z + p)^{p^2 - 1} \equiv z^{p^2 - 1} + (p - 1)pz^{p^2 - 2} \equiv 1 - pz^{p^2 - 2} \equiv 1 \pmod{p^2}.$$

As before, $z + p$—which has the same image in $Z_p^*$ as $z$ does—has order $p - 1$ or $p(p - 1)$, and we've just seen that it can't be $p - 1$, so it must be $p(p - 1)$, i.e., $z + p$ generates $Z_{p^2}^*$. Thus in any case, $Z_{p^2}^*$ is indeed cyclic. \(\square\)

**Remark.** A similar argument shows, via induction, that $Z_{p^n}^*$ is cyclic for any $n > 0$.

Clearly, an injective $\theta$ exists $\iff q|(p^2 - 1)$, i.e., $q|(p - 1)$. So when $q$ does divide $p - 1$, we find, arguing as for groups of order $pq$, that there is just one nonabelian group of order $p^2q$ having a cyclic $S_p$, namely, with $W$ the unique order-$q$ subgroup of $Z_{p^2}^*$, the group of transformations $T_{z,w} : Z_{p^2} \rightarrow Z_{p^2}$ ($z \in Z_{p^2}, w \in W$) where

$$T_{z,w}(x) = wx + z.$$ 

Now the fun begins.

Suppose next that $S_p \cong Z_p \times Z_p$, a two-dimensional vector space over the field $Z_p$. Any group automorphism of $Z_p \times Z_p$ is an invertible $Z_p$-linear map (why?), and so $\text{Aut}(Z_p \times Z_p)$ is isomorphic to the group $\text{GL}_2(Z_p)$ of invertible $2 \times 2$ matrices with $Z_p$-entries.

Noting that any automorphism $\phi$ of $G$ must take the unique order-$p^2$ subgroup $H := S_p$ to itself, and that $H$ is abelian, deduce from the handout on isomorphisms of semi-direct products that, for two homomorphisms $\theta_i : Z_q \rightarrow \text{Aut}(S_p)$,

$$S_p \rtimes_{\theta_1} Z_q \cong S_p \rtimes_{\theta_2} Z_q \iff \theta_1(Z_q) \text{ and } \theta_2(Z_q) \text{ are conjugate subgroups of } \text{Aut}(S_p).$$

Thus the classification problem becomes the linear-algebra problem of determining the conjugacy classes of order-$q$ subgroups of $\text{GL}_2(Z_p)$. 

1
One often says two matrices in $\text{GL}_2(\mathbb{Z}_p)$ are “similar” rather than “conjugate.” (Both terms mean the same thing here.) How do we detect similarity?

**Lemma 2.** Let $A$ be a $2 \times 2$ matrix over a field $k$. If $A$ is not a scalar multiple of the identity matrix, then $A$ is similar to the matrix

$$
\begin{pmatrix}
0 & -d \\
1 & t
\end{pmatrix} \\
(d = \det A, \ t = \text{trace } A)
$$

**Proof.** Representing elements of $k^2$ as $2 \times 1$ column vectors, let $T: k^2 \to k^2$ be the linear map given by left multiplication by $A$. If every vector in $k^2$ is an eigenvector of $A$, then $A$ is a scalar multiple of the identity. (Show this, e.g., by using that $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, and $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ are eigenvectors.)

Otherwise, some nonzero vector $v \in k^2$ is not an eigenvector of $A$, and the pair $(v, Tv)$ forms a basis of $k^2$. The matrix of $T$ w.r.t. this basis has the form $\begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix}$. This matrix, being similar to $A$, has the same determinant and trace, i.e., $-a = d$ and $b = t$. □

**Corollary.** Two non-scalar $2 \times 2$ matrices over $k$ are similar iff they have the same eigenvalues.

Now we can start counting conjugacy classes. Henceforth, $A$ is a matrix of order $q$, i.e., if $I$ is the $2 \times 2$ identity matrix then $A^q = I$ and $A \neq I$. The eigenvalues of such an $A$ are $q$-th roots of unity.

If these eigenvalues are both 1, and $A \neq I$, then Lemma 2 gives that $A$ is similar to $B := \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}$. By induction, one shows that for $n > 0$,

$$B^n = \begin{pmatrix} 0 & -1 \\ 1 & 2 \end{pmatrix}^n = \begin{pmatrix} 1-n & -n \\ n & n+1 \end{pmatrix}.$$

Hence $B^p = I$, hence $B^q \neq I$ (else $B = I$ would follow), hence $A^q \neq I$. So the eigenvalues can’t both be 1.

Recall that $q$ divides $p^2 - 1$, so $q$ divides $p - 1$ or $p + 1$, but not both if $q$ is odd.

There are, then, three cases to examine.

(A) $q = 2$.

(B) $q|(p+1)$, $q \nmid (p-1)$.

(C) $q|(p-1)$, $q \nmid (p+1)$.

