Before we get started, let me prove a fact we have referred to several times during the semester, but for which I haven’t yet actually shown you a proof:

**Theorem 0.1.** Let $p$ be a prime number, and let $G$ be a group of order $p$. Then $G$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

**Proof.** First, I claim that $G$ is cyclic, i.e., that $G$ can be generated by a single element. Here is a proof of this claim, by contrapositive: suppose that $G$ is not cyclic. Then, for any element $g \in G$, the subgroup $\langle g \rangle$ of $G$ generated by $g$ cannot be all of $G$, or otherwise $g$ would be a one-element generating set for $G$. So the order of $\langle g \rangle$ must divide the order of $G$. But the order of $G$ is prime, so the order of $\langle g \rangle$ must be either 1 or $p$. The order of $\langle g \rangle$ cannot be $p$, since then $\langle g \rangle = G$, and $G$ has a one-element generating set, contradicting our assumption that $G$ is not cyclic. So the order of $\langle g \rangle$ must be 1. So $g$ must be the identity element of $G$. But this argument made no assumptions on the choice of element $g \in G$, so every element $g \in G$ is the unit element. So $G$ has only a single element, so $p = 1$, a contradiction. So our assumption that $G$ is not cyclic must be false. So $G$ is cyclic.

So $G$ is cyclic. You proved in an earlier homework assignment that every cyclic group is isomorphic to either $\mathbb{Z}$ or to $\mathbb{Z}/n\mathbb{Z}$ for some positive integer $n$, and the only possibility which has the correct order is $\mathbb{Z}/p\mathbb{Z}$. So $G \cong \mathbb{Z}/p\mathbb{Z}$. □

1. **The Sylow theorems.**

**Definition 1.1.** Let $G$ be a finite group and let $p$ be a prime number. A subgroup $H$ of $G$ is called a $p$-Sylow subgroup of $G$ if the order of $H$ is the largest power of $p$ which divides the order of $G$.

**Theorem 1.2.** (The Sylow theorems.) Let $G$ be a finite group and let $p$ be a prime number.

1. If $p^n$ divides the order of $G$, then $G$ contains a subgroup of order $p^n$. In particular, $G$ contains a $p$-Sylow subgroup.
2. Any two $p$-Sylow subgroups of $G$ are conjugate to one another. Furthermore, any subgroup of $G$ whose order is a power of $p$ is contained in some $p$-Sylow subgroup of $G$.
3. Suppose $p^n$ is the largest power of $p$ that divides $\#(G)$. Then the number of $p$-Sylow subgroups of $G$ is congruent to 1 modulo $p$, and also is a divisor of $\#(G)/p^n$.

**Proof.** We prove the three parts in order:

1. By induction: clearly the claim is true when $\#(G) = 1$. Suppose the claim have already been shown for all group of order $< m$, and suppose that $G$ is a group of order $m$. If there exists an element $x \in G$ such that $x \not\in Z(G)$ and $p$ does not divide $[G : C_G(x)]$, then we also know that $p^n$ divides $\#(G) = [G : C_G(x)]\#(C_G(x))$, so $p^n$ must divide $\#(C_G(x))$. Since $x \not\in Z(G)$, we also know that $\#(C_G(x)) < m$.
hence \( C_G((x)) \) contains a subgroup of order \( p^n \), by the inductive hypothesis, and that subgroup of order \( p^n \) is also a subgroup of \( G \), and we are done!

So suppose instead that \( G \) does not contain an element \( x \) such that \( x \notin Z(G) \) and such that \( p \) does not divide \( [G : C_G((x))] \). Then \( p \) divides \( [G : C_G((x))] \) for all \( x \notin Z(G) \). So, reducing the class equation modulo \( p \), we have that \( \#(G) \equiv \#(Z(G)) \mod p \). The claim is immediate when \( p = 1 \), so assume that \( n > 1 \), so that \( p^n \geq p \). Then \( p \) divides \( \#(G) \), so \( p \) divides \( \#(Z(G)) \) by the class equation. So \( Z(G) \) contains an element of order \( p \). Choose an element \( a \in Z(G) \) of order \( p \). Then \( \langle a \rangle \) is a subgroup of \( Z(G) \) isomorphic to \( C_p \), and this subgroup is normal, since it is contained in \( Z(G) \) and hence is fixed by conjugation in \( G \). The quotient group \( G/\langle a \rangle \) has order \( \#(G)/p \), so by the inductive hypothesis, \( G/\langle a \rangle \) contains a subgroup \( H \) of order \( p^{n-1} \).

