Math 3110 **Final Exam** **December 9^{th}, 2009**

ANSWER KEY

1. (12 points) For each of the following pairs of groups, if the groups are isomorphic, circle $G_1 \cong G_2$ and explain why they are isomorphic. If the groups aren't isomorphic, circle $G_1 \ncong G_2$ and explain why not.

(a) $\mathbb{Q} \ncong Q$ [where $\mathbb{Q}$ = rationals, Q = quaternions]

There are pleanty of reasons why the rationals and quaternions cannot be isomorphic. The easiest reasons are (1) The rationals are an infinite group while the quarternions are a group of order 8 and (2) the rationals are an abelian group while the quaternions are not.

But there are other (harder & sillier) ways to see that these groups aren't isomorphic. For example, all of the non-identity elements in $\mathbb{Q}$ have infinite order ($0 \neq r \in \mathbb{Q}$ then $r + r + \cdots + r = nr \neq 0$ unless $n = 0$). On the other hand, the non-identity elements of Q have orders 2 and 4.

(b) $A_4 \ncong D_6$ [where A_4 = even permutations in S_4]

These are both non-abelian groups of order 12 ($|A_4| = 4!/2 = 24/2 = 12$ and $|D_6| = 2 \cdot 6 = 12$). So we need to look deeper. If we start examining the orders of elements, we find out that the orders don't match.

S_4 consists of the identity (order 1), transpositions (i.e. 2-cycles which have order 2), 3-cycles (order 3), 4-cycles (order 4), and pairs of disjoint transpositions (e.g. (12)(34) whose orders are $\text{lcm}(2,2) = 2$). Since A_4 is a subgroup of S_4 it must also only have elements of orders 1, 2, 3, and 4. In fact, to be precise, A_4 only has elements of orders 1, 2, and 3 (4-cycles are odd).

On the other hand D_6 consists of 6 reflections (all order 2) and the cyclic subgroup of rotations. Since this cyclic subgroup has order 6 it is isomorphic with $\mathbb{Z}_6$ and thus has the same element orders. This gives us 1 element of order 1, 1 (more) element of order 2, 2 elements of order 3, and 2 elements of order 6.

In particular, D_6 has an element of order 6 while A_4 does not. Therefore, they cannot be isomorphic. Another way to arrive at this conclusion is to count the number of element of a particular order. D_6 has 2 elements of order 3 while A_4 has many more — for example: (123), (132), (124), (142), ...

(c) $U(5) \cong \mathbb{Z}_4$

$U(5) = \{1, 2, 3, 4\}$ (the group of units of $\mathbb{Z}_5$ under **multiplication** mod 5).

Both groups are abelian of order 4. $\mathbb{Z}_4$ is cyclic, so if $U(5)$ is cyclic, we'll have two cyclic groups of the same order – therefore isomorphic. Or if $U(5)$ isn't cyclic, it cannot be isomorphic with $\mathbb{Z}_4$.

Consider powers of 2: $2^1 = 2$, $2^2 = 4$, $2^3 = 8$ mod 5 is 3, $2^4 = 16$ mod 5 is 1. So $\langle 2 \rangle = \{2, 4, 3, 1\} = U(5)$ and thus $U(5)$ is cyclic. Therefore the groups are isomorphic.

2. (12 points) Sub-Things

(a) Let G be a group. Recall that $Z(G) = \{x \in G \mid gx = xg \text{ for all } g \in G\}$ is the "center" of G. Prove that $Z(G)$ is a normal subgroup of G. [Hint: You may either *show it is a subgroup* **and** *show it is normal*, or you can find a homomorphism with kernel $Z(G)$.]

Traditional Approach: First, notice that $ge = g = eg$ for all $g \in G$. Thus $e \in Z(G)$ so $Z(G)$ is a non-empty subset of G. Next, suppose that $x, y \in Z(G)$ and let $g \in G$. Since g commutes with x and y, it commutes with their product: $g(xy) = (gx)y = (xg)y = x(gy) = x(yg) = (xy)g$. Therefore, $xy \in Z(G)$. Also, $gx^{-1} = (xg^{-1})^{-1} = (g^{-1}x)^{-1} = x^{-1}g$ since $(g^{-1})^{-1} = g$ and $(ab)^{-1} = b^{-1}a^{-1}$. Thus $x^{-1} \in Z(G)$. This shows us that $Z(G)$ is a subgroup of G.

