

Final

The grader cannot be expected to work his way through a sprawling mess of identities presented without a coherent narrative through line. If he can't make sense of it in finite time you could lose coherent narrative through line. If he can't make sense of it in finite time you could lose serious points. Coherent, readable exposition of your work is half the job in mathematics.

Problem 1 :

Let G be a finite group of order $|G| = p^2$ for some prime $p > 1$.

1. (3pts) Explain why there must exist cyclic subgroups of order p in G .
2. (3pts) Explain why all such subgroups must be normal in G .
3. (6pts) Deduce from the previous question, prove that $G \simeq \mathbb{Z}/p^2\mathbb{Z}$ or $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Hint : The Sylow theorems will not help. (Why?).

Solution :

1. Cauchy's theorem says : p a prime divisor of $n \geq |G|$ implies there is $a \in G$ such that $o(a) = p$.
2. Cauchy's 2nd theorem says : if $p^2 = |G|$ for some prime p then G is abelian. Hence all subgroups in G are normal.
3. Look at $x \in G$ with maximal possible order (either p or p^2). If there is x such that $o(x) = p^2$ then $\langle x \rangle = G$ and $G \simeq (\mathbb{Z}/p^2\mathbb{Z}, +)$. Otherwise $\max\{o(x)\} = p$ and $x^p = e$ for all $p \neq e$. Take $a \neq e$ and form $A = \langle a \rangle \simeq \mathbb{Z}/p\mathbb{Z}$. There must be some $b \notin A$; Then $B = \langle b \rangle \simeq \mathbb{Z}/p\mathbb{Z}$. There must be some $b \notin A$; Then $B = \langle b \rangle \simeq \mathbb{Z}/p\mathbb{Z}$, $B \neq A$ since $b \notin A$ since $b \notin A$, and $B \cap A = \{e\}$ by Lagrange. Then,

$$|BA| = |B| \cdot |A|/|A \cap B| = p^2$$

so $AB = G$ and since A is normal in G and B is normal in G , we have $G = A \times B$ (internal direct product) and

$$G \simeq \mathbb{Z}/p \times \mathbb{Z}/p\mathbb{Z}$$

Problem 2 :

Let $n = p^k$ for some prime $p > 1$ and $k \geq 1$. If $m \in \mathbb{N}$,

1. (4pts) Prove that $\gcd(m, p^k) \neq 1 \Leftrightarrow p$ divides m Thus

$$U_{p^k} = \{[m] : 0 \leq m \leq p^k \text{ and } m \text{ is not a multiple of } p\}$$

2. (5pts) Prove that the group of units in $\mathbb{Z}/p^k\mathbb{Z}$ has order

$$|U_{p^k}| = p^{k-1}(p-1) \text{ for all } k \geq 1$$

3. (5pts) Deduce from the previous question the cardinality $|U_{37}|$ and $|U_{120}|$. (Hint : This can be answered without exhaustively listing the element in U_n .)

Solution :

1. Let $c = \gcd(m, p^k)$ and show that $c > 1$ if and only if p divides m .
 \Leftarrow If $p|m$ then $p|p^k$ automatically so $p|\gcd > 1$.
 \Rightarrow If $\gcd = c > 1$. Then $c|m$ and $c|p^k$. By unique factorization, there is a such that $p^k = a \cdot c$ and a, c can only be powers of p . Thus, since $c > 0$, $c = p^r$ for some $r > 0$. Thus $p|c$ and $c|m$ which implies $p|m$ as claimed.

2. $|\mathbb{Z}/p^k\mathbb{Z}| = p^k$ and

$$|\{x \in \mathbb{Z}/p^k\mathbb{Z} : x \neq 0\}| = p^k - 1$$

$U_{n,k}$ lies in this set. By (a),

$$\{[m] \in \mathbb{Z}/p^k\mathbb{Z} : 1 \leq m \leq p^k - 1 \text{ and } m \text{ is not a multiple of } p\}$$

But the multiples of p in $[1, p^k - 1]$ are $p, 2p, \dots, rp, \dots, p^k - p$ and there are $p^{k-1} - 1$ such values of m . Thus

$$\begin{aligned} |U_{p^k}| &= (p^k - 1) - \#\{1 \leq m \leq p^k - 1 : m \text{ a multiple of } p\} \\ &= (p^k - 1) - (p^{k-1} - 1) = p^k - p^{k-1} = p^{k-1}(p - 1) \end{aligned}$$

