Exam I

Exam Date: May 24th (Monday)
Exam Length: 100 minutes

- Please submit your work on Blackboard **between 09:00 am and 11:59 pm**.
- You are required to submit your work as a single pdf.
- Please make sure your handwriting is clear enough to read. Thanks.
- You will be allowed to use your notes and the book during the exam.
- **No collaborations are allowed.**
- **No consulting any online sources is allowed.**
- **No late work will be accepted.**
- Total score: *100 points*.

---

(1) Solve the following congruences.

(a) [**10 points**] $5x \equiv 1 \pmod{13}$ $\boxed{x \equiv 8 \pmod{13}}$

(i) Trial and error: $5 \cdot 8 \equiv 40 \equiv 1 \pmod{13}$

(ii)

k	1	2	3	4	5	6	7	8	9
$[5]^k$	$[5]$	$[-1]$	$[-5]$✓	$[1]$		$\cdots$			

(iii) Euclidean Algorithm (Matrix form): $2 \cdot 13 + 5 \cdot \overset{\checkmark}{(-5)} = 1$

$$\begin{bmatrix} 1 & 0 & 13 \\ 0 & 1 & 5 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -2 & 3 \\ 0 & 1 & 5 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -2 & 3 \\ -1 & 3 & 2 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 2 & -5 & 1 \\ -1 & 3 & 2 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 2 & -5 & 1 \\ -5 & 13 & 0 \end{bmatrix}$$

(iv) Euler's theorem: Since $(5, 13) = 1$, we have
$5^{\varphi(13)} \equiv 5^{12} \equiv 1 \pmod{13} \Rightarrow [5]^{-1} = [5]^{11} = ([5]^2)^5[5] = [-1]^5[5] = [-5] = [8]$

(b) [**10 points**] $12x \equiv 40 \pmod{88}$ $\boxed{x \equiv 18, 40, 62, 84 \pmod{88}}$

$(12, 88) = 4 | 40$✓ $\Rightarrow 3x \equiv 10 \pmod{22}$
So we need to find the solution to $3x \equiv 1 \pmod{22}$ first, it follows from any method in part (a) that $x \equiv 15 \pmod{22}$.
Thus, $x \equiv 15 \cdot 10 \equiv 18 \pmod{22}$.
That is, $x \equiv 18, 40, 62, 84 \pmod{88}$ are the desired solutions.

(2) [**20 points**] Let $S = \{x \in \mathbf{R} \mid x \neq 3\}$. Define $*$ on S by

$$a * b = 12 - 3a - 3b + ab.$$

Prove that $(S, *)$ is a group.

(i) Closure: We need to show $a * b \in S$ for any $a, b \in S$. That is, we need to show $a * b \neq 3$ for any real numbers $a \neq 3, b \neq 3$.
$a * b = 12 - 3a - 3b + ab = 3 + (3 - a)(3 - b) \neq 3$ since $(3 - a)(3 - b) \neq 0$. ✓

(ii) Associativity: For any $a, b, c \in S$, we need to show $(a * b) * c = a * (b * c)$.

$$\begin{aligned}(a*b)*c =&(12-3a-3b+ab)*c\\ =&12-3(12-3a-3b+ab)-3c+(12-3a-3b+ab)c\\ =&-24+9a+9b+9c-3ab-3ac-3bc+abc\end{aligned}$$

$$\begin{aligned}a*(b*c) =&a*(12-3b-3c+bc)\\ =&12-3a-3(12-3b-3c+bc)+a(12-3b-3c+bc)\\ =&-24+9a+9b+9c-3bc-3ab-3ac+abc\end{aligned}$$

(iii) Identity: The identity element $e = 4$.

$$a * 4 = 12 - 3a - 12 + 4a = a \text{ and } 4 * a = 12 - 12 - 3a + 4a = a.$$

(iv) Inverses: The inverse of a is $\dfrac{8-3a}{3-a} \neq 3$. It is well defined since $a \neq 3$.

