1. (15 points) Consider the group $G = \mathbb{Z}_9 \times \mathbb{Z}_{25}$. Find an element $(a, b) \in G$ whose order is 15. Justify your answer.

$G$ is abelian. So the order of $(a, b)$ is the smallest positive integer $m$ such that:

$$m \cdot (a, b) = (a, b) + \ldots + (a, b) = (0, 0)$$

Note: observe that the element $(3, 5) \in \mathbb{Z}_9 \times \mathbb{Z}_{25}$ satisfies:

$$15 \cdot (3, 5) = (46, 75) = (0, 0)$$

so $(3, 5)$ has order a divisor of 15. But the divisors of 15 are 1, 3, 5, 15 and:

$$1 \cdot (3, 5) = (3, 5) \neq (0, 0)$$

$$3 \cdot (3, 5) = (9, 15) = (0, 15) \neq (0, 0)$$

$$6 \cdot (3, 5) = (18, 30) = (0, 0)$$

So $(3, 5)$ has order 15.
2. (15 points) Consider the system of equations:

\[
\begin{align*}
5x & \equiv 3 \pmod{7} \\
2x & \equiv 12 \pmod{7}
\end{align*}
\]

Does it have solutions? If not, explain why. If yes, determine all the solutions.

Note that 5 has inverse 3 in \( \mathbb{Z}_7 \) since

\[5 \cdot 3 = 15 \equiv 1 \pmod{7}\]

and 2 has inverse 4 in \( \mathbb{Z}_7 \) since

\[2 \cdot 4 = 8 \equiv 1 \pmod{7}\]

Hence:

\[
\begin{align*}
5x & \equiv 3 \pmod{7} \\
2x & \equiv 12 \pmod{7}
\end{align*}
\]

\[\equiv \begin{cases}
3-5x & \equiv 3-3 \pmod{7} \\
4-2x & \equiv 4-12 \pmod{7}
\end{cases}
\]

\[\equiv \begin{cases}
x & \equiv 2 \pmod{7} \\
x & \equiv 6 \pmod{7}
\end{cases}
\]

Impossible, since congruence classes are disjoint.

No solutions!
3. (15 points) Let $D_6$ be the dihedral group (the group of symmetries of a regular hexagon), with generators $\sigma$ (reflection along a line of symmetry) and $r$ (rotation by $2\pi/6$). Show that $D_6$ has a normal subgroup isomorphic to $S_3$.

We know:  
\[
D_6 = \{e, r, r^2, \ldots, r^5, \sigma, r\sigma, \ldots, r^5\sigma\} \cong \left\{ e^2, e^3 \right\} \cong S_3
\]

This is the group of symmetries of a regular hexagon:

Consider the symmetries that preserve an isosceles triangle:

\[H = \{e, r^2, r^4, \sigma, r^2\sigma, r^4\sigma\} \subset D_6\]

This is a subgroup isomorphic to $D_3 = \{e, r, r^2, s, sr, sr^2\}$:

\[
\phi : H \to D_3 : \phi(e) = e, \phi(r^2) = r, \phi(r^4) = r^2 \\
\phi(\sigma) = s, \phi(r^2\sigma) = sr, \phi(r^4\sigma) = sr^2
\]

Finally, observe that $D_3$ and $S_3$ are both the group of symmetries of a triangle. An isomorphism is given by:

\[
\begin{align*}
R & \to (123) \\
R^2 & \to (12) \\
SR & \to (12)(123) = (23) \\
SR^2 & \to (12)(321) = (13)
\end{align*}
\]
4. (15 points) Let \( G \) a group and denote by \( Z(G) \) its center: 
\[
Z(G) = \{ z \in G : zg = gz, \forall g \in G \}.
\]

(a) Show that \( Z(G) \) is an abelian;
(b) Is \( Z(G) \) a normal subgroup? Justify your answer.

\[(a) \ Z(G) \text{ is abelian subgroup: } \]
\[
2_1 2_2 \in Z(G) \Rightarrow 2_1 2_2 g = 2_1 g 2_2 = g 2_1 2_2, \ \forall g \in G
\]
\[
\Rightarrow 2_1 2_2 \in Z(G)
\]
\[
2 \in Z(G) \Rightarrow 2g = g2, \ \forall g \in G
\]
\[
\Rightarrow g^2 = 2^2 g, \ \forall g \in G
\]
\[
\Rightarrow 2^1 \in Z(G)
\]

Hence, \( Z(G) \) is a subgroup. By definition, \( 2_1 2_2 = 2_2 2_1 \) for all \( 2_1, 2_2 \in Z(G) \), so it is abelian.

\[(b) \text{ Note that } \]
\[
2 \in Z(G) \Rightarrow g2^1 = g22 = 2, \ \forall g \in G
\]
So we have:
\[
g2(2)2^1 = 2(2), \ \forall g \in G
\]

which means that \( Z(G) \) is a normal subgroup of \( G \).
5. (10 points) How many distinct words can one form with the letters of the word ILLINI?

