Name: Solutions

Math 412 Winter 2019 Final Exam

Time: 120 mins.

1. Answer each question in the space provided. If you require more space, you may use the back of a page, but indicate that you have done so in the original answer space.
2. You may use any results proved in class, on the homework, or in the textbook, except for the specific question being asked. You should clearly state any facts you are using.
3. Remember to show all your work.
4. No calculators, notes, or other outside assistance allowed.

Best of luck!

Problem	Score
1	
2	
3	
4	
5	
6	
7	
8	
9	
Total	

Problem 1 (20 points). Write complete, precise definitions for, or precise mathematical characterizations of, each of the following italicized terms. Include any quantifiers as needed.

a) A *group* G.

A set G with an associative operation $\cdot$ such that:

(identity) there exists $e \in G$ such that $eg = ge = g$ for all $g \in G$

(inverses) For every $x \in G$ there exists $y \in G$ such that $xy = yx = e$.

b) A *normal* subgroup H of a group G.

A subgroup H of G such that $gH = Hg$ for all $g \in G$.

c) Given an action of a group G on a set X, the *stabilizer* of a point $x \in X$.

$\mathrm{Stab}(x) = \{ g \in G : g \cdot x = x \}$

d) The *order* of the element g in a group G.

$|g| = |\langle g \rangle|$

number of elements in the subgroup generated by g.

e) An[1] *ideal* I in a ring R.

A nonempty subset $I \subseteq R$ such that

- $(I, +)$ is a subgroup of $(R, +)$
- For every $r \in R$, $a \in I$, we have $ra \in I$ and $ar \in I$.

[1] Recall that in our definition, all rings have a multiplicative identity.

Problem 2 (15 points)**.** For each of the questions below, give an example with the required properties. No explanations required.

a) A group that is not cyclic.

$\mathbb{Z}_2 \times \mathbb{Z}_2$

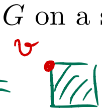
b) A finite field.

$\mathbb{Z}_2$

c) An odd permutation in $\mathcal{S}_9$.

$(1\,2)$

d) A group action of a group G on a set X with orbits $O(x_1)$ and $O(x_2)$ of different cardinalities.

$G = D_4$, $X =$  square

$x_1 =$ center of the square

$x_2 =$ vertex v

$\left(\begin{array}{l} |O(x_1)| = 1 \\ |O(x_2)| = 4 \end{array} \right)$

e) Two ideals $I, J \subseteq \mathbb{Z}_7[x]$ such that the quotient rings $\mathbb{Z}_7[x]/I$ and $\mathbb{Z}_7[x]/J$ both have 49 elements, but are not isomorphic to each other.

$I = (x^2)$, $J = (x^2+1)$

(sidenotes: $\mathbb{Z}_7[x]/I$ has 49 elements when $I = (f)$, deg $f = 2$.

x^2 is reducible $\Longrightarrow$ $\mathbb{Z}_7[x]/I$ is not a domain

x^2+1 is $\underbrace{\text{irreducible}}$ $\Longrightarrow$ $\mathbb{Z}_7[x]/J$ is a field ($\Longrightarrow$ domain)

note squares mod 7 are 0, 1, 2, or 4 only, not 6, so x^2+1 is irreducible)

Problem 3 (16 points)**.** For each of the questions below, indicate clearly whether the statement is *true* or *false*, and give a short justification.

a) Every group of order 10 is cyclic.

False. D_5 has order 10 but it is not abelian, so it is not cyclic.

b) If G is a finite group, and N is a normal subgroup, then the order of G/N divides the order of G.

True. the order of G/N is the index of N in G, $[G:N]$.
By Lagrange's theorem, $|G| = |N|\,[G:N] \Rightarrow |G/N| \mid |G|$.

c) If $p > 0$ is prime, then every two groups of order p are isomorphic.

True. Every group of order p is cyclic, so isomorphic to $\mathbb{Z}_p$.

d) If every element in a group G has finite order, then G is finite.

False. If $G = \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots}_{\text{infinitely many copies of } \mathbb{Z}_2}$, G is infinite, but every non-trivial element has order 2.

Problem 4 (12 points)**.** For each sentence below, circle the best word(s) or phrase(s) to fill in the blank(s) to make a correct statement.

(a) If $a \in \mathbb{Z}$ is invertible modulo n, we can use the __________ to find an inverse for a modulo n.

- division algorithm
- greatest common divisor
- Chinese Remainder Theorem
- Euclidean algorithm

(b) If R is a ________________, then the cancellation rule $ab = ac, a \neq 0 \Longrightarrow b = c$ holds.

- commutative ring
- domain
- prime ideal
- matrix ring

(c) If $\varphi : G \to H$ is a group homomorphism, the kernel of φ is a ________________.

- normal subgroup of G
- nontrivial subgroup of G
- proper subgroup of G
- normal subgroup of H
- nontrivial subgroup of H
- proper subgroup of H

(d) If H is a ________________ of the group G, then the set of H-cosets of G forms a group.

- subgroup
- finite subgroup
- normal subgroup
- abelian subgroup

(e) If a finite set G acts on a finite set X, and $x \in X$, then the ________________ times the ________________ equals the order of G.

- number of orbits of x; number of stabilizers of x
- number of orbits of x; number of elements in the stabilizer of x
- number of elements in the orbit of x; number of stabilizers of x
- number of elements in the orbit of x; number of elements in the stabilizer of x
- number of orbits in X; number of stabilizers of X

Problem 5 (9 points)**.** Indicate whether each of the following statements is true or false, and prove or disprove it.

