Name:

Math 412 Fall 2021 Final Exam–Solutions

Time: 120 mins.

1. Answer each question in the space provided. If you require more space, you may use the blank page at the end of this exam, but you must clearly indicate in the provided answer space that you have done so.
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	
Total	

Problem 1 (3 points each)**.** Give examples as requested. No explanation needed:

1. An abelian group which is not cyclic.

2. A subgroup of a group which is not normal.

3. A group of order 75 and a 5-Sylow subgroup.

4. A non-zero proper subgroup of $Z_5^\times$.

Solution.

1. An example is given by $G = \mathbf{Z}_2 \times \mathbf{Z}_2$.

2. For example, if $G = S_3$, then the subgroup $H = \langle (12) \rangle$ is not normal.

3. For example, if $G = \mathbf{Z}_{75}$, then the subgroup $\langle [3]_{75} \rangle$ is a 5-Sylow subgroup.

4. The only one is $G = \big\{ [1]_5, [4]_5 \big\}$.

Problem 2 (4 points each)**.** For a given group G and an element $g \in G$, compute the order of g (and give a justification).

1. $G = \mathbb{Z}_{12}$ and $g = [3]_{12}$,

2. $G = S_7$ and $g = (123)(345)(67)$,

3. $G = S_4/N$ where $N = \{e, (12)(34), (13)(24), (14)(23)\}$ and $g = (1234)N$.

Solution.

1. The order is 4: we have $3m \equiv 0 \pmod{12}$ if and only if 4 divides m.

2. Note that $(123)(345)(67) = (12345)(67)$. Since (12345) is a cycle of length 5, its order is 5, and since (67) is a cycle of order 2, its order is 2. These two cycles are disjoint, hence commute, hence the order of of g divides the product of the 2 orders, which is 10. On the other hand, we have $g^2 = (13524) \neq e$ and $g^5 = (67) \neq e$, hence the order of g is 10.

3. We need to find the smallest positive integer m such that $(1234)^m \in N$. Note that $(1234) \notin N$: indeed, all permutations in N are even, hence $N \subseteq A_4$. On the other hand, (1234) is odd, hence $(1234) \notin N$. On the other hand, we have $(1234)^2 = (13)(24) \in N$. Therefore, the order of g is 2.

Problem 3 (4 points each)**.** Let $R = \mathbb{Z}_3[x]/(x^2 + 2x + 1)$.

1. Find the number of elements of R.

2. Find the number of elements of $R^\times$.

3. Is $R^\times$ a cyclic group? Justify your answer.

Solution.

1. We have seen in class that every element in R can be represented by a unique polynomial in R of degree 1. Therefore R has $3 \times 3 = 9$ elements.

2. A polynomial $f \in \mathbb{Z}_3[x]$ of degree 1 gives an invertible element of R if and only if there are $g, h \in \mathbb{Z}_3[x]$ such that $fg + (x^2+2x+1)h = 1$. This is the case if and only if f and x^2+2x+1 are relatively prime; since $x^2 + 2x + 1 = (x + 1)^2$, this condition is further equivalent to the fact that $x + 1$ does not divide f, that is, $f(-1) \neq 0$. We are thus looking for polynomials $a + bx \in \mathbb{Z}_3[x]$ with $a - b \neq 0$. It follows that $R^\times$ has 6 elements.

3. Using the fact that $x^2 = -2x - 1$ in R, it is straightforward to check that
$$x^2 = x + 2, x^3 = 2, x^4 = 2x, x^5 = 2x + 1, x^6 = 1.$$
This shows that x has order 6, hence $R^\times$ is cyclic. One could also argue by noticing that $R^\times$ is abelian (since R is a commutative ring) and every abelian group of order 6 is cyclic.

Problem 4 (3 points each)**.** For each of the questions below, indicate clearly whether the statement is *true* or *false*, and give a short justification.

1. There exists a group of order 9 acting on a set X such that such that some $x \in X$ has orbit of cardinality 5.

2. The map $f\colon \mathbb{Z}_5 \longrightarrow \mathbb{Z}_5$ given by $f(x) = x^3$ is a ring isomorphism.

3. If an action of a group G on a set X is faithful, then $\operatorname{Stab}(x) = \{e\}$ for every $x \in X$.

4. The only group homomorphism $\varphi\colon D_3 \to \mathbb{Z}_3$ is the trivial homomorphism $\varphi(x) = [0]_3$ for all $x \in D_3$.

