Solution 1:

By the first homomorphism theorem we know that

$$R \cong \tfrac{\mathbb{Z}}{\ker f}.$$

Recall $\ker f$ is an ideal in $\mathbb{Z}$. Since $\mathbb{Z}$ is a PID we see that $\ker f = (n)$ for some integer n.

Case 1: Suppose $n = 0$.

This implies

$$R \cong \tfrac{\mathbb{Z}}{\{0\}} \cong \mathbb{Z}.$$

Case 2: Suppose $n \neq 0$.

Then $(n) = n\mathbb{Z}$. Thus

$$R \cong \tfrac{\mathbb{Z}}{(n)} = \tfrac{\mathbb{Z}}{n\mathbb{Z}}.$$

Solution 2:

The statement is false. Let $R = \mathbb{Q}[x]$ and $I = (x^2)$. Then R is a domain because $\mathbb{Q}$ is a field. (Actually all we need is that $\mathbb{Q}$ is a domain to conclude R is a domain.) However,

$$x \cdot x \equiv 0 \pmod{x^2}.$$

Thus x is a zero divisor in R/I, and hence R/I is not a domain.

Solution 3:

We will first consider the function $f_p : \mathbb{Z}[x] \to (\mathbb{Z}/p\mathbb{Z})[x]$ defined by

$$f_p\left(\sum_{n=0}^{\infty} a_n x^n\right) = \sum_{n=0}^{\infty} [a_n] x^n$$

where $[a_n]$ defines the residue class of a_n mod p.

We will first show that this is a ring homomorphism. Given

$$\sum_{n=0}^{\infty} a_n x^n \text{ and } \sum_{n=0}^{\infty} b_n x^n \in R,$$

then

$$\begin{aligned} f_p\left(\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n\right) &= f_p\left(\sum_{n=0}^{\infty} (a_n + b_n) x^n\right) \\ &= \sum_{n=0}^{\infty} [a_n + b_n] x^n \\ &= \sum_{n=0}^{\infty} [a_n] x^n + \sum_{n=0}^{\infty} [a_n] x^n \\ &= f_p\left(\sum_{n=0}^{\infty} a_n x^n\right) + f_p\left(\sum_{n=0}^{\infty} b_n x^n\right) \end{aligned}$$

Thus f_p preserves addition.

As well,

$$\begin{aligned}
f_p\left(\left(\sum_{n=0}^{\infty} a_n x^n\right)\left(\sum_{n=0}^{\infty} b_n x^n\right)\right) &= f_p\left(\sum_{n=0}^{\infty}\left(\sum_{m=0}^{n} a_{n-m}b_m\right)x^n\right)\\
&= \left(\sum_{n=0}^{\infty}\left[\sum_{m=0}^{n} a_{n-m}b_m\right]x^n\right)\\
&= \left(\sum_{n=0}^{\infty}\left(\sum_{m=0}^{n} [a_{n-m}][b_m]\right)x^n\right)\\
&= \left(\sum_{n=0}^{\infty}[a_n]x^n\right)\left(\sum_{n=0}^{\infty}[b_n]x^n\right)\\
&= f_p\left(\sum_{n=0}^{\infty} a_n x^n\right)\cdot f_p\left(\sum_{n=0}^{\infty} b_n x^n\right)
\end{aligned}$$

This proves f_p preserves multiplication. Clearly $f_p(1) = 1$. Therefore f_p is is a ring homomorphism. It is clear that it is surjective.

Next consider the quotient map

$$q_p : \mathbb{Z}/p\mathbb{Z}\,[x] \to (\mathbb{Z}/p\mathbb{Z}\,[x])/(x^2+1)$$

defined by

$$q_p(a(x)) = a(x) + (x^2+1).$$

The quotient map is always surjective. Therefore the composition $q_p \circ f_p : \mathbb{Z}[x] \to (\mathbb{Z}/p\mathbb{Z}\,[x])/(x^2+1)$ is surjective.

We would like to show the kernel of $q_p \circ f_p$ is (p, x^2+1). First we will show $(p, x^2+1) \subset \ker q_p \circ f_p$. Choose an element $a(x)p + b(x)(x^2+1) \in (p, x^2+1)$. Then

$$\begin{aligned}
(q_p \circ f_p)(a(x)p + b(x)(x^2+1)) &= (q_p \circ f_p)(a(x)p) + (q_p \circ f_p)(b(x)(x^2+1))\\
&= q_p(0) + ((q_p \circ f_p)(b(x)))((q_p \circ f_p)(x^2+1))\\
&= 0 + ((q_p \circ f_p)(b(x)))(q_p(x^2+1))\\
&= ((q_p \circ f_p)(b(x)))0\\
&= 0.
\end{aligned}$$

Thus $(p, x^2+1) \subset \ker q_p \circ f_p$.