Now let \( q : G \to G/\langle a \rangle \) be the quotient map, and consider the preimage \( q^{-1}(H) \subseteq G \); you know from basic material on subgroups that taking preimages gives you a bijection between subgroups of \( G/\langle a \rangle \) and subgroup of \( G \) that contains \( \langle a \rangle \), so \( q^{-1}(H) \) is a subgroup of \( G \) which surjects on to \( H \) with kernel \( \langle a \rangle \), so the order of \( q^{-1}(H) \) is \( \#(G)/\#(H) = (p)(p^{n-1}) = p^n \). So \( q^{-1}(H) \) is a subgroup of \( G \) of order \( p^n \).

Hence every group \( G \) of order \( m \) contains a subgroup of order \( p^n \), completing the inductive step.

(2) For proofs of the remaining parts, refer to your textbook.

\[ \square \]

**Lemma 1.3.** Let \( G \) be a group and let \( H \) be a subgroup of \( G \). Suppose that the index of \( H \) in \( G \) is 2. Then \( H \) is normal in \( G \).

**Proof.** Let \( g \in G \). If \( g \in H \), then \( g^{-1}Hg = H \), since \( H \) is a subgroup. If \( g \notin H \), then \( Hg = G\setminus H \), since there are only two cosets of \( H \) in \( G \). But if \( g \notin H \) then we also have that \( g^{-1} \notin H \) and hence \( g^{-1}Hg = g^{-1}(G\setminus H) = H \). So \( g^{-1}Hg \) for all \( g \in G \). So \( H \) is normal in \( G \). \[ \square \]

**Theorem 1.4.** Let \( p > 2 \) be a prime number and let \( G \) be a group of order \( 2p \). Then \( G \) is either a cyclic group or \( G \) is isomorphic to the dihedral group of order \( 2p \).

**Proof.** Since \( G \) has order \( 2p \), \( G \) contains an element \( a \) of order \( p \) and an element \( b \) of order 2. The subgroup \( \langle a \rangle \) generated by \( a \) in \( G \) is index 2, hence \( \langle a \rangle \) is a normal subgroup of \( G \), by Lemma 1.3. Hence \( b^{-1}ab \) is equal to some element of \( \langle a \rangle \), say, \( a^x \). Now \( b^2 = 1 = b^{-2} \), so

\[
\begin{align*}
a &= b^{-2}ab^2 \\
  &= b^{-1}(b^{-1}ab)b \\
  &= b^{-1}(a^x)b \\
  &= b^{-1}a(bb^{-1})a(bb^{-1})a...a(bb^{-1})a(bb^{-1})ab \\
  &= (b^{-1}ab)(b^{-1}ab)(b^{-1}ab)...(b^{-1}ab)(b^{-1}ab) \\
  &= a^x a^{x^2} a^{x^3} ... a^{x^2} \\
  &= a^{x^2}.
\end{align*}
\]

So \( a = a^{x^2} \), so \( n^2 \) is congruent to 1 modulo \( p \). The only square roots of 1 modulo \( p \) are 1 and -1, so \( n \) is congruent to \( \pm 1 \) modulo \( p \), so \( b^{-1}ab = a \) and \( b^{-1}ab = a^{-1} \) are the only two
Proposition 1.5. (Burnside’s pq theorem.) Let $G$ be a group of order $pq$, where $p, q$ are prime numbers, and $q < p$.

1. If $q$ does not divide $p - 1$, then $G$ is cyclic.
2. If $q$ divides $p - 1$, then either $G$ is cyclic or $G$ can be generated by two elements $a, b$ satisfying equations

$$a^p = 1$$
$$b^q = 1$$
$$b^{-1}ab = a^n,$$

with $n \neq 1$ modulo $p$.