Solution.

1. This is false: if G has 9 elements, acts on X, and $x \in X$ has an orbit with 5 elements, then it follows from the Orbit-Stabilizer theorem that $\frac{|G|}{|\operatorname{Stab}(x)|} = 5$. However, 5 does not divide 9.

2. This is false: note that $f\big([1]_5\big) = [1]_5$, while $f\big([2]_5\big) = [8]_5 = [3]_5$, which is different from $f\big([1]_5\big) + f\big([1]_5\big) = [2]_5$. Hence f is not a ring homomorphism.

3. This is false: the fact that the group action is faithful says that $\bigcap_{x \in X} \operatorname{Stab}(x) = \{e\}$. For example, the action of D_4 on the vertices of a square is faithful, but the stabilizer of any element has order 2.

4. This is true: if we have a homomorphism $\varphi\colon D_3 \to \mathbb{Z}_3$ which is not the trivial homomorphism, then it is surjective. If $H = \ker(\varphi)$, then H is a normal subgroup of D_3 such that $D_3/H \simeq \mathbb{Z}_3$ by the First Isomorphism theorem. Using Lagrange's theorem we conclude that $|H| = \frac{|D_3|}{|\mathbb{Z}_3|} = 2$. However, every subgroup of order 2 of D_3 (which is generated by one of the reflections), is not a normal subgroup of D_3.

Problem 5 (2 points each)**.** Write the following groups as products of cyclic groups $\mathbb{Z}_n$ (e.g. $\mathbb{Z}_5^\times$ is isomorphic to the cyclic group $\mathbb{Z}_4$). No justification required.

1. $\mathbb{Z}_{12}^\times$
2. $\mathbb{Z}_{16}^\times$
3. $\mathbb{Z}_{36}/4\mathbb{Z}_{36}$
4. S_4/A_4
5. $<(12),(34),(56)>$ as a subgroup of S_6
6. $<\begin{bmatrix}1 & 2\\ 0 & 1\end{bmatrix}>$ as a subgroup of $\mathbb{GL}_2(\mathbb{Z}_8)$
7. $Z(D_3)$
8. $D_4/Z(D_4)$.

Answers.

1. $\mathbb{Z}_2 \times \mathbb{Z}_2$
2. $\mathbb{Z}_4 \times \mathbb{Z}_2$
3. $\mathbb{Z}_4$
4. $\mathbb{Z}_2$
5. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
6. $\mathbb{Z}_4$
7. $\{e\} = \mathbb{Z}_1$
8. $\mathbb{Z}_2 \times \mathbb{Z}_2$ (note that $Z(D_4) = \{e, \theta\}$, where θ is the rotation by π. The quotient is a group with 4 elements in which the square of every element is the identity).

Problem 6 (6 points each)**.** Let R be a ring. Consider an operation $\star$ on the set $R \times R$ defined as follows:

$$(x_0, x_1) \star (y_0, y_1) := (x_0 + y_0, x_1 + y_1 + x_0 y_0).$$

where $x_0, x_1, y_0, y_1 \in R$.

1. Show that $a \star (b \star c) = (a \star b) \star c$ for $a, b, c \in R \times R$.
2. Prove that $(R \times R, \star)$ is a group.

Solution.

1. Let's write $a = (x_0, x_1)$, $b = (y_0, y_1)$, and $c = (z_0, z_1)$. By definition, we have

   $$a \star (b \star c) = (x_0, x_1) \star (y_0 + z_0, y_1 + z_1 + y_0 z_0) = (x_0 + y_0 + z_0, x_1 + y_1 + z_1 + y_0 z_0 + x_0 y_0 + x_0 z_0).$$

   We similarly have

   $$(a \star b) \star c = (x_0 + y_0, x_1 + y_1 + x_0 y_0) \star (z_0, z_1) = (x_0 + y_0 + z_0, x_1 + y_1 + x_0 y_0 + z_1 + x_0 z_0 + y_0 z_0).$$

   The two expressions agree since addition is commutative in R.

