Show all your work, and return this sheet with your exam. Name: _____

Notation: $\mathbb{Z}$ is the group of integers with group operation given by addition; $\mathbb{Z}_n$ is the group of congruence classes modulo n with operation addition of congruence classes; $\mathbb{Z}_n^*$ is the group of invertible congruence classes modulo n with operation multiplication of congruence classes; S_n is the group of permutations of the set $\{1, 2, \ldots, n\}$ with operation composition of permutations; D_n is the group of symmetries of the regular n-sided polygon with operation composition of functions.

1. [12 points] For each group below, find the order of the group and determine if the group is abelian.

(a) $\mathbb{Z}_{15}$ (b) $\mathbb{Z}_{15}^*$ (c) S_5 (d) D_5

(a) $|\mathbb{Z}_{15}| = 15$ this group is abelian: addition of integers is commutative, so addition of congruence classes of integers is commutative

(b) $|\mathbb{Z}_{15}^*| = \varphi(15) = 8$ this group is abelian: multiplication of integers is commutative, so multiplication of congruence classes of integers is commutative

(c) $|S_5| = 5! = 120$ this group is not abelian: e.g., $(1,2)(1,3) = (1,3,2) \neq (1,2,3) = (1,3)(1,2)$

(c) $|D_5| = 2 \cdot 5 = 10$ this group is not abelian: e.g, a rotation followed by a reflections is in general different from a reflection followed by a rotation

2. [19 points] Let G be the group with the given multiplication table:

$\circ$	u	v	w	x	y	z
u	z	x	y	v	w	u
v	w	y	x	u	z	v
w	v	u	z	y	x	w
x	y	w	v	z	u	x
y	x	z	u	w	v	y
z	u	v	w	x	y	z

(a) Which element is the identity of G?

(b) Find the order of v, and the inverse of v.

(c) Recall that for $a \in G$, the centralizer of a is $C(a) = \{g \in G : ga = ag\}$. Find $C(y)$.

(d) For **any** group G, and $a \in G$, prove that $C(a)$ is a subgroup of G.

(a) Since $zg = g = gz$ for every element $g \in G$, z is the identity element of G.

(b) Since $v^2 = y$ and $v^3 = v^2v = yv = vy = vv^2 = z$, the order of v is 3, and $v^{-1} = y$.

(c) $C(y) = \{z, v, y\}$.
Note that $uy = w \neq x = yu$, $wy = x \neq u = yw$, $xy = u \neq w = yx$ so $u, w, x \notin C(y)$.

(d) Fix $a \in G$. Note that $C(a)$ is nonempty since the identity element e of G is in $C(a)$ (as $ea = a = ae$). Let $g, h \in C(a)$. To show that $C(a)$ is a subgroup of G, it is enough to show that gh^{-1} is in $C(a)$. We have $ga = ag$ and $ha = ah$ since $g, h \in C(a)$. Using the group cancellation laws, the second of these equalities shows that $ah^{-1} = h^{-1}a$, so $h^{-1} \in C(a)$. Now compute $(gh^{-1})a = g(h^{-1}a) = g(ah^{-1}) = (ga)h^{-1} = (ag)h^{-1} = a(gh^{-1})$. This shows that $gh^{-1} \in C(a)$, and $C(a)$ is a subgroup of G.

3. [18 points] Let σ be the permutation $\sigma = (2,3,4)(1,5)$ in the symmetric group S_5, and let $H = (\sigma)$ be the cyclic subgroup generated by σ.

(a) Find all distinct elements in H.

(b) If $\tau = (45)$, find all the elements of the left coset τH.

(c) State Lagrange's Theorem, and find the number of distinct left cosets of H in S_5.

(a) Since σ is the product of disjoint cycles of length 2 and 3, the order of σ is $[2,3] = 6$. So $H = \{e = \sigma^0, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5\}$. Since disjoint cycles commute, $\sigma^2 = (2,3,4)^2(1,5)^2 = (2,3,4)^2 = (2,4,3)$, $\sigma^3 = (2,3,4)^3(1,5)^3 = (1,5)^1 = (1,5)$, $\sigma^4 = (2,3,4)^4(1,5)^4 = (2,3,4)^1 = (2,3,4)$, $\sigma^5 = (2,3,4)^5(1,5)^5 = (2,3,4)^2(1,5)^1 = (2,4,3)(1,5)$.

(b) $\tau H = \{\tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3, \tau\sigma^4, \tau\sigma^5\}$. Computing using part (a) yields $\tau\sigma = (1,4,2,3,5)$, $\tau\sigma^2 = (2,5,4,3)$, $\tau\sigma^3 = (1,4,5)$, $\tau\sigma^4 = (2,3,5,4)$, $\tau\sigma^5 = (1,4,3,2,5)$.

(c) *If G is a finite group, and H is a subgroup of G, then $|G| = [G:H] \cdot |H|$, where $[G:H]$ is the index of H in G, the number of distinct left cosets of H in G.*
Since $|S_5| = 120$ and $|H| = 6$, there are 20 distinct left cosets of H in S_5.

4. [16 points] Let $G = \mathbb{Z}_{14}^* = \{1,3,5,9,11,13\}$ be the group of invertible congruence classes modulo 14 (that is, the units in $\mathbb{Z}_{14}$), with group operation given by multiplication of congruence classes.

(a) What is the relationship between the order of an element $g \in G$ and the order of the group G?

(b) Which of the subsets $H = \{1,5,11\}$ and $K = \{1,9,11\}$ of G is a subgroup of G? Explain.

(c) The group G is cyclic. Find a generator.