Next we will show $\ker q_p \circ f_p \subset (p, x^2+1)$. Suppose $s(x) \in \ker q_p \circ f_p$. By the division algorithm $s(x) = q(x)(x^2+1) + (ax+b)$ for some $a, b \in \mathbb{Z}$. As $q(x)(x^2+1) \in \ker q_p \circ f_p$ we find

$$ax + b = s(x) - q(x)(x^2+1) \in \ker q_p \circ f_p.$$

Thus

$$q_p \circ f_p(ax+b) = q_p([a]x + [b]) = 0.$$

However, as q_p is a quotient map this implies $[a]x + [b] \in (x^2+1)$. Hence $[a]x + [b] = 0$. Therefore $a \equiv 0 \pmod{p}$ and $b \equiv 0 \pmod{p}$. Therefore $ax + b \in (p, x^2+1)$. This proves $\ker q_p \circ f_p \subset (p, x^2+1)$.

By the first isomorphism theorem this proves

$$R/\ker q_p \circ f_p = R/I \cong (\mathbb{Z}/p\mathbb{Z}\,[x])/(x^2+1).$$

Next notice that by the division algorithm every coset in $(\mathbb{Z}/p\mathbb{Z}\,[x])/(x^2+1)$ can be written uniquely in the form $ax + b$ for some $a, b \in \mathbb{Z}/p\mathbb{Z}$. Therefore there are p^2 elements in $(\mathbb{Z}/p\mathbb{Z}\,[x])/(x^2+1)$.

Suppose $p = 5$. Then there is an isomorphism $h : (\mathbb{Z}/5\mathbb{Z}\,[x])/(x^2+1) \to \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ given by

$$h(a(x)) = (a(2), a(3)).$$

We know that the evaluation maps are homomorphism, thus h is a homomorphism. It remains to show that this is a bijection. However, since these are both finite sets with 25 elements it suffices to show that it is an injective function. Suppose $h(ax+b) = (0,0)$ then $2a+b = 3a+b = 0$. This implies $a = b = 0$, and hence $ax+b = 0$. This prove h is injective, and hence an isomorphism.

Therefore

$$R/I \cong (\mathbb{Z}/5\mathbb{Z}\,[x])/(x^2+1) \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$

Suppose $p = 7$. Notice (x^2+1) does not have any roots in $\mathbb{Z}/7\mathbb{Z}$ we see that (x^2+1) is irreducible. Since (x^2+1) is irreducible we will show $(\mathbb{Z}/7\mathbb{Z}\,[x])/(x^2+1)$ is a field with 49 elements.

Notice that it is a commutative ring since $\mathbb{Z}/7\mathbb{Z}\,[x]$ is a commutative ring. It remains to show that every element is invertible. Choose $ax+b \in (\mathbb{Z}/7\mathbb{Z}\,[x])/(x^2+1)$ where $ax+b \neq 0$. By the Euclidean algorithm there exist polynomials $a(x)$ and $b(x) \in (\mathbb{Z}/7\mathbb{Z}\,[x])$ such that

$$a(x)(ax+b) + b(x)(x^2+1) = 1.$$

Thus

$$a(x)(ax+b) \equiv 1 \pmod{(x^2+1)}.$$

This proves $(ax+b)^{-1} = a(x)$. Hence every element is invertible. Therefore R/I is isomorphic to a field with $p^2 = 49$ elements.

<u>Solution 4:</u>

Consider the function $f : R \to F$ given by taking the constant term of the power series, that is,

$$f\left(\sum_{n=0}^{\infty} a_n x^n\right) = a_0.$$

<u>Step 1:</u> First we will show this is a ring homomorphism.
Given

$$\sum_{n=0}^{\infty} a_n x^n \text{ and } \sum_{n=0}^{\infty} b_n x^n \in R,$$

then

$$\begin{aligned} f\left(\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n\right) &= f\left(\sum_{n=0}^{\infty} (a_n+b_n) x^n\right) \\ &= a_0 + b_0 \\ &= f\left(\sum_{n=0}^{\infty} a_n x^n\right) + f\left(\sum_{n=0}^{\infty} b_n x^n\right) \end{aligned}$$

Thus f preserves addition.

$$\begin{aligned} f\left(\left(\sum_{n=0}^{\infty} a_n x^n\right)\left(\sum_{n=0}^{\infty} b_n x^n\right)\right) &= f\left(a_0b_0 + (a_1b_0 + a_0b_1)x + \ldots\right) \\ &= a_0b_0 \\ &= f\left(\sum_{n=0}^{\infty} a_n x^n\right) \cdot f\left(\sum_{n=0}^{\infty} b_n x^n\right) \end{aligned}$$

This proves f preserves multiplication. Clearly $f(1) = 1$. Therefore f is is a ring homomorphism.