2. We have already seen that $\star$ is associative. The identity element is given by $(0, 0)$: indeed, we have

   $$(x_0, x_1) \star (0, 0) = (x_0, x_1) = (0, 0) \star (x_0, x_1) \quad \text{for every} \quad (x_0, x_1) \in R \times R.$$

   In order to see that $(R \times R, \star)$ is a group, it is enough to check that inverses exist. Given $(x_0, x_1) \in R \times R$, we are looking for (y_0, y_1) such that

   $$(x_0 + y_0, x_1 + y_1 + x_0 y_0) = (0, 0) = (y_0 + x_0, y_1 + x_1 + y_0 x_0). \tag{1}$$

   The first equality means that we need $y_0 = -x_0$ and $x_1 + y_1 + x_0 y_0 = 0$. This means that $y_1 = -x_1 + x_0^2$. It is straightforward to check now that $(-x_0, -x_1 + x_0^2)$ also satisfies the second equality in (1); therefore this is the inverse of (x_0, x_1).

Problem 7 (12 points)**.** Let p be an odd prime number and let $a \in \mathbb{Z}_p$ be nonzero. Show that $a = x^2$ for some $x \in \mathbb{Z}_p$ if and only if $a^{\frac{p-1}{2}} = 1$.

Solution. Since p is a prime number, we know that the group $\mathbb{Z}_p^\times = \mathbb{Z}_p \smallsetminus \{0\}$ is cyclic. Let y be a generator. Suppose first that $a = x^2$ for some $x \in \mathbb{Z}_p$. Since $a \neq 0$, it follows that $x \neq 0$ and we have

$$a^{\frac{p-1}{2}} = x^{p-1} = 1,$$

since the order of x in $\mathbb{Z}_p^\times$ divides the order of the group (which is $p-1$) by the corollary to Lagrange's theorem.

Conversely, suppose that $a^{\frac{p-1}{2}} = 1$. Since $\mathbb{Z}_p^\times$ is generated by y, we have $a = y^m$, for some integer m. We thus have

$$a^{\frac{p-1}{2}} = y^{m\frac{p-1}{2}} = 1.$$

Since y has order $p-1$, we conclude that $p-1$ divides $m\frac{p-1}{2}$, hence m is even. If we write $m = 2k$ and take $x = y^k$, we conclude that $a = x^2$.

Problem 8 (6 points each)**.** Let H be a subgroup of a group G.

1. The *normalizer* $N_G(H)$ is given by
$$N_G(H) = \{g \in G \mid gH = Hg\}.$$
Show that $N_G(H)$ is a subgroup of G and H is a normal subgroup of $N_G(H)$.

2. Two subgroups H_1 and H_2 of G are *conjugate* if there is $g \in G$ such that $H_2 = gH_1g^{-1}$. Show that if G is finite, then the number of subgroups of G conjugate to H is equal to $[G : N_G(H)]$.

Solution.

1. Note first for any $a \in G$, we have $a \in N_G(H)$ if and only if $aHa^{-1} = H$.

   It is clear that $e \in N_G(H)$: indeed $eH = H = He$. Let's show now that if $x, y \in N_G(H)$, then $xy \in N_G(H)$. Note that
$$(xy)H(xy)^{-1} = x(yHy^{-1})x^{-1} = xHx^{-1} = H,$$
   where the first equality follows using $y \in N_G(H)$ and the last equality follows using $x \in N_G(H)$.

   Finally, we need to show that if $x \in N_G(H)$, then $x^{-1} \in N_G(H)$. Indeed, we have $xHx^{-1} = H$. Multiplying by x^{-1} on the left and by x on the right gives
$$H = x^{-1}(xHx^{-1})x = x^{-1}Hx,$$
   hence $x \in N_G(H)$.

   Since H is a subgroup of G, in order to check that it is a subgroup of $N_G(H)$, we only need to check $H \subseteq N_G(H)$. This is easy: if $h \in H$, then $hH = H = Hh$.

   Finally, for every $x \in N_G(H)$, we have $xHx^{-1} = H$, hence H is a normal subgroup of G.

2. We define an action of G on the set of subgroups of G given by
$$g \star H = gHg^{-1}.$$
   This is indeed and action: $e \star H = H$ for every H and
$$g_1 \star (g_2 \star H) = g_1 \star (g_2Hg_2^{-1}) = (g_1g_2)H(g_1g_2)^{-1} = (g_1g_2) \star H.$$
   The subgroups of G conjugate to H form the orbit of H. On the other hand, by definition we have $\mathrm{Stab}(H) = N_G(H)$. By the Orbit-Stabilizer theorem, we thus deduce that the number of subgroups conjugate to H is
$$\frac{|G|}{|\mathrm{Stab}_G(H)|} = [G\colon N_G(H)],$$
   where the equality follows from Lagrange's theorem.