We also need to show that $Z(G)$ is normal. We could either show that the left and right cosets of $Z(G)$ in G are equal: $gZ(G) = \{gx \,|\, x \in Z(G)\} = \{xg \,|\, x \in Z(G)\} = Z(G)g$ **OR** we can show that $Z(G)$ absorbs conjugates: if $x \in Z(G)$, then $gxg^{-1} = xgg^{-1} = x \in Z(G)$. Either way, we have shown that $Z(G)$ is normal.

Kernel Approach: The kernel of a homomorphism is a normal subgroup of the domain of that map and every normal subgroup is the kernel of some homomorphism. So if we can invent a homomorphism whose kernel is $Z(G)$, we'll get that $Z(G)$ is a normal subgroup "for free".

Consider $\psi : G \to \text{Aut}(G)$ (the automorphisms of G) defined by $\psi(x) = \varphi_x$ where $\varphi_x(g) = xgx^{-1}$. We showed that φ_x is always an automorphism, so ψ does indeed map into $\text{Aut}(G)$. Next, notice that $\psi(xy) = \varphi_{xy} = \varphi_x \circ \varphi_y = \psi(x) \circ \psi(y)$ since $\varphi_{xy}(g) = (xy)g(xy)^{-1} = xygy^{-1}x^{-1} = x(\varphi_y(g))x^{-1} = \varphi_x(\varphi_y(g))$. Thus ψ is a homomorphism. Finally, suppose $\psi(x) = \text{id}_G$. This holds if and only if $\varphi_x(g) = \text{id}_G(g) = g$ for all $g \in G$. Which holds if and only if $xgx^{-1} = g$ for all $g \in G$. Which in turn hold if and only if $xg = gx$ for all $g \in G$. Thus $x \in \text{Ker}(\psi)$ if and only if $x \in Z(G)$. Since $Z(G) = \text{Ker}(\psi)$ it is a normal subgroup. Hmmm...I think the first way is easier.

(b) Let $S = \{m + n\sqrt{5} \,|\, m, n \in \mathbb{Z}\}$. Show S is a sub**ring** of $\mathbb{R}$.

We need to run through the subring test. S is (obviously) a non-empty subset of $\mathbb{R}$. Next, suppose $a + b\sqrt{5}, m + n\sqrt{5} \in S$ [where $a, b, m, n \in \mathbb{Z}$]. Then $(a + b\sqrt{5}) - (m + n\sqrt{5}) = (a - m) + (b - n)\sqrt{5}$ which is an element of S since both $a - m$ and $b - n$ are integers. Thus S is closed under subtraction. $(a + b\sqrt{5})(m + n\sqrt{5}) = (am + 5bn) + (an + bm)\sqrt{5}$ is an element of S since both $am + 5bn$ and $an + bm$ are integers. Thus S is closed under mutliplication. Therefore, S is a subring of $\mathbb{R}$.

(c) Let $T = \{m + n\sqrt{5} \,|\, m, n \in \mathbb{Z}$ and m is **EVEN**$\}$. Show T is a **subgroup** of $\mathbb{R}$ (under addition of course) and then give a concrete counter-example which shows why T is **not** a sub**ring** of $\mathbb{R}$.

If T is not a subring, some part of the subring test must fail. T is a non-empty subset of $\mathbb{R}$, so no help there. Suppose $a + b\sqrt{5}, m + n\sqrt{5} \in T$ [where $a, b, m, n \in \mathbb{Z}$ and a & m are even]. Then $(a + b\sqrt{5}) - (m + n\sqrt{5}) = (a - m) + (b - n)\sqrt{5} \in T$ since $a - m, b - n \in \mathbb{Z}$ and $a - m$ is even since a and m are even. So T is closed under subtraction. Again, no help there. It must be that T is not closed under multiplication. $(a + b\sqrt{5})(m + n\sqrt{5}) = (am + 5bn) + (an + bm)\sqrt{5}$ which might not be in T since it isn't necessarily true that $am + 5bn$ is even. Let's come up with a counter-example. We need to make $am + 5bn$ odd, using integers a, b, m, n and where a & m are even. The easiest choice is $a = m = 0$ and $b = n = 1$.

T is not a subring: $\sqrt{5} = 0 + 1\sqrt{5} \in T$ but $\sqrt{5} \cdot \sqrt{5} = 5 = 5 + 0\sqrt{5} \notin T$. Therefore, T is not closed under multiplication hence T is not a subring of $\mathbb{R}$.

3. (13 points) Calculatin' mod 50. [$\mathbf{50 = 2 \cdot 5^2}$]

(a) Is 3 a unit, zero divisor, or neither in $\mathbb{Z}_{50}$? If 3 is a unit, find its inverse. If 3 is zero divisor, show this by finding some $0 \neq m \in \mathbb{Z}_{50}$ such that $3m = 0 \pmod{50}$.