(a) The map $\mathbb{Z}_{35} \xrightarrow{f} \mathbb{Z}_{35}$ given by $x \mapsto 17x$ is a group isomorphism.

True. f is a group homomorphism:

$$f(x+y) = 17(x+y) = 17x + 17y = f(x) + f(y)$$

f has an inverse g given by $g(x) = -2x = 33x$:

$$(fg)(x) = f(-2x) = -17 \cdot 2x = -34x = x \quad \forall x \in \mathbb{Z}_{35}$$

$$(gf)(x) = g(17x) = -2 \cdot 17x = -34x = x$$

(b) The map $\mathbb{Z}_{35} \longrightarrow \mathbb{Z}_{35}$ given by $x \mapsto 17x$ is a ring isomorphism.

False. This is not a ring homomorphism, since $1 \mapsto 17 \neq 1$.

(c) The map $\mathbb{Z}_{85} \longrightarrow \mathbb{Z}_{85}$ given by $x \mapsto x^{17}$ is a bijection.

True. This map is the identity!

Fermat's Little theorem: $x^{p-1} \equiv 1 \pmod p$ when $x \not\equiv 0 \pmod p$, p prime.

Consequence: $x^p \equiv x \pmod p$ for all x if p is prime.

$\mathbb{Z}_{85} \cong \mathbb{Z}_{17} \times \mathbb{Z}_5$ and 5 and 17 are prime. Then:

- $x^{17} \equiv x \pmod{17}$
- $x^{17} \equiv (x^4)^4 x \equiv \begin{cases} 1 \cdot x & \text{if } x \not\equiv 0 \\ 0 \cdot x & \text{if } x \equiv 0 \end{cases} \equiv x \pmod 5$

Problem 6 (8 points). (a) Find the order of the permutation $(2\,3)(5\,6\,8\,9)$ in $\mathcal{S}_{10}$.

this is a product of disjoint permutations, so they commute, and

$$|(23)(5689)| = \operatorname{lcm}(|(23)|, |(5689)|)$$
$$= \operatorname{lcm}(2, 4)$$
$$= 4.$$

(b) Find the order[2] of the coset $Ng \in G/N$, where $G = \mathrm{GL}_2(\mathbb{Z}_7)$, $N = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \;\middle|\; a \in \mathbb{Z}_7^\times \right\}$, and $g = \begin{bmatrix} 2 & 3 \\ 0 & 5 \end{bmatrix}$.

$g \notin N$, so $|Ng| > 1$

$$g^2 = \begin{bmatrix} 2 & 3 \\ 0 & 5 \end{bmatrix} = \begin{bmatrix} 4 & 2\cdot 3 + 3\cdot 5 \\ 0 & 25 \end{bmatrix} = \begin{bmatrix} 4 & 21 \\ 0 & 25 \end{bmatrix} = \begin{bmatrix} 4 & 0 \\ 0 & 4 \end{bmatrix} \in N$$

so $|Ng| = 2$.

[2]Order as an element of the group, not cardinality

Problem 7 (5 points)**.** Give an example or prove that no such example exists:
a polynomial $f \in \mathbb{Q}[x]$ of degree 3 with exactly two distinct rational roots and one irrational root.

there is no such polynomial! Suppose there is.
f has a root $\lambda \in \mathbb{Q} \iff (x-\lambda)$ is a factor of f.

If f has at least 2 rational roots α, β, then
$f(x) = (x-\alpha)(x-\beta)\, g(x)$. But then g has degree 1, which means f has a third rational root!

Problem 8 (5 points)**.** The number of "moves" on a Rubik's cube is

$$N = 43{,}252{,}003{,}274{,}489{,}856{,}000 = 2^{27} \cdot 3^{14} \cdot 5^3 \cdot 7^2 \cdot 11,$$

where a "move" consists of any combination of twists on the cube. The set of moves on a Rubik's cube forms a group under composition. Explain why, if a move M is such that M repeated 26 times in a row leaves all of the tiles unchanged, then M repeated twice in a row leaves all of the tiles unchanged.

we know $M^{26} = e$, so $|M| \mid 26$.
By Lagrange's theorem, $|M| \mid N$, but $(N, 13) = 1$.
we conclude that $|M| \mid 2$, so $M^2 = e$.

Problem 9 (10 points)**.** (a) Let G be a group. Show that the rule $g \cdot h = ghg^{-1}$ defines a group action (of the group G on itself as a set $X = G$).

1) For all $h \in G$, $e \cdot h = h$:

$$e \circ h = ehe^{-1} = h.$$

2) For all $g, f \in G$, and all $h \in G$, $g \cdot (f \cdot h) = (gf) \cdot h$.

$$g \circ (f \cdot h) = g \circ (fhf^{-1}) = g(fhf^{-1})g^{-1}$$
$$= (gf)h(gf)^{-1} = (gf) \cdot h.$$

(b) Prove that if G is any group of order p^2, where $p > 0$ is prime, then the center of G is not $\{e\}$.

Consider the action of G on G by conjugation.
the fixed points of this action are pecisely the elements of the center:

$$|O(h)| = 1 \iff \forall g \in G \ \ ghg^{-1} = h \iff \forall g \in G \ \ gh = hg \iff h \in Z(G)$$

By the orbit-stabilizer theorem, the size of each orbit divides p^2, so orbits have 1, p or p^2 elements. then

$$|Z(G)| \cdot 1 + (\#\text{orbits of size } p) \cdot p + (\#\text{orbits of size } p^2) \cdot p^2 = p^2$$

$\Longrightarrow |Z(G)|$ is a multiple of p $\Longrightarrow$ $|Z(G)| \geq p$.
since $e \in Z(G)$