<u>Step 2:</u> Next we will show that f is surjective.

Given $a \in F$, we see that $a \in R$. As $f(a) = a$ we have shown f is surjective.

<u>Step 3:</u> Now we will describe the kernel.

Notice that the kernel of f is the set of polynomials with no constant terms. These are exactly the elements in R which are a multiple of x. This implies $\ker f = (x)$.

Step 4: By the first isomorphism theorem for rings we find

$$R/\ker f = R/(x) \cong F.$$

Step 5: Now we will show that any element which does not belong to (x) is invertible.
Suppose $\sum_{n=0}^{\infty} a_n x^n \notin (x)$. This implies $a_0 \neq 0$.

We will now construct the inverse for this element. Let $b_0 = \frac{1}{a_0}$. Assume b_k is defined. As $a_0 \neq 0$ we can let

$$b_{k+1} = -\tfrac{b_0 a_{k+1} + \ldots + b_k a_1}{a_0}.$$

Multiplying the following power series we find

$$\begin{aligned}\left(\sum_{n=0}^{\infty} a_n x^n\right)\left(\sum_{n=0}^{\infty} b_n x^n\right) &= a_0 b_0 + \sum_{n=1}^{\infty} \left(a_{k+1} b_0 + \ldots + a_0 b_{k+1}\right) x^n \\ &= a_0 \tfrac{1}{a_0} + \sum_{n=1}^{\infty} \left(a_{k+1} b_0 + \ldots + -\tfrac{b_0 a_{k+1} + \ldots + b_k a_1}{a_0} a_0\right) x^n \\ &= 1.\end{aligned}$$

Thus each element which is not in (x) is invertible.

Step 6: We will now show that if J is a non-trivial ideal then $J \subset (x)$.

Suppose J is an ideal which is not contained in (x). Then by Step 5 we know that J contains an invertible element r. However, by the multiplicative property in the definition of an ideal $r^{-1} r = 1 \in J$. Once an ideal contains 1 it contains every element $s \in R$ since the multiplicative property in the definition of an ideal implies that $(sr^{-1})r = s \in J$. Thus J is the trivial ideal, i.e., $J = S$. Therefore if J is a non-trivial ideal then $J \subset (x)$.

Solution 5:

1. First we note that the operation is commutative; that is,

$$a * b = a + b - ab = b + a - ba = b * a.$$

2. Let $a, b \in F - \{1\}$. Clearly $a * b \in F$. Suppose $a * b = 1$. Then

$$a + b - ab = 1.$$

Taking all the terms to one side shows

$$0 = ab - a - b + 1.$$

Factoring this we find

$$0 = (a-1)(b-1).$$

However, $a \neq 1$ and $b \neq 1$. Hence $a * b \in F - \{1\}$. This shows $*$ is a binary operation.

3. First notice

$$\begin{aligned}(a * b) * c &= (a + b - ab) * c \\ &= (a + b - ab) + c - (a + b - ab)c \\ &= a + b - ab + c - ac - bc + abc \\ &= a + b + c - ab - ac - bc + abc.\end{aligned}$$

On the other hand,

$$\begin{aligned}a * (b * c) &= a * (b + c - bc) \\ &= a + (b + c - bc) - a(b + c - bc) \\ &= a + b + c - bc - ac - ab + abc.\end{aligned}$$

This proves $*$ is associative.

4. For $a \in G$ we see
$$a * 0 = a + 0 - 0 = a.$$
Therefore 0 satisfies the properties of the identity.

5. Notice
$$a * \left(\tfrac{1}{a-1}\right) = a + \tfrac{a}{a-1} - \tfrac{a^2}{a-1}.$$
Finding a common denominator we see that
$$a * \left(\tfrac{1}{a-1}\right) = \tfrac{(a^2-a)+a-a^2}{a-1} = 0.$$
Therefore $\left(\tfrac{a}{a-1}\right)$ is the inverse to a.