Proof. Let $k$ be the number of $p$-Sylow subgroups of $G$. Then $k$ divides $\#(G)/p = q$, so either $k = 1$ or $k = q$, but if $k = q$ then it is impossible for $k$ to be congruent to 1 modulo $p$, since this implies that $q$ is congruent to 1 modulo $p$, and by assumption, $q < p$. So it must be the case that $k = 1$ and there is a unique (hence normal) $p$-Sylow subgroup of $G$, and it is of order $p$, hence cyclic, hence equal to $(a)$ for some $a$ satisfying $a^p = 1$.

Now choose an element $b$ of $G$ of order $q$, and observe that the subgroup $\langle b \rangle$ generated by $b$ is a $q$-Sylow subgroup of $G$. Let $j$ be the number of $q$-Sylow subgroups of $G$, and again there are two cases: since $j$ divides $p$, either $j = 1$ or $j = p$. If $j = 1$ then $\langle b \rangle$ is normal in $G$, and so the element $b^{-1}a^{-1}ba$ is contained in both $\langle a \rangle$ and in $\langle b \rangle$, a $p$-Sylow subgroup and a $q$-Sylow subgroup, where $p \neq q$. So $b^{-1}a^{-1}ba = 1$. So $ab = ba$. So $G$ is abelian and isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$.

The other possibility is that $j = p$. In this case $j$ is also congruent to 1 modulo $q$, again by the Sylow theorems, so $p$ is congruent to 1 modulo $q$. So $q$ divides $p - 1$ (hence, if $q$ does not divide $p - 1$, we must be in the cyclic case above, and the first claim in the statement of the theorem follows). Since $\langle a \rangle$ is still normal in $G$, we have that $b^{-1}ab = n$ for $a^n$. If $n$ were equivalent to 1 modulo $p$ then we would have that $b^{-1}ab = a^n = a$, and hence $ab = ba$ and $G$ is abelian, the case we already covered. So instead $n \neq 1$ modulo $p$. □

2. Nonexistence results for simple groups of a given order.

Definition 2.1. We say that a group $G$ is simple if it has no normal subgroups except the trivial subgroup 1 and $G$ itself.

A major project of 20th century mathematics was the project to classify all finite simple groups. This is a pretty desirable thing to do, since all finite groups can be built up by short exact sequences using finite simple groups as the “building blocks.” This project is now complete and was a major accomplishment of 20th century mathematics, and took the work of many many people to complete.

Suppose $p$ is a prime number. Every group of order $p$ is simple, since you know already that it’s isomorphic to $\mathbb{Z}/p\mathbb{Z}$, which has no subgroups at all (normal or otherwise) except for 1 and $\mathbb{Z}/p\mathbb{Z}$ itself. Proposition 1.5 tells us also that, if $p, q$ are distinct prime numbers, then there are no simple groups of order $pq$. Hence, if $G$ is a nonabelian simple group, then the order of $G$ must be divisible by at least three distinct primes. (It turns out that the smallest nonabelian simple group is $A_5$, the alternating group on 5 letters/symbols, which...
has \(5!/2 = 2^33^5 = 60\) elements.) Typically nonabelian simple groups have order divisible by more than 3 primes, however.

You can prove an enormous number of things about finite groups, especially about finite simple groups, using Sylow theory, if you’re patient and persistent with it. Here is an example:

**Proposition 2.2.** There does not exist a finite simple group of order 30.

**Proof.** First, 30 is divisible by 2, 3, and 5, so Proposition 1.5 doesn’t rule out the possibility of a group of order 30. Instead we have to use some Sylow theory directly. Suppose \(G\) is a group of order 30, and let \(k_3\) be the number of 3-Sylow subgroups of \(G\). Then \(k_3\) is a divisor of \(30/3 = 10\) congruent to 1 modulo 3, so \(k_3\) is 1 or 10. Suppose \(k_3 = 10\). Then \(G\) has 10 3-Sylow subgroups, all congruent to one another. Since 3 is the largest power of 3 dividing 30, each 3-Sylow subgroup of \(G\) has order 3, i.e., each 3-Sylow subgroup of \(G\) is isomorphic to \(\mathbb{Z}/3\mathbb{Z}\). So any two distinct 3-Sylow subgroups intersect only at the identity element \(1 \in G\). So there are ten of these copies of \(\mathbb{Z}/3\mathbb{Z}\) inside \(G\), and each one has 2 elements not contained in any of the others. This accounts for a total of 21 (two times ten, plus one more for the identity element of \(G\)) elements of \(G\) that are contained in 3-Sylow subgroups of \(G\).