3. For $|U_{37}|$, note that p is prime and we mentioned that $|U_p| = |\{x \in \mathbb{Z}/p\mathbb{Z} : x \neq 0\}| = p - 1$, so $|U_{37}| = 36$ without appeal to any formulas.
For $n = 120 = 8 \cdot 15 = 2^3 \cdot 3 \cdot 5$, we know $U_{120} \simeq U_8 \times U_3 \times U_5$, so $|U_{120}| = |U_8| \cdot |U_3| \cdot |U_5| = |U_8| \cdot 2 \cdot 4$. But by the previous question, $|U_{2^3}| = 2^{3-1} \cdot (2 - 1) = 4$, so $|U_{120}| = 4 \cdot 2 \cdot 4 = 32$.

Problem 3 :

Let $G = (U_{11}, \cdot)$ be the multiplicative group of units in $\mathbb{Z}/11\mathbb{Z}$. Make a table in which you list the orders of all elements $x \in U_{11}$ and the subgroups $H = \langle x \rangle$ they generate. Use this to answer the following questions.

1. (3pts) How many distinct cyclic subgroups are there in G ? Is G itself cyclic?
2. (3pts) How many distinct 5-Sylow subgroups are there in G ? Describe them as subsets of G . Do the same for the 2-Sylow subgroups.
3. (4pts) When $n = 5$, how many distinct homomorphisms $\Phi : (\mathbb{Z}/5\mathbb{Z}, +) \rightarrow (U_{11}, \cdot)$ are there? Describe them by telling me where in U_{11} each homomorphism $\Phi^{(i)}$ sends the additive generator $a = [1]_5$ of the group $(\mathbb{Z}/5\mathbb{Z}, +)$.

4. (4pts) For $2 \leq n \leq 10$ fill in the values for $|U_n|$ in the following table.

n	2	3	4	5	6	7	8	9	10
$ U_n $									
Nontrivial Φ ?									

Identify all such n for which there is a nontrivial homomorphism $\Phi : (\mathbb{Z}/3\mathbb{Z}, + \rightarrow (U_n, \cdot))$. Explain.

Note : Φ is trivial if $\Phi(x)$ equals the identity element $e = [1]_n$ in U_n for all $x \in \mathbb{Z}/3\mathbb{Z}$. As a check on your calculations remember : $o(x)$ must divide $|U_{11}|$ for each $x \in U_{11}$.

Solution :

$U_{11} = \{1, 2, \dots, 10\}$ since $p = 11$ is prime ; $|U_{11}| = 10 = 5 \cdot 2$.

x	$o(x)$	$\langle x \rangle$
1	1	1
2	10	1, 2, 4, 8, 5, 10, 9, 7, 3, 6
3	5	1, 3, 9, 5, 4
4	5	1, 4, 5, 9, 3
5	5	1, 5, 3, 4, 9
6	10	1, 6, 3, 7, 9, 10, 5, 8, 4, 2
7	10	1, 7, 5, 2, 3, 10, 4, 6, 9, 8
8	10	1, 8, 9, 6, 10, 3, 2, 5, 7
9	5	1, 9, 4, 3, 5
10	2	1, 10

1. Distinct cyclic $\langle 1 \rangle$, $\langle 2 \rangle$, $\langle 3 \rangle$, $\langle 10 \rangle$ 4 in all isomorphic to $\{e\}$, $\mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$. G itself is cyclic, for example $G = \langle 2 \rangle$.
2. There is just one 5-Sylow, $H_5 = \langle 3 \rangle = \langle 4 \rangle = \langle 5 \rangle = \langle 9 \rangle$. It is $\simeq \mathbb{Z}/5\mathbb{Z}$. There is just one 2-Sylow : $H_2 = \langle 10 \rangle \simeq \mathbb{Z}/2\mathbb{Z}$.
3. Homomorphisms $\Phi : \mathbb{Z}/5\mathbb{Z} \rightarrow (U_{11}, \cdot) \simeq (\mathbb{Z}/10\mathbb{Z}, +)$ must send the generator $a = [1]_5$ to an element $\Phi(a) \in (U_{11}, \cdot)$ such that $\Phi(a)^5 = [1]_{11}$ is to the element $b = [1]_{11}$ or to one of the elements of multiplicative order 5, namely $b = [3]_{11}$, $[4]_{11}$, $[5]_{11}$ or $[9]_{11}$.
- 4.