Since these four properties hold this is a group. It also happens to be an abelian group.

Solution 6:

There are $3! = 6$ bijective functions from $\{1,2,3\}$ to $\{1,2,3\}$. These elements of S_3 are listed below:
$$e, (12), (13), (23), (123) \text{ and } (132).$$
A cycle of length n has order n.
Thus e has order 1.
The elements $(12), (13)$ and (23) have order 2.
The elements (123) and (132) have order 3.

Solution 7:

Let $x, y \in G$. Then
$$x^2y^2 = 1 \cdot 1 = 1 = (xy)^2.$$
In other words,
$$xxyy = xyxy.$$
Taking inverses on either side we see that
$$x^{-1}xxyyy^{-1} = x^{-1}xyxyy^{-1}.$$
Canceling off implies $yx = xy$. As this holds for all $x, y \in G$, we conclude that G is abelian.

Let h be the set of 3×3 matrices with entries in $\mathbb{Z}/3\mathbb{Z}$, of the form
$$\left\{ \left(\begin{smallmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{smallmatrix}\right) a, b, c \in \mathbb{Z}/3\mathbb{Z} \right\}$$
Step 1: We will first show this is a subgroup of the group of invertible matrices $\mathrm{GL}_3(\mathbb{Z}/3\mathbb{Z})$. Notice
$$\begin{pmatrix} 1 & a_1 & b_1 \\ 0 & 1 & c_1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a_2 & b_2 \\ 0 & 1 & c_2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a_1 + a_2 & b_2 + a_1c_2 + b_1 \\ 0 & 1 & c_1 + c_2 \\ 0 & 0 & 1 \end{pmatrix}$$
This proves if $g_1, g_2 \in H$ then $g_1 \cdot g_2 \in H$.

From the previous formula we find
$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a-a & (-ac+b)+ac+b \\ 0 & 1 & c-c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$
Thus each element in H has an inverse in H.

Step 2: Next we can see that since there are 3 choices for each entry a, b and c, there are 27 elements in H. This shows that H has order 27.

Step 3: This group is non-abelian since $\left(\begin{smallmatrix}1&1&0\\0&1&0\\0&0&1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1&0&0\\0&1&1\\0&0&1\end{smallmatrix}\right) \in H$. If we multiply these elements we find

$$\begin{pmatrix}1&1&0\\0&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix}=\begin{pmatrix}1&1&1\\0&1&1\\0&0&1\end{pmatrix}$$

However, multiplying them in the opposite order gives us

$$\begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix}\begin{pmatrix}1&1&0\\0&1&0\\0&0&1\end{pmatrix}=\begin{pmatrix}1&1&0\\0&1&1\\0&0&1\end{pmatrix}$$

The top right-hand entry is different. Therefore this group is non-commutative.

Step 4: Finally we can see that each element g of H satisfies $G^3 = 1$.

$$\begin{aligned}\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix} &= \begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}\begin{pmatrix}1&2a&2b+ac\\0&1&2c\\0&0&1\end{pmatrix}\\ &= \begin{pmatrix}1&3a&2b+ac+2ac+b\\0&1&3c\\0&0&1\end{pmatrix}\\ &= \begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}\end{aligned}$$

Thus we have found a group with the required properties.

Solution 8:

Suppose $g, h \in H_1 \cap H_2$. As H_1 is a subgroup

$$g \cdot h \in H_1 \text{ and } g^{-1} \in H_1.$$

Similarly, as H_2 is a subgroup

$$g \cdot h \in H_2 \text{ and } g^{-1} \in H_2.$$

Thus

$$g \cdot h \in H_1 \cap H_2 \text{ and } g^{-1} \in H_1 \cap H_2.$$

This proves $H_1 \cap H_2$ is a group.

The union of two subgroups in not necessarily a subgroup. Consider the group $\mathbb{Z} \times \mathbb{Z}$ with componentwise addition as the group operation. Then $H_1 = \mathbb{Z} \times 0$ and $H_2 = 0 \times \mathbb{Z}$ are both subgroups. However, the union is not a subgroup. For example, $(1,0) \in H_1$ and $(0,1) \in H_2$, however,

$$(1,0) + (0,1) = (1,1) \notin H_1 \cup H_2.$$

This shows $H_1 \cup H_2$ is not closed under addition, and so is not a subgroup.

Solution 9:

Step 1: Consider the set

$$H = \{a^i \mid i \in \mathbb{Z}\}.$$

We begin by showing that $a^i = 1$ for some natural (finite) number i.