Now let \(k_5\) be the number of 5-Sylow subgroups of \(G\). Then \(k_5\) is a divisor of \(30/5 = 6\) congruent to 1 modulo 5, so \(k_5\) is 1 or 6. By the same logic as above, \(G\) contains six copies of \(\mathbb{Z}/5\mathbb{Z}\) which intersect only at the identity element, for a total of 25 (six times four, plus one for the identity element of \(G\)) elements of \(G\).

So there are 19 non-identity elements of \(G\) contained in some 3-Sylow subgroup, and 24 elements of \(G\) contained in some 5-Sylow subgroup. But \(G\) has only 30 elements. So there is some nonidentity element of \(G\) contained in both a 3-Sylow subgroup and a 5-Sylow subgroup, a contradiction. So either \(k_3\) had to be 1, or \(k_5\) had to be 1. In the first case, \(G\) has a normal 3-Sylow subgroup, and in the second case, \(G\) has a normal 5-Sylow subgroup. Either way, \(G\) is not simple! □

**Exercise 2.3.** For which primes \(p < 50\) does there exist a simple group of order \(p + 1\)? (Hint: if you do this without Sylow theory, you will be very unhappy, but if you use Sylow theory and some theorems we have already proven like Burnside’s \(pq\)-theorem, this is actually quite easy!)

3. **Classification of groups of a given order.**

The combination of the Sylow theorems and the theory of semidirect products gives you a powerful set of tools for computing all the isomorphism classes of groups of a given order. Here is an example:

**Example 3.1.** Up to isomorphism, there are exactly five groups of order 18.

**Proof.** **First part: finding a normal subgroup:** Let \(G\) be a group of order 18, and let \(k_3\) be the number of 3-Sylow subgroups of \(G\). Then the Sylow theorems tell us that \(k_3 \equiv 1 \mod 3\), and \(k_3\) divides \(18/9 = 2\). Of course the only divisor of 2 which is congruent to 1 mod 3 is 1, so \(G\) has a unique 3-Sylow subgroup, hence a normal 3-Sylow subgroup, for which I will write \(\text{Syl}_3(G)\). Hence we have a group extension

\[
\text{Syl}_3(G) \to G \to G/\text{Syl}_3(G),
\]

in which \(\text{Syl}_3(G)\) has order 9 and \(G/\text{Syl}_3(G)\) has order 2. Hence \(G/\text{Syl}_3(G) \cong \mathbb{Z}/2\mathbb{Z}\) and \(\text{Syl}_3(G) \cong \mathbb{Z}/9\mathbb{Z}\) or \(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}\).
**Second part: splitting the group extension:** The group $G$ is of order 18, and 2 is a prime dividing 18, hence $G$ contains an element of order 2 by Cauchy’s theorem. Choose such an element $g \in G$, and let $\iota : \mathbb{Z}/2\mathbb{Z} \to G$ denote the group homomorphism sending a generator of $\mathbb{Z}/2\mathbb{Z}$ to $g$. I claim that the composite $\pi \circ \iota$ is the identity map on $\mathbb{Z}/2\mathbb{Z}$. Clearly $\pi \circ \iota$ sends the unit element of $\mathbb{Z}/2\mathbb{Z}$ to itself, since $\iota$ and $\pi$ are both group homomorphisms. Let $x$ denote a generator of $\mathbb{Z}/2\mathbb{Z}$, and suppose that $\pi(\iota(x))$ is the unit element of $\mathbb{Z}/2\mathbb{Z}$. Then $\iota(x)$ must be in the normal subgroup $\text{Syl}_3(G)$ of $G$, by the definition of a group extension and the fact that $3.0.1$ is a group extension. Hence $\text{Syl}_3(G)$ contains an element of order 2. But this is impossible, since 2 does not divide 9. Hence $\pi \circ \iota$ is the identity map on $\mathbb{Z}/2\mathbb{Z}$, hence the group extension $3.0.1$ splits, hence $G$ is a semidirect product: $G \cong \text{Syl}_3(G) \rtimes_\phi G/\text{Syl}_3(G)$ for some group homomorphism $\phi : G/\text{Syl}_3(G) \to \text{Aut}(\text{Syl}_3(G))$.