The gcd of 3 and 50 is 1, thus $3x \equiv 1 \bmod 50$ has a solution and thus 3 is a unit in $\mathbb{Z}_{50}$. We need to find 3^{-1} (i.e. we need to solve the congruence $3x \equiv 1 \bmod 50$). We can either guess until we find the right answer, or better yet, run the Euclidean algorithm.

50 divided by 3 gives $50 = 3 \cdot 16 + 2$. 3 divided by 2 gives $3 = 2 \cdot 1 + 1$. 2 is evenly divisible by 1, so the algorithm ends and we find that 1 is the gcd (which we already knew). Now we are left with the equations: $(1)50 + (-16)3 = 2$ and $(1)3 + (-1)2 = 1$. Subbing $(1)50 + (-16)3$ in for 2 in the second equation, we find that $(1)3 + (-1)[(1)50 + (-16)3] = 1$ so that $(17)3 + (-1)50 = 1$.

Answer: In $\mathbb{Z}_{50}$, 3 is a unit and $3^{-1} = 17$.

(b) Is 20 a unit, zero divisor, or neither in $\mathbb{Z}_{50}$? If 20 is a unit, find its inverse. If 20 is zero divisor, show this by finding some $0 \neq m \in \mathbb{Z}_{50}$ such that $20m = 0 \pmod{50}$.

Obviously 20 and 50 are **not** relatively prime. Therefore, 20 is not a unit, so it must be a zero divisor. The least common multiple of 20 and 50 is 100. $20 \cdot 5 = 100 \equiv 0 \bmod 50$.

Answer: In $\mathbb{Z}_{50}$, 20 is a zero divisor. In fact, $20 \neq 0$ and $5 \neq 0$, but $20 \cdot 5 = 0$.

(c) Find all of the principle ideals of $\mathbb{Z}_{50}$.

We know that in $\mathbb{Z}_n$, principle ideals, subrings, subgroups, and cyclic subgroups are all the same. So to finding principle ideals is the same as finding cyclic subgroups. This is done by considering all of the divisors of 50. They are: 1, 2, 5, 10, 25, and 50. There is a unique cyclic subgroup of order k (for each divisor k of n) and it is generated by ℓ where $k \cdot \ell = n$. So the cyclic subgroup of order 1 is generated by $50 = 0$, order 2 is generated by 25, order 5 is generated by 10, order 10 is generated by 5, order 25 is generated by 2, and order 50 is generated by 1 (of course this is the whole ring $\mathbb{Z}_{50}$).

Answer: The principle ideals of $\mathbb{Z}_{50}$ are $(0) = \{0\}$, $(25) = \{0, 25\}$, $(10) = \{0, 10, 20, 30, 40\}$, $(5) = \{0, 5, 10, \ldots, 45\}$, $(2) = \{0, 2, 4, \ldots, 48\}$, and $\mathbb{Z}_{50}$.

(d) How many elements generate $\mathbb{Z}_{50}$?
[That is: How many $x \in \mathbb{Z}_{50}$ are there such that $(x) = \langle x \rangle = \mathbb{Z}_{50}$?]

This is asking, "How many elements of order 50 are contained in $\mathbb{Z}_{50}$?". Let's make a table to help figure out how many elements of each order there are.

Order =	1	2	5	10	25	50
Number of elements =	1	1	4	4	20	20

There is only 1 element of order 1 (the identity). Any element of order 2 will generate a subgroup of order 2. There is a unique subgroup of order k for each divisor k, so there is only 1 subgroup of order 2. This subgroup contains the identity and so the remaining $2 - 1 = 1$ element is of order 2. In a similar manner, taking out the identity leaves $5 - 1 = 4$ elements of order 5 in the unique subgroup of order 5. Now 1, 2, 5, and 10 all divide 10. Taking out the elements of order 1, 2, and 5 leaves $10 - 4 - 1 - 1 = 4$ elements of order 10. Next, 1, 5, and 25 divide 25 so taking out the elements of order 1 and 5 leaves $25 - 4 - 1 = 20$ elements of order 25. Finally, taking out all of the elements of lower order leaves $50 - 20 - 4 - 4 - 1 - 1 = 20$ elements of order 50.

Alternatively, if we know about Euler's totient φ-function: $\varphi(50) = \varphi(2 \cdot 5^2) = \varphi(2)\varphi(5^2)$
$= 2^0(2-1)5^1(5-1) = 20$.

Another alternative is to enumerate all of the elements of $U(50) = \{k \in \mathbb{Z}_{50} \mid (k, n) = 1\}$ since $U(50)$ is the set of generators of $\mathbb{Z}_{50}$.