$$a*\frac{8-3a}{3-a} = 12-3a-3\frac{8-3a}{3-a}+a\frac{8-3a}{3-a} = 12-3a+\frac{-24+9a+8a-3a^2}{3-a} = 4\checkmark$$

$$\frac{8-3a}{3-a}*a = 12-3\frac{8-3a}{3-a}-3a+\frac{8-3a}{3-a}a = 12-3a+\frac{-24+9a+8a-3a^2}{3-a} = 4\checkmark$$

(3) [**15 points**] Let $(G, \cdot)$ be an abelian group with identity element e. Let

$$H = \{a \in G \mid a \cdot a \cdot a \cdot a = e\}.$$

Prove that H is a subgroup of G.

(i) Closure: For any $a, b \in H$, we need to show $a \cdot b \in H$.

$$(a\cdot b)\cdot(a\cdot b)\cdot(a\cdot b)\cdot(a\cdot b) \overset{!}{=} (a\cdot a\cdot a\cdot a)\cdot(b\cdot b\cdot b\cdot b) = e\cdot e = e\checkmark$$

In the above calculation, $\overset{!}{=}$ holds since G is an abelian group.

(ii) Identity: The identity element $e \in H$ since $e \cdot e \cdot e \cdot e = e$.

(iii) Inverses: For any element $a \in H$, its inverse is a^{-1}.

$$a^{-1}\cdot a^{-1}\cdot a^{-1}\cdot a^{-1} = (a\cdot a\cdot a\cdot a)^{-1} = e^{-1} = e\checkmark$$

(4) (a) [**6 points**] Find the cyclic subgroup of S_8 generated by the element $(135)(68)$.

Using the property that the disjoint cycles commute with each other makes your calculations simpler. Note that the order of $(135)(68)$ is $\text{lcm}[3, 2] = 6$.

$$\begin{aligned}((135)(68))^2 =&(135)^2(68)^2 = (153)\\ ((135)(68))^3 =&(153)(135)(68) = (68)\\ ((135)(68))^4 =&(68)(135)(68) = (135)(68)^2 = (135)\\ ((135)(68))^5 =&(135)(135)(68) = (153)(68)\\ ((135)(68))^6 =&(153)(68)(135)(68) = (153)(135)(68)(68) = (1)\end{aligned}$$

Thus, the cyclic subgroup of S_8 generated by the element $(135)(68)$ is

$$\langle(135)(68)\rangle = \{(1), (135), (153), (68), (135)(68), (153)(68)\}.$$

(b) [**7 points**] Find a subgroup H of S_8 that contains 15 elements.
You do not have to list all of the elements in H. Just prove it. That is,
Prove that H (the one you find) is a subgroup of order 15 in S_8.

As we know that the order of a product of disjoint cycles is the least common multiple of their lengths, then the element $(12345)(678)$ is a desired example since $\operatorname{lcm}[3,5]=15$. In particular, let $H=\langle(12345)(678)\rangle$. Since the cyclic subgroup H is generated by $(12345)(678)$, thus $|H|=|\langle(12345)(678)\rangle|=o((12345)(678))=15$.

(5) [**15 points**] Let G be a group and the center of G is defined as

$$Z(G)=\{x\in G \mid xg=gx \text{ for all } g\in G\}.$$

In Homework 3 (7), we have showed that the center $Z(G)$ is a subgroup of G. Let H be a subgroup of G. Prove that the set

$$HZ(G)=\{hz \mid h\in H, z\in Z(G)\}$$

is a subgroup of G.