**Third part: classifying the possible semidirect products:** There are two possibilities: either $\text{Syl}_3(G)$ is isomorphic to $\mathbb{Z}/9\mathbb{Z}$ or to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Let’s handle them separately:

$\text{Syl}_3(G) \cong \mathbb{Z}/9\mathbb{Z}$: The semidirect products $\text{Syl}_3(G) \rtimes_\phi G/\text{Syl}_3(G)$ are all given by group homomorphisms $G \text{Syl}_3(G) \to \text{Aut}(\text{Syl}_3(G))$, and

$$\text{Aut}(\text{Syl}_3(G)) \cong \text{Aut}(\mathbb{Z}/9\mathbb{Z}) \cong \mathbb{Z}/(9)\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}.$$

Since $G/\text{Syl}_3(G)$ is of order 2, we have $G/\text{Syl}_3(G) \cong \mathbb{Z}/2\mathbb{Z}$, and now we get that there are two semidirect products $\mathbb{Z}/9\mathbb{Z} \rtimes_\phi \mathbb{Z}/2\mathbb{Z}$: we can choose $\phi : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ to be the trivial homomorphism (i.e., the morphism sending everything to the unit element), in which case $\text{Syl}_3(G) \rtimes_\phi G/\text{Syl}_3(G) \cong \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, or we can choose $\phi : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ to send the generator of $\mathbb{Z}/2\mathbb{Z}$ to the unique element of order 2 in $\mathbb{Z}/6\mathbb{Z}$, i.e., the automorphism of $\mathbb{Z}/9\mathbb{Z}$ sending 1 to $-1 = 8$. This gives us the semidirect product

$$\mathbb{Z}/9\mathbb{Z} \rtimes_\phi \mathbb{Z}/2\mathbb{Z} \cong \langle \sigma, \tau \mid \sigma^3, \tau^3, \sigma^{-1}\tau\sigma = \tau^5 \rangle,$$

i.e., $\mathbb{Z}/9\mathbb{Z} \rtimes_\phi \mathbb{Z}/2\mathbb{Z} \cong D_{18}$, the dihedral group of order 18.

$\text{Syl}_3(G) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$: Now we need to know the group homomorphisms $\phi : \mathbb{Z}/2\mathbb{Z} \to \text{Aut}(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z})$, i.e., we need to know the elements of order 2 in the group $\text{Aut}(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \cong GL_2(\mathbb{Z}/3\mathbb{Z})$, i.e., we need to know the two-by-two matrices $M$ with entries in $\mathbb{Z}/3\mathbb{Z}$ such that $M^2 = \text{id}$.

If two such matrices are conjugate, this corresponds to a change of basis in $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, i.e., this corresponds to making a different choice of generators for $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, which clearly does not change the semidirect product $(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \rtimes_\phi \mathbb{Z}/2\mathbb{Z}$, up to isomorphism; so now we just need to know the conjugacy classes of two-by-two matrices $M$ with entries in $\mathbb{Z}/3\mathbb{Z}$ such that $M^2 = \text{id}$.

You can compute this by brute force, or save yourself some effort by remembering some methods from linear algebra: rational canonical form is one way to do it. Every square matrix over a field is conjugate to a unique matrix in rational canonical form, and a two-by-two matrix $M$ with two blocks in its rational canonical form is simply a diagonalizable matrix, while a matrix $M$ with one block in its rational canonical form is a two-by-two companion.
matrix, i.e., $M$ is of the form
\[
\begin{bmatrix}
0 & a \\
1 & 0
\end{bmatrix}
\]
for some $a \in \mathbb{Z}/3\mathbb{Z}$; but the requirement that $M^2 = \text{id}$ immediately implies that $a = 1$.