(a) The order of g is equal to the order of the cyclic subgroup generated by g, $o(g) = |(g)|$.
By Lagrange's Theorem, $o(g)$ divides $|G| = 6$ (so $o(g)$ could be 1, 2, 3, or 6).

(b) Since $5 \cdot 11 \equiv 13 (\mathrm{mod}\, 14)$, $5 \cdot 11 \notin H$, H is not closed under the operation of G (i.e., multiplication), and H is not a subgroup of G.
Check that $9 \cdot 9 \equiv 11 (\mathrm{mod}\, 14)$, $9 \cdot 11 = 11 \cdot 9 \equiv 1 (\mathrm{mod}\, 14)$, and $11 \cdot 11 \equiv 9 (\mathrm{mod}\, 14)$. From this (essentially, the multiplication table of K), it is easy to check that K is a subgroup of G.

(c) Since $(3) = \{3^0, 3^1, 3^2, 3^3, 3^4, 3^5\} = \{1,3,9,13,11,5\}$ (computing modulo 14), $G = (3)$, and 3 is a generator of G. Similarly, $(5) = \{1,5,11,13,9,3\}$, $G = (5)$ and 5 is a generator of G.
Since $(1) = \{1\}$, $(9) = \{1,9,11\}$, $(11) = \{1,11,9\}$, and $(13) = \{1,13\}$, the elements 1, 9, 11, and 13 are not generators of G.

5. [17 points] Let $\sigma = (1,3,6)(1,2)(2,6,4,3)(5,6)$ in the symmetric group S_6

(a) Write σ in two row notation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ \sigma(1) & \sigma(2) & \sigma(3) & \sigma(4) & \sigma(5) & \sigma(6) \end{pmatrix}$

(b) Write σ as a product of disjoint cycles, and find the order of σ.

(c) Is σ^{-1}, the inverse of σ, an even permutation or an odd permutation?

(d) The group S_8 acts on $X = \{1,2,3,4,5,6\}$, $(\tau, k) \mapsto \tau(k)$. Find the elements of X fixed by σ.

(a) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 6 & 4 & 5 \end{pmatrix}$

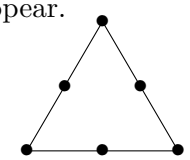
(b) $\sigma = (1,2)(4,6,5)$. Since σ is the product of disjoint cycles of length 2 and 3, the order of σ is $[2,3] = 6$.

(c) Since $\sigma = (1,2)(4,6,5) = (1,2)(4,5)(4,6)$ is the product of 3 transpositions, σ is odd. Consequently, $\sigma^{-1} = (4,6)(4,5)(1,2)$ is also odd.

(d) There was a typo in this part. It should have read S_6 acts, not S_8 acts...
Viewing $\sigma \in S_6$ acting on $X = \{1,2,3,4,5,6\}$, σ fixes only 3, i.e., $X_\sigma = \{3\}$.
Viewing $\sigma \in S_8$ acting on $X = \{1,2,3,4,5,6,7,8\}$, σ fixes 3, 7, and 8, i.e., $X_\sigma = \{3,7,8\}$.

6. [18 points]

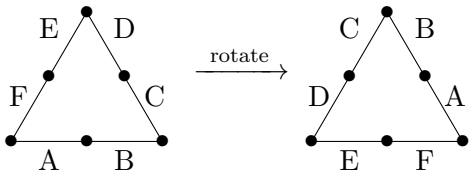
(a) Complete the statement the Burnside Theorem. Clearly define all terms that appear.
If G is a finite group that acts on a finite set X, then the number N of distinct orbits of G on X is...



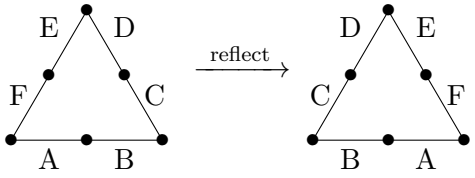
(b) Each side of an equilateral triangle is divided into two equal parts, and each part is colored purple or gold. Find the number of different color patterns.

(a) $\ldots N = \dfrac{1}{|G|} \displaystyle\sum_{g \in G} |X_g|$, *where $|G|$ is the order of G, $X_g = \{x \in X : gx = x\}$ is the fixed set of $g \in G$, $|X_g|$ is the cardinality of X_g, and the sum is over all elements of G.*

(b) If X is the set of such colorings of the triangle, then $|X| = 2^6$. The relevant group of symmetries is the dihedral group D_3, the group of symmetries of the triangle (which is equal to the symmetric group S_3). This group has 6 elements, the identity, two nontrivial rotations, and three reflections. The identity fixes all of X; each nontrivial rotation fixes 2^2 elements of X, and each reflection fixes 2^3 elements of X (see below). So, by the Burnside Theorem, the number of different color patterns is $N = (2^6 + 2 \cdot 2^2 + 3 \cdot 2^3)/6 = 16$.



This coloring is fixed if A=C=E and B=D=F. There are 2^2 such colorings.



This coloring is fixed if A=B, C=F, and D=E. There are 2^3 such colorings.

Extra Credit. Encrypt your (two) initials using the RSA cryptosystem with $n = 2759$ and $e = 11$.
For me, this would be DC $\to 0403 \to 403^{11} (\mathrm{mod}\, 2759) \to (403^8 \cdot 403^2 \cdot 403) (\mathrm{mod}\, 2759) \to 0589$

SPRING 2014 MATH 4023-1 EXAM 2 STATISTICS

In light of the typo in problem **5.**(d) noted above, you should consider this part (worth 3 points) as extra, and the exam as out of 97.

Score	Number
90 – 97	3
80 – 89	4
70 – 79	3
60 – 69	5
50 – 59	3
0 – 49	1
total	19

average: 71
median: 70