(i) Closure: For $h_1z_1, h_2z_2\in HZ(G)$, we need to show that $(h_1z_1)(h_2z_2)\in HZ(G)$.

$$(h_1z_1)(h_2z_2)=((h_1z_1)h_2)z_2=(h_1(z_1h_2))z_2\overset{!}{=}(h_1(h_2z_1))z_2=(h_1h_2)(z_1z_2)\checkmark$$

In the above calculation, $\overset{!}{=}$ holds by the definition of $Z(G)$.
$(h_1z_1)(h_2z_2)=(h_1h_2)(z_1z_2)\in HZ(G)$ since H and $Z(G)$ are subgroups of G.

(ii) Identity: The identity element $e\in HZ(G)$ since $e=ee\in HZ(G)$.

(iii) Inverses: For any element $hz\in HZ(G)$, its inverse is $h^{-1}z^{-1}\in HZ(G)$.

$$(hz)(h^{-1}z^{-1})=hzh^{-1}z^{-1}=h(zh^{-1})z^{-1}\overset{!}{=}h(h^{-1}z)z^{-1}=(hh^{-1})(zz^{-1})=e$$
$$(h^{-1}z^{-1})(hz)=h^{-1}z^{-1}hz=h^{-1}(z^{-1}h)z\overset{!}{=}h^{-1}(hz^{-1})z=(h^{-1}h)(z^{-1}z)=e$$

Or, in G, we have $(hz)^{-1}=z^{-1}h^{-1}$. So for $hz\in HZ(G)$, we have $(hz)^{-1}=z^{-1}h^{-1}\overset{!}{=}h^{-1}z^{-1}\in HZ(G)$. Here we see $z^{-1}\in Z(G)$ since $Z(G)$ is a subgroup.

Another much easier way: It is clear that $h^{-1}zh\overset{!}{=}h^{-1}hz=z\in Z(G)$ for all $h\in H$ and $z\in Z(G)$. Thus $HZ(G)$ is a subgroup of G.

(6) (a) [**5 points**] What is the order of $([15]_{20},[20]_{24})$ in $\mathbf{Z}_{20}\times\mathbf{Z}_{24}$?

Since $\gcd(15,20)=5$, then $o([15]_{20})=o([5]_{20})=4$, and
since $\gcd(20,24)=4$, then $o([20]_{24})=o([4]_{24})=6$.
Thus, the order of $([15]_{20},[20]_{24})$ is $\operatorname{lcm}[4,6]=12$.

(b) [**6 points**] What is the largest order of an element in $\mathbf{Z}_{20}\times\mathbf{Z}_{24}$?
And use your answer to show that $\mathbf{Z}_{20}\times\mathbf{Z}_{24}$ is not cyclic.

In $\mathbf{Z}_{20}$, the possible orders are $1,2,4,5,10$, and 20.
In $\mathbf{Z}_{24}$, the possible orders are $1,2,3,4,6,8,12$, and 24.
The largest possible least common multiple we can have is $\operatorname{lcm}[20,24]=120$.
So there is no element of order $|\mathbf{Z}_{20}\times\mathbf{Z}_{24}|=480$ and the group is not cyclic.
Another way to see that $\mathbf{Z}_{20}\times\mathbf{Z}_{24}$ is not cyclic since $\gcd(20,24)\neq 1$.

(c) [**6 points**] Let $G=\mathbf{Z}_{10}^{\times}\times\mathbf{Z}_{10}^{\times}$. Let $H=\langle(3,7)\rangle$ and $K=\langle(7,7)\rangle$. Find HK in G. *Here,* $(3,7)$ *means* $([3]_{10},[7]_{10})$. *Just use this simplified notations in your answer.*

$H=\langle(3,7)\rangle=\{(3,7)^m, m\in\mathbf{Z}\}=\{(1,1),(3,7),(9,9),(7,3)\}$ has order 4
$K=\langle(7,7)\rangle=\{(7,7)^m, m\in\mathbf{Z}\}=\{(1,1),(7,7),(9,9),(3,3)\}$ has order 4
$HK=\{(1,1),(3,7),(9,9),(7,3),(1,9),(9,1),(3,3),(7,7)\}$ has order $8=4\cdot 4/2$