Since there are finitely many elements in G there are finitely many elements in H. Thus

$$a^i = a^j \text{ for some } i, j \in \mathbb{N} \text{ where } i \neq j.$$

Without loss of generality we can assume $i > j$. Multiplying both sides by a^{-j} we see that:

$$a^i a^{-j} = a^j a^{-j} = 1.$$

Thus $a^{i-j} = 1$, which shows that the order of a is at most $i - j$. Let $d \in \mathbb{N}$ be the order of a.

Step 2: We will now show that the cardinality of H is d.

The elements $a^i \neq a^j$ for $1 \leq j < i \leq d$, otherwise $a^{i-j} = 1$ which contradicts the definition of d. As well, the $a^m = a^r$ where $m \equiv r$ modulo d. Thus the only distinct elements in H are $a, a^2, \ldots, a^d$. This proves the cardinality of H is d.

Step 3: Next we show that H is a subgroup.

Given $a^i, a^j \in H$ we see that

$$a^i \cdot a^j = a^{i+j} \in H.$$

Thus H is closed under multiplication.

Now we must show that each element in H has an inverse in H. Notice that

$$a^m \cdot a^{dm-m} = (a^d)^m = 1.$$

This shows that a^{dm-m} is the inverse of a^m. Therefore H is a group.

Step 4: Finally we will show that $a^n = 1$.

Lagrange's Theorem states that the cardinality of a subgroup H divides the cardinality of the whole group G. Together with the result from Step 2 we find that $d \mid n$. Therefore $n = dk$ for some natural number k. This means

$$a^n = (a^d)^k = 1^k = 1.$$

Step 5: This allows us to prove Fermat's Little Theorem.

We know there are $p - 1$ elements in $(\mathbb{Z}/p\mathbb{Z})^\times$. Thus for $a \not\equiv 0 \pmod{p}$, we find

$$a^{p-1} \equiv 1 \pmod{p}.$$

Multiplying both sides by a proves

$$a^p \equiv a \pmod{p}.$$

Solution 10:

Suppose that $a, b \in Z(S)$. Then

$$as = sa \text{ for all } s \in S \text{ and}$$
$$bs = sb \text{ for all } s \in S.$$

This proves

$$abs = asb = sab \text{ for all } s \in S.$$

Therefore $ab \in Z(S)$.

Suppose $a \in Z(S)$. This implies

$$as = sa \text{ for all } s \in S.$$

Multiplying by a^{-1} on both sides gives us

$$a^{-1}asa^{-1} = a^{-1}saa^{-1} \text{ for all } s \in S.$$

Thus

$$sa^{-1} = a^{-1}s \text{ for all } s \in S.$$

This proves $a^{-1} \in Z(S)$. Therefore, $Z(S)$ is a subgroup.

Solution 11:

Consider the function $f : G_2 \to G_1$ defined by $f(x) = e^x$. This is a group homomorphism because

$$f(x + y) = e^{(x+y)} = e^x \cdot e^y = f(x) \cdot f(y).$$

Notice that $f^{-1}(x) = \ln x$. As f has a (two-sided) inverse function we see that f is bijective. This proves f is an isomorphism.

Solution 12:

We will assume the following facts:

1. Every element in S_n can be written as a product of 2-cycles. This follows from the following decomposition of a cycle into a product of 2-cycles:

$$(a_0 a_1 \dots a_n) = (a_0 a_n)(a_0 a_{n-1}) \dots (a_0 a_1).$$

2. The alternating group A_n, which is the set of elements which can be written as an even number of 2-cycles, is well-defined and a group.

3. The conjugacy class of an element is determined by its cycle decomposition.

Step 1: As conjugacy is an equivalence relation, conjugacy classes are equivalence classes. Therefore different conjugacy classes are disjoint.

Step 2: Next we will explain why any normal subgroup N is a union of disjoint conjugacy classes.

Suppose $a \in N$. By the definition of a normal subgroup $gag^{-1} \in N$ for all $g \in G$. This means that the entire conjugacy class of a is in N. Therefore N is a union of disjoint conjugacy classes.

Step 3: Next we will show the converse holds. We will show that a subgroup which is a disjoint union of conjugacy classes is normal.

Suppose N subgroup which is a disjoint union of conjugacy classes. Let $n \in N$ and $g \in G$. Then gng^{-1} is a conjugate of an element in N hence it is in N by our assumption on N. Thus $gNg^{-1} \in N$ for every element $g \in G$. This shows N is a normal subgroup.