**If $M$ is diagonalizable:** Then
\[
M = \begin{bmatrix}
a & 0 \\
0 & b
\end{bmatrix}
\]
where $a, b \in \{1, -1\} \subseteq \mathbb{Z}/3\mathbb{Z}$. If $M = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, then
\[
(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \rtimes_\varphi \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},
\]
and if $M = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ or $M = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$, then
\[
(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \rtimes_\varphi \mathbb{Z}/2\mathbb{Z} \cong \langle \sigma, \tau, \upsilon \mid \sigma^2, \tau^3, \upsilon^3, \tau\upsilon = \upsilon\tau, \sigma^{-1}\tau\sigma = \tau, \sigma^{-1}\upsilon\sigma = \upsilon^2 \rangle
\]
\[
\cong \mathbb{Z}/3\mathbb{Z} \times D_6.
\]

**If $M$ is not diagonalizable:** Then $M = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$, and
\[
(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \rtimes_\varphi \mathbb{Z}/2\mathbb{Z} \cong \langle \sigma, \tau, \upsilon \mid \sigma^2, \tau^3, \upsilon^3, \tau\upsilon = \upsilon\tau, \sigma^{-1}\tau\sigma = \tau^2, \sigma^{-1}\upsilon\sigma = \upsilon^2 \rangle.
\]

So there are at most six isomorphism classes of groups of order 18:
\[
\mathbb{Z}/18\mathbb{Z},
\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},
D_{18},
D_6 \times \mathbb{Z}/3\mathbb{Z},
G_1 = \langle \sigma, \tau, \upsilon \mid \sigma^2, \tau^3, \upsilon^3, \tau\upsilon = \upsilon\tau, \sigma^{-1}\tau\sigma = \tau^2, \sigma^{-1}\upsilon\sigma = \upsilon^2 \rangle,
G_2 = \langle \sigma, \tau, \upsilon \mid \sigma^2, \tau^3, \upsilon^3, \tau\upsilon = \upsilon\tau, \sigma^{-1}\tau\sigma = \upsilon, \sigma^{-1}\upsilon\sigma = \tau \rangle.
\]
Fourth part: checking which groups are isomorphic to others on our list: Clearly \(\mathbb{Z}/18\mathbb{Z}\) and \(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\) are the only two abelian groups on our list of six groups of order 18, and clearly these two abelian groups are not isomorphic to one another (\(\mathbb{Z}/18\mathbb{Z}\) contains an element of order 18, while \(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\) does not). So neither of those two abelian groups are secretly isomorphic to some other groups on the list of six.

On the other hand, take a look at the group \(G_2\): it has the same number of 2-Sylow subgroups (three of them) as \(D_6 \times \mathbb{Z}/3\mathbb{Z}\). This should make you suspicious (although it doesn’t mean for sure that the groups are isomorphic). In fact, if you go looking for an isomorphism between them, you find one: the homomorphism

\[
G_2 = \langle \sigma, \tau, \upsilon \mid \sigma^2, \tau^3, \upsilon^3, \tau \upsilon = \upsilon \sigma, \sigma^{-1} \tau = \tau \sigma \rangle \to \langle x, y, z \mid x^2, y^3, z^3, xy = yx, x^{-1}y = y^3, x^{-1}x = z \rangle = D_6 \times \mathbb{Z}/3\mathbb{Z}
\]

given by \(f(\sigma) = x\) and \(f(\tau) = yz\) and \(f(\upsilon) = y^2z\) (you can easily check that this indeed defines a group homomorphism) has an inverse group homomorphism \(g : D_6 \times \mathbb{Z}/3\mathbb{Z} \to G_2\) given by letting \(g(x) = \sigma\) and \(g(y) = \tau^2\upsilon\) and \(g(z) = \tau^2\upsilon^2\). Hence \(f\) is an isomorphism of groups.

With more effort (by counting 2-Sylow subgroups, for example) you can check that there are no further isomorphisms between the five groups

\[
\mathbb{Z}/18\mathbb{Z}, \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, D_{18}, D_6 \times \mathbb{Z}/3\mathbb{Z}, G_1.
\]

So there are five isomorphism classes of groups of order 18. \(\square\)