Answer: There are 20 generators in $\mathbb{Z}_{50}$.

4. (15 points) The set $I = (4) = \{0, 4, 8, 12, 16\}$ is an ideal of $\mathbb{Z}_{20}$. Let $R = \mathbb{Z}_{20}/I$

(a) Write down all of the distinct cosets of I in $\mathbb{Z}_{20}$.

$0 + I = \{0, 4, 8, 12, 16\}$, $1 + I = \{1, 5, 9, 13, 17\}$, $2 + I = \{2, 6, 10, 14, 18\}$, and $3 + I = \{3, 7, 11, 15, 19\}$.

(b) Finish filling out the following addition and multiplication tables for R:

For example: $(2 + I) + (3 + I) = (2 + 3) + I = 5 + I = 1 + I$ (since 1 and 5 both belong to $1 + I$). Also, $(2 + I)(3 + I) = 2(3) + I = 6 + I = 2 + I$ (since 6 and 2 both belong to $2 + I$).

$+$	$0+I$	$1+I$	$2+I$	$3+I$
$0+I$	$0+I$	$1+I$	$2+I$	$3+I$
$1+I$	$1+I$	$2+I$	$3+I$	$0+I$
$2+I$	$2+I$	$3+I$	$0+I$	$1+I$
$3+I$	$3+I$	$0+I$	$1+I$	$2+I$

$\times$	$0+I$	$1+I$	$2+I$	$3+I$
$0+I$	$0+I$	$0+I$	$0+I$	$0+I$
$1+I$	$0+I$	$1+I$	$2+I$	$3+I$
$2+I$	$0+I$	$2+I$	$0+I$	$2+I$
$3+I$	$0+I$	$3+I$	$2+I$	$1+I$

(c) Fill out the following table of information about R.

R **has a "unity"?** Yes. $1+I$ is the multiplicative identity.

R **is commutative?** Yes. $\mathbb{Z}_{20}$ is commutative. Thus any quotient is as well. Or just look at the multiplication table.

R **is an integral domain?** No. $(2+I)(2+I) = 0+I$, so $2+I$ is a zero divisor. Thus R is not an integral domain.

R **is a field?** No. Since R isn't an integral domain, it can't be a field [since Field $\Rightarrow$ Integral Domain]. Or notice that $2+I$ has no (multiplicative) inverse, so it isn't a unit. Thus not all non-zero elements are units.

(d) Fill out the following table concerning R.

Zero Divisors	I am a zero divisor because...
$2+I$	$(2+I)(2+I) = 0+I$

Units	My multiplicative inverse is...
$1+I$	$(1+I)^{-1} = 1+I$ since $(1+I)(1+I) = 1+I$
$3+I$	$(3+I)^{-1} = 3+I$ since $(3+I)(3+I) = 1+I$

5. (12 points) Homomorphisms.

(a) Show $\varphi : \mathbb{Z}_3 \to \mathbb{Z}_6$ defined by $\varphi(x) = 2x$ is a **well-defined** homomorphism.

Suppose $x = y$ in $\mathbb{Z}_3$. This implies that $x = y + 3k$ for some $k \in \mathbb{Z}$. Thus $2x = 2y + 6k$, so $2x = 2y$ in $\mathbb{Z}_6$. Thus $x = y$ implies that $\varphi(x) = \varphi(y)$, so φ is well-defined. Next, $\varphi(x+y) = 2(x+y) = 2x + 2y = \varphi(x) + \varphi(y)$ thus φ is a homomorphism. [**Note:** The word "group" should be added to the problem statement. φ is a *group* homomorphism. If we check $\varphi(xy) = 2xy \neq 2x2y = \varphi(x)\varphi(y)$, we see that φ is **not** a ring homomorphism.]

(b) Find the kernel and image of φ. Is φ one-to-one? onto? an isomorphism?

$$\begin{array}{ccc} & \varphi & \\ 0 & \mapsto & 2 \cdot 0 = 0 \\ 1 & \mapsto & 2 \cdot 1 = 2 \\ 2 & \mapsto & 2 \cdot 2 = 4 \end{array}$$

Answer: $\text{Ker}(\varphi) = \{0\}$ thus φ is one-to-one, and $\varphi(\mathbb{Z}_3) = \{0, 2, 4\}$ thus φ is not onto. Since φ is not onto, it isn't an isomorphism.