n	2	3	4	5	6	7	8	9	10
$ U_n $	1	2	2	4	2	6	4	6	4
Nontrivial Φ ?						yes		yes	

Nontrivial homomorphism $\Phi : \mathbb{Z}/3\mathbb{Z} \rightarrow U_n$ exist if $n = 7, 9$. Since $|U_7| = |U_9| = 6$ implies that there is cyclic subgroups of order 3 (by Cauchy). No such Φ exist for $n = 2, 3, 4, 5, 6, 8, 10$.

Problem 4 : Short answer questions

- (4pts) List all elements of $(\mathbb{Z}/15\mathbb{Z}, +)$ that are additive generators of this group.
- (8pts) Here is a list of several abelian group of order $|G| = 225 = 3^2 5^2$. Make a table identifying all pairs that are isomorphic. Which of these groups are cyclic?

$$\begin{aligned}
 G_1 & \mathbb{Z}/225\mathbb{Z} \\
 G_2 & \mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \\
 G_3 & \mathbb{Z}/25\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \\
 G_4 & \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \\
 G_5 & \mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \\
 G_6 & \mathbb{Z}/75\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \\
 G_7 & \mathbb{Z}/45\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}
 \end{aligned}$$

Hint : For each G_i what is $\max\{o(x)\}$.

Solution :

Cyclic groups : $G_1, G_2, G_1 = \mathbb{Z}/225\mathbb{Z}$ Also G_2 which is isomorphic G by Chinese Remainder.

Isomorphic groups : $G_1 \simeq G_2, G_3 \simeq G_6$ (by CRT), $G_4 \simeq G_7$ (by CRT). Max order = 225 for G_1, G_2 ; $\max = 25$ for G_3, G_6 ; $\max = 45$ for G_4, G_7 ; $\max = 15$ for G_5 .

- (8pts) In the dihedral group $D_n = \{\rho^i \sigma^j : i \in \mathbb{Z}/n\mathbb{Z}, j \in \mathbb{Z}/2\mathbb{Z}\}$ the normal subgroup $N = \langle \rho \rangle$ has just 2 cosets, namely N and $N\sigma$.

(a) Prove that every element of the "outside" coset $N\sigma$ has order 2.

(b) In the particular group D_7 exhibit examples of

i. A 7-Sylow subgroup;

ii. A 2-Sylow subgroup;

described as explicit subsets of $D_7 = \{\rho^i \sigma^j : i \in \mathbb{Z}/7\mathbb{Z}, j \in \mathbb{Z}/2\mathbb{Z}\}$.

Solution :

(a) $x \in N\sigma$ implies $x = \rho^k \sigma$. Then $x^2 = \rho^k \sigma \rho^k \sigma = \rho^k \rho^{-k} = e$, but $\rho^k \sigma \neq e$ since it lies in $N\sigma$. Thus $o(\rho^k \sigma) = 2$ for all k .

(b) In D_7 , the subgroup of rotation $H_7 = \{\rho_\theta^k : 0 \leq k \leq 6\}$ is a 7-Sylow (and is normal). A 2-Sylow is $H_2 = \langle \sigma \rangle$, which is not normal.

- (4pts) Given the following permutations factored as disjoint cycles, identify (if any) lie in the same conjugacy class in S_8 .

(a) $C_1 = (1, 2, 3)(4857)$;

(b) $C_2 = (231)(5748)(6)$;

(c) $C_3 = (4382)(615)$;

(d) $C_4 = (12)(43)(685)$;

Solution : Elements are conjugate in S_8 if and only if they have same cycle type (Remember to count the 1-cycles). Types are $C_1 = 134$, $C_2 = 134$, $C_3 = 134$ (all conjugate in S_8) $C_4 = 1223$.

5. (4pt) If G is a finite group with $n = |G|$, explain why must have $x^n = e$ for all $x \in G$.

