1. (**3 pts. each**) Let H be a subgroup of a group G. For any $a, b \in G$,

(a) Show that $\sim$ is an equivalence relation on G, where $\sim$ is defined on G by $a \sim b$ iff $a^{-1}b \in H$.

(b) Show that it is either $aH = bH$ or $aH \cap bH = \phi$.

Solution:

(a) We show that $\sim$ is reflexive, symmetric and transitive:

- Reflexive: If $a \in G$, then $a \sim a$ because $a^{-1}\, a = e \in H$.
- Symmetric: If $a \sim b$, then $a^{-1}b \in H$ and so is $(a^{-1}b)^{-1} = b^{-1}a \in H$ because H contains the inverse of any of its elements. Thus $b \sim a$.
- Transitive: If $a \sim b$ and $b \sim c$, then $a^{-1}b, b^{-1}c \in H$. Since H is a subgroup of G, it contains the product of $a^{-1}b$ and $b^{-1}c$. Thus, $a^{-1}b \cdot b^{-1}c = a^{-1}c \in H$. Hence $a \sim c$.

Therefore, $\sim$ is an equivalence relation on G.

(b) Assume that there is $x \in aH \cap bH$, then $x \in aH$ and $x \in bH$. That is $ah_1 = x = bh_2$ and hence $bh_2 \in aH$ and $ah_1 \in bH$ which implies that $aH = bH$. Otherwise, there is no $x \in aH \cap bH$ and hence $aH \cap bH = \phi$.

2. (**3 pts. each**) Let p be a prime number.

(a) Show that $(\mathbb{Z}_p^*, \odot)$ is an abelian group.

(b) Show that if G is a group of order p^2, then G has at least one subgroup of order p.

Solution:

(a) i. Let $[a], [b] \in \mathbb{Z}_p^*$, then $[a] \odot [b] = [ab] \in \mathbb{Z}_p^*$ since $[ab] \neq [p]$.

ii. Clearly, $[1] \in \mathbb{Z}_p^*$ (the identity is in $\mathbb{Z}_p^*$).

iii. Let $[a] \in \mathbb{Z}_p^*$, then (the greatest common divisor of a and p) $GCD(a, p) = 1$ which implies

$$\exists\, b, c \in \mathbb{Z} \text{ such that } ab + pc = 1 \Rightarrow ab = 1 - pc \Rightarrow ab = 1 \,(\text{mod } p) \Rightarrow [b] = [a]^{-1} \in \mathbb{Z}_p^*.$$

(b) Note that $p > 1$ which implies that there is $a \in G$ (not equal e) with $o(a) | p^2$ (by Lagrange's Theorem). That is $o(a)$ is either p or p^2. If $o(a) = p$, then $\langle\, a \,\rangle$ is a subgroup of order p and we are done.

Otherwise, $o(a) = p^2$. Then, by Fundamental Theorem of Finite Cyclic Groups we have $o(a^p) = \dfrac{p^2}{gcd(p, p^2)} = \dfrac{p^2}{p} = p$. Therefore, $\langle\, a^p \,\rangle$ is a subgroup of order p.

3. (**3+1+2+2 pts.**) Let $\mathbb{U}_n = \{\, [k] : 1 \leq k < n \text{ and } GCD(k,n) = 1 \,\}$.

(a) Use the Euclidean algorithm to find the inverse of [21] in $\mathbb{U}_{220}$.

(b) Does [14] belong to $\mathbb{U}_{220}$? Explain.

(c) What is the order of [21] in $\mathbb{U}_{220}$? Explain.

(d) Find the order of $\mathbb{U}_{220}$.

Solution:

(a) We use Euclid's Algorithm to find 21^{-1} in $\mathbb{U}_{220}$:

$$220 = 21 \cdot 10 + 10$$
$$21 = 10 \cdot 2 + 1$$
$$10 = 1 \cdot 10 + 0$$

Therefore, $GCD(21, 220) = 1$. Hence,

$$1 = \cdots = (21)(21) + (220)(-2).$$

Therefore, $21^{-1} = 21$.

(b) No. Since 2 divides both 14 and 220. That is, $GCD(14, 220) \neq 1$.

(c) Note that $(21)(21) = 1 + (2)(220)$. That is, $(21)^2 \cong 1 \mod 220$. Hence $o(21) = 2$ in $\mathbb{U}_{220}$.

(d) Note that $220 = 2^2 \cdot 5 \cdot 11$. Therefore,

$$\phi(220) = 220 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) \cdot \left(1 - \frac{1}{11}\right) = 220 \cdot \left(\frac{1}{2}\right) \cdot \left(\frac{4}{5}\right) \cdot \left(\frac{10}{11}\right) = 80.$$

4. (**3 pts. each**)

(a) Compute all distinct left cosets of $H = \langle\, (1\ \ 2\ \ 3)\,\rangle \times \langle\, [1]\,\rangle$ in $S_3 \times Z_2$.

(b) If H is a subgroup of index 2 of a group G, then show that for any $a \in G$, we have $a^{-1}Ha = H$.

Solution: Note that $|\,G\,| = 12$.

(a) Note that $H = \{\,(e,0\,),(\,e,1\,),(\,(1\ \ 2\ \ 3),0\,),(\,(1\ \ 2\ \ 3),1\,),(\,(1\ \ 3\ \ 2),0\,),(\,(1\ \ 3\ \ 2),1\,)\,\}$. Therefore, $(e,0)H = H$ and $((1\ \ 2),0)H$ are all left cosets of H in $S_3 \times Z_2$, where

$$((1\ \ 2),0)H = \{\,(\,(1\ \ 2),0\,),(\,(1\ \ 2),1\,),(\,(2\ \ 3),0\,),(\,(2\ \ 3),1\,),(\,(1\ \ 3),0\,),(\,(1\ \ 3),1\,)\,\}.$$

(b) Note that $G = H \cup aH = H \cup Ha$ since $[G : H] = 2$. That is $aH = Ha$ for any $a \in G$. Hence $a^{-1}Ha = H$.