(A) Two order-2 subgroup of $\text{GL}_2(\mathbb{Z}_p)$ are conjugate if and only if their unique generators are similar. The eigenvalues of $A$ are $(-1, -1)$ or $(1, -1)$. It follows that every order-2 subgroup of $\text{GL}_2(\mathbb{Z}_p)$ is similar to one and only one of the three groups generated respectively by

$$
\begin{pmatrix}
-1 & 0 \\
0 & -1
\end{pmatrix}, \quad
\begin{pmatrix}
-1 & 1 \\
0 & -1
\end{pmatrix}, \quad
\begin{pmatrix}
1 & 0 \\
0 & -1
\end{pmatrix}.
$$

The corresponding three pairwise nonisomorphic semidirect products $G$ have generators $x, y, z$ which satisfy $x^p = y^p = z^2 = e$, $xy = yx$, and $zx = x^{-1}z$, $zy = y^{-1}z$, respectively $zx = x^{-1}z$, $zy = xy^{-1}z$, respectively $zx = xz$, $zy = y^{-1}z$. (The third of these is isomorphic to $\mathbb{Z}_p \times D_{2p}$.)
(B) Since $q$ doesn’t divide $p - 1$, $\mathbb{Z}_p^*$ has no elements of order $q$, that is, 1 is the only $q$-th root of unity in $\mathbb{Z}_p$. Hence the eigenvalues $\lambda$ and $\lambda'$ of $A$ satisfy $\lambda \lambda' = \det A = 1$. If $\lambda = 1$, then $\lambda' = 1$, which, we’ve seen, can’t happen. Since $\lambda$ is a root of a quadratic equation—the characteristic equation of $A$—therefore $\mathbb{Z}_p[\lambda]$ is a quadratic extension of $\mathbb{Z}_p$ (considered as a field); and this quadratic extension contains all the roots of the equation $X^q = 1$ (over $\mathbb{Z}_p$), namely the powers of $\lambda$.

Now if $B \neq I$ satisfies $B^q = I$, then the eigenvalues of $B$ must be of the form $(\lambda^a, 1/\lambda^a)$ $(a, q) = 1$. Hence $B$ is similar to $A^a$, and there is at most one conjugacy class of order-$q$ subgroups of $\text{GL}_2(\mathbb{Z}_p)$.

To show that there is at least one order-$q$ subgroup, i.e., that there is an element of order $q$, we need only show that $q$ divides the order of $\text{GL}_2(\mathbb{Z}_p)$. But to specify an invertible $2 \times 2$ $\mathbb{Z}_p$-matrix, we can put any one of the $p^2 - 1$ nonzero row vectors in the first row, and then put any one of the $p^2 - p$ row vectors which are not scalar multiples of the first row in the second row. Thus $\text{GL}_2(\mathbb{Z}_p)$ has order $(p^2 - 1)(p^2 - p)$, which is indeed divisible by $q$.

In conclusion, in this case there exists a unique nonabelian semidirect product.

(C) Now there are $q$ $q$-th roots of unity, forming a subgroup, necessarily cyclic, of $\mathbb{Z}_p^*$, with generator, say, $\zeta$. The eigenvalues of $A$ must then have the form $(\zeta^a, \zeta^b)$, where at least one of $a, b$, say $a$, is not divisible by $q$; and then if $c = a^{-1}$ (mod $q$), $A^c$ has eigenvalues $(\zeta, \zeta^d)$ $(0 \leq d < q)$, and $A^c$ generates the same order-$q$ subgroup, call it $U$, as $A$ does.

Suppose $B$ generates an order-$q$ subgroup $V$, and that the eigenvalues of $B$ are $(\zeta, \zeta^c)$. Then $U$ is conjugate to $V$ iff $A$ is similar to some power $B^f$, i.e., the unordered pairs $(\zeta, \zeta^d)$ and $(\zeta^f, \zeta^{cf})$ are the same. This means that either $f = 1$ and $c = d$ or $f = d \neq 0$ and $c = d^{-1}$.

In conclusion, when $q$ is odd and $q|(p - 1)$, the set of conjugacy classes of order-$q$ subgroups of $\text{GL}_2(\mathbb{Z}_p)$ corresponds 1-1 with the set consisting of the $(q - 3)/2$ pairs $(d, d^{-1})$ $(d \neq d^{-1} \in \mathbb{Z}_q^*)$ together with the pairs $(1, 1)$, $(1, -1)$, and $(1, 0)$. Thus there are $(q + 3)/2$ such conjugacy classes, and correspondingly, there are $(q + 3)/2$ nonabelian semidirect products.

*Question:* Which of these is $\mathbb{Z}_p \times H_{pq}$, where $H_{pq}$ is the nonabelian group of order $pq$?

**Exercise.** How many distinct nonabelian groups are there having the following orders?

98, 147 (cf. D&F, p. 185,#10), 847, 1183, 5887.