Step 4: Next we will describe the conjugacy classes of S_4.

As conjugacy classes are determined by their cycle decomposition, the following elements are representatives for the 5 conjugacy classes of S_4:

$$e, (12), (123), (12)(34), (1234).$$

Step 5: Now we will find the normal subgroups of S_4.

We claim the normal subgroups are the following:

1. The trivial subgroup $\{e\}$ and G are always normal subgroups.

2. The set $V = \{e, (12)(34), (13)(24), (14)(23)\}$ is a subgroup. It is closed under taking inverses because each element is its own inverse.

   Next we will show that V is closed under multiplication. Let $a, b \in V$. If a or b is the identity then clearly $ab \in V$. If $a = b$ then $ab = e$ as each element is its own inverse. Multiplying two distinct non-identity elements gives you the third non-identity element (i.e., $((12)(34))((13)(24)) = (14)(23)$). Therefore V is closed under multiplication.

   Finally by Step 3 we know V is normal.

3. Finally A_4, the set of elements which are a product of an even number of transpositions (2-cycles), is a subgroup of S_4. It is made up of the identity and the elements which have a cycle decomposition which is a 3-cycle or 2 disjoint 2-cycles. Thus it is a union of disjoint cycles. By Step 3 this proves A_4 is normal.

Next we will show these are the only possibilities. In particular, we will show that if N is a normal subgroup, since it a union of conjugacy classes which is closed under multiplication, thus it will be one of the 4 subgroups listed above.

Case a: Suppose N is a normal subgroup which contains a transposition. By Step 2 this implies N contains all the transposition. However, all the elements of G can be written as a product of transpositions. In order for N to be closed under its operation this means $N = G$.

Case b: Suppose N is a normal subgroup which contains 4-cycle. By Step 2 this implies N contains all the 4-cycles. Thus N contains the following product of 4-cycles:

$$(1243)(1234)(1243) = (1243)(132) = (34) \in N.$$

Thus N contains a transposition. By Case a this implies $N = G$.

Case c: Suppose N contains an element which is a 3-cycles and no 4-cycles or transpositions. Then by Step 2 this implies N contains all the elements which are 3-cycles. Thus N contains the following product of 3-cycles:

$$(123)(124) = (13)(24) \in N.$$

By Step 2 this means N contains all the elements which are the product of 2 disjoint 2-cycles. Therefore N is A_4.

Step 6: Next we will describe the conjugacy classes of S_5.

As conjugacy classes are determined by their cycle decomposition, the following elements are representatives for the 7 conjugacy classes of S_5:

$$e, (12), (123), (12)(34), (1234), (12)(345), (12345).$$

Step 7: Now we will find the normal subgroups of S_5.

1. The trivial subgroup $\{e\}$ and G are always normal subgroups.
2. Again A_5, the set of elements which are a product of an even number of transpositions, is a subgroup of S_5. It is made up of the identity and the elements which have a cycle decomposition which is a 3-cycle, a 5-cycle or 2 disjoint 2-cycles. Thus it is a union of disjoint cycles. By Step 3 this proves A_5 is normal.

Next we will show these are the only possibilities. In particular, we will show that if N is a normal subgroup, since it a union of conjugacy classes which is closed under multiplication, thus it will be one of the 3 subgroups listed above.

Case a: For the same reason as in Case a of the S_4 situation, if N is a normal subgroup which contains a transposition then $N = G$.

Case b: For the same reason as in Case b of the S_4 situation if N is a normal subgroup which contains a 4-cycle then $N = G$.

Case c: Suppose N is a normal group which contains an element which is a disjoint product of a 2-cycle and a 3-cycles. By Step 2 this means N contains (12)(345). Hence

$$((12)(345))^3 = (12)^3(345)^3 = (12) \in N.$$

Thus by Case a $N = G$.

Case d: Suppose N is a normal subgroup G which is contained in A_5. We will show that if N contains any element which is not the identity then $N = A_5$. We will do this by noticing the following:

1. If N contains all the 3-cycles then
$$(123)(345) = (12345) \in N.$$
This means N contains all the 5-cycles.
2. If N contains all the 5-cycles then
$$(12345)(12354) = (13)(24).$$
Thus N contains all the elements which are a product of 2 disjoint 2-cycles.
3. If N contains all the elements which are a product of 2 disjoint 2-cycles then
$$((12)(34))((34)(25)) = (125).$$
Thus N contains all the 3-cycles.

Therefore if N contains any element of A_5 which is not the identity $N = A_5$.