Solution : By Lagrange, if $m = o(x)$ for $x \in G$. Then m divides $n = |G|$, hence there is k such that $n = mk$. Then $x^n = (x^m)^k = e^k = e$.

6. (10pts) Below we show the action of a certain permutation $\sigma \in S_{10}$ on the integers 1, 2, ..., 10.

1	2	3	4	5	6	7	8	9	10
1	5	9	8	10	3	2	4	6	7

Based on this information :

- (a) Determine the decomposition of σ into disjoint cycles.

Solution :

$(1)(2, 5, 10, 7)(3, 9, 6)(4, 8)$

- (b) Decide whether σ is odd or even. **Solution :**

Even (sum of a k -cycle is $(-1)^{k-1}$).

- (c) What is the order of this element in S_{10} ? **Solution :**

$= \text{lcm of orders of factors. } o(\sigma) = \text{lcm}(4, 3, 2) = 12$.

- (d) What is the size of the conjugacy class of σ in S_{10} ?

Solution : $(10 \cdot 9 \cdot 8 \cdot 7)/4 \cdot (6 \cdot 5 \cdot 4)/3 \cdot (3 \cdot 2)/2 = 151200$

- (e) Determine the cycle decomposition of the conjugate $(135)\sigma(135)^{-1}$.

Solution : Since $\tau = (135)$ maps $1 \rightarrow 3 \rightarrow 5 \rightarrow 1$ leaving all other $k \in [1, 10]$:

$$(135)\sigma(135)^{-1} = \tau\sigma\tau^{-1} = (3)(2, 1, 10, 7)(5, 9, 6)(4, 8)$$

7. (6pts) Please note that you can use any question before even if you have not proven them.

- (a) Show that

$$(\text{Aut}(\mathbb{Z}/11\mathbb{Z}), \circ) \cong (\mathbb{Z}/10\mathbb{Z}, \cdot)$$

Solution :

We can prove that an automorphism of $\mathbb{Z}/11\mathbb{Z}$ is fully given by the image of a generator of $\mathbb{Z}/11\mathbb{Z}$ say $[1]$, we need to send it to some $[k]$ in $\mathbb{Z}/11\mathbb{Z}$, but in order to be an automorphism it is necessary and sufficient to choose $[k]$ in U_{11} . (Proved in class!) and then calling $\phi_{[k]} : [1] \rightarrow [k]$ then we get the isomorphism of group by sending $\phi_{[k]}$ to $[k]$.

(b) Show that every homomorphism

$$\phi : \mathbb{Z}/3\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/11\mathbb{Z})$$

is trivial, i.e $\phi(g) = \text{Id}$ for every $g \in \mathbb{Z}/3\mathbb{Z}$.

Solution :

To completely determine ϕ it is enough to know where to send a generator of $\mathbb{Z}/3\mathbb{Z}$, say $[1]$ but since $[1]$ has order 3 then order of its image by ϕ need to divide 3, but by Lagrange again it has also to divide 10 and the only possibility is that $\phi([1]) = [1]$

(c) Show that every semi-direct product of $\mathbb{Z}/11\mathbb{Z}$ by $\mathbb{Z}/3\mathbb{Z}$ (with $\mathbb{Z}/11\mathbb{Z}$ being normal in the semi-direct product) is actually a direct product.

Solution :

We know that a semi-direct product

$$\mathbb{Z}/11\mathbb{Z} \rtimes_{\phi} \mathbb{Z}/3\mathbb{Z}$$

is fully determined by an action of $\mathbb{Z}/3\mathbb{Z}$ on $\mathbb{Z}/11\mathbb{Z}$ or equivalently a morphism $\phi : \mathbb{Z}/3\mathbb{Z} \rightarrow \text{Aut}(\mathbb{Z}/11\mathbb{Z})$ but we have proven that the only morphism like this is the trivial one leading to a direct product.

8. (6 pts)

(a) Describe the action of G on itself by conjugation and show it is an action.

(b) Show that under this action $|\text{orb}(g)| = 1$ if and only if $g \in Z(G)$.

(c) Suppose that $|G| = p^n$.

i. Using the properties of group actions to prove that if $|\text{orb}(g)| \neq 1$ then $p \mid |\text{orb}(g)|$.

ii. Deduce from the previous question that G has non-trivial center.

Solution :

This proof has been done in class check class notes