Consider the action on $S_6$ on the set $X$ of words formed with the letters $I, I, I, L, L, N$. This action is transitive, hence:

$$\#\text{words} = \frac{|S_6|}{|S_{\text{stab}(w)}|}$$

where $w$ is any word. Taking $w = \text{ILLINI}$ we see that:

$$|S_{\text{stab}(w)}| = 5 \times 4 \times 3 = 60$$

Therefore:

$$\#\text{words} = \frac{|S_6|}{12} = 5 \times 4 \times 3 = 60$$
6. (10 points) Let $D$ be an integral domain. Show that if $d \in D$ is a prime element then it is irreducible.

Recall that for $d \neq 0$, but a unit:
- $d$ prime $\iff (d|ab \Rightarrow d|a \text{ or } d|b)$
- $d$ irreducible $\iff (d = ab \Rightarrow a \text{ is unit or } b \text{ is unit})$

So assume $d$ is a prime. If $d|ab$ then $d|a$ and $d|b$ so either $d|a$ or $d|b$. Now:
- if $d|a$ $\Rightarrow a = kd$ then $d = ab = kdb$ so $1 = kb$ $\Rightarrow b$ is unit.
- if $d|b$ $\Rightarrow b = sd$ then $d = ab = sad$ so $1 = sa$ $\Rightarrow a$ is unit.

Hence, either $a$ is a unit or $b$ is a unit, so $d$ is irreducible.
7. (10 points) Let \( \mathbb{R}[x] \) be the ring of polynomials with real coefficients and consider the ideal \( I = \langle x^2 + 1 \rangle \subset \mathbb{R}[x] \).

(i) Is \( I \) a maximal ideal?

(ii) Is \( I \) a prime ideal?

Justify your answer.

**Hint:** The ring homomorphism \( \phi: \mathbb{R}[x] \to \mathbb{C}, \ p \mapsto p(i) \), has kernel \( I = \langle x^2 + 1 \rangle \).

Using the hint, observe that \( \phi \) is surjective: if \( z = a + bi \) then taking \( p(x) = ax + b \) we have \( \phi(p) = z \). Hence, by the isomorphism theorem for rings, we have

\[
\begin{array}{ccc}
\mathbb{R}[x] & \xrightarrow{\phi} & \mathbb{C} \\
\downarrow & & \downarrow \phi \\
\mathbb{R}[x]/ \langle x^2 + 1 \rangle & \xrightarrow{\phi} & \mathbb{C}
\end{array}
\]

so \( \mathbb{R}[x]/ \langle x^2 + 1 \rangle \) is a field. Hence, \( I = \langle x^2 + 1 \rangle \) is a maximal ideal.

Every maximal ideal is prime, so \( I \) is also a prime ideal.
8. (10 points) Let $(D, +, \cdot)$ be an integral domain. Which of the following statements are true:
   (a) If $D$ is a UFD then $D$ is a PID.
   (b) If $D$ is a PID then $D[x]$ is a UFD.
   (c) If $D$ is a UFD then $D[x]$ is a PID.
   (d) $D$ is a subring of a field $K$.
   Justify your answer by quoting some result or by giving a counterexample.

(a) **False**: $\mathbb{Z}[x]$ is a UFD but not a PID
(b) **True**: If $D$ is a PID then $D$ is a UFD. By a Thm it follows that $D[x]$ is a UFD
(c) **False**: $\mathbb{Z}$ is a UFD but $\mathbb{Z}[x]$ is not a PID
(d) **True**: Take $K = \text{Frac}(D)$ to be the ring of fractions of $D$. It is a field and $D \subseteq \text{Frac}(D)$. 
9. (Extra Credit: 10 points) Let \( p \in \mathbb{N} \) be a prime number. Show that \( p \) is a prime element in \( \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} \) if and only if the equation
\[
p = n^2 + m^2
\]
has no integer solutions \( n, m \in \mathbb{Z} \). Is the number \( 5 \in \mathbb{Z}[i] \) a prime?

**Hint:** \( \mathbb{Z}[i] \) is a UFD.

If \( p \in \mathbb{Z}[i] \) prime \( \Rightarrow \) \( p \) is not a prime

Assume \( p \) is a prime. Then
\[
(n - im)(n - im) = n^2 + m^2 - p
\]
is a factorization of \( p \). Moreover, since the units of \( \mathbb{Z}[i] \) are \( \pm 1, \pm i, \pm \bar{i} \), we have that \( n + im \) are not units. So this shows that \( p \) is not irreducible.

Since \( \mathbb{Z}[i] \) is a UFD, it follows that \( p \) is not a prime.

\( 5 \) is not a prime in \( \mathbb{Z}[i] \) because:

\[
5 = (1 + 2i)(1 - 2i), \quad 1 \pm 2i \text{ are not units.}
\]