(c) $S = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \,\middle|\, a, b \in \mathbb{R} \right\}$ is a subring of $M_2(\mathbb{R}) = \mathbb{R}^{2\times 2}$. Define $\psi : S \to \mathbb{R}$ by $\psi\left(\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}\right) = a$. Show that ψ is a ring homomorphism.

$$\psi\left(\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} + \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}\right) = \psi\left(\begin{bmatrix} a+c & 0 \\ 0 & b+d \end{bmatrix}\right) = a + c = \psi\left(\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}\right) + \psi\left(\begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}\right)$$

$$\psi\left(\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \cdot \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}\right) = \psi\left(\begin{bmatrix} ac & 0 \\ 0 & bd \end{bmatrix}\right) = ac = \psi\left(\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}\right)\psi\left(\begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}\right)$$

(d) Find the kernel and image of ψ. Is ψ one-to-one? onto? an isomorphism?

Suppose $\psi\left(\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}\right) = a = 0$. Thus $\mathrm{Ker}(\psi) = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & b \end{bmatrix} \,\middle|\, b \in \mathbb{R} \right\}$. Thus ψ is not one-to-one.

Next, given $a \in \mathbb{R}$, we have that $A = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \in S$ and $\psi(A) = a$. Thus $\psi(S) = \mathbb{R}$ and so ψ is onto.

ψ is not an isomorphism since ψ is not one-to-one.

6. (12 points) Some random proofs.

(a) Let R be a ring with 1. Let u be a unit of R. Show that u cannot be a zero divisor. (This shows that all fields are integral domains.)

u is a unit, so u^{-1} exists. Suppose that $ua = 0$ then $a = u^{-1}ua = u^{-1}0 = 0$ and so $a = 0$. Likewise, $au = 0$ implies that $a = auu^{-1} = 0u^{-1} = 0$ and so $a = 0$. Therefore, to get $au = 0$ or $ua = 0$ we must have $a = 0$. Thus u is not a zero-divisor. [*Note:* We need to check both $ua = 0 \Rightarrow a = 0$ **and** $au = 0 \Rightarrow a = 0$ to establish that u is not a zero divisor. The first computation verifies u is not a left zero-divisor and the second shows u is not a right zero-divisor.]

Remark: The parenthetical comment follows because a field is a commutative ring with $1 \neq 0$ such that all non-zero elements are units and thus no non-zero element can be a zero divisor. Therefore, all fields are integral domains.

(b) Let R be a commutative ring with 1. Suppose $a \in R$ and recall that $(a) = \{ra \,|\, r \in R\}$ is the principle ideal generated by a. Prove that (a) is an ideal of R.

First, $1a = a \in (a)$ so (a) is a *non-empty* subset of R. We need to check (a) is closed under subtraction and absorbs multiplication on the left and right.

Suppose $x, y \in (a)$ and $r \in R$. Then $x = sa$ and $y = ta$ for some $s, t \in \mathbb{R}$. $x - y = sa - ta = (s-t)a \in (a)$, so (a) is closed under subtraction. Also, using commutativity we have that $xr = rx = (rs)a \in (a)$, so (a) absorbs multiplication on both sides.

Therefore, $(a) \lhd R$.

(c) Let G be a group such that $(xy)^{-1} = x^{-1}y^{-1}$ for all $x, y \in G$. Show that G is abelian.

Let $x, y \in G$. Then $(x^{-1}y^{-1})^{-1} = (y^{-1})^{-1}(x^{-1})^{-1} = yx$ by the "socks-shoes" law and $(x^{-1}y^{-1})^{-1} = (x^{-1})^{-1}(y^{-1})^{-1} = xy$ by assumption. Therefore, $xy = (x^{-1}y^{-1})^{-1} = yx$, so G is abelian.

Alternatively, $x^{-1}y^{-1} = (xy)^{-1} = y^{-1}x^{-1}$ (first equals is our assumption and second equals is "socks-shoes"). Thus $x^{-1}y^{-1} = y^{-1}x^{-1}$. Multiply both sides by yx on the left and get $e = yy^{-1} = yxx^{-1}y^{-1} = yxy^{-1}x^{-1}$. So $e = yxy^{-1}x^{-1}$. Now multiply both sides by xy on the right and get $exy = yxy^{-1}x^{-1}xy = yxy^{-1}y = yx$. Thus $xy = yx$, so G is abelian.

7. (12 points) Just a little harmless permuting.

(a) Let $H = \{(1), (12)\}$. Find all of the **left and right** cosets of H in $S_3 = \{(1), (12), (13), (23), (123), (132)\}$. Is H a normal subgroup?

The left cosets of H are:

- $H = \{(1), (12)\}$
- $(13)H = \{(13)(1), (13)(12)\} = \{(13), (123)\}$
- $(23)H = \{(23)(1), (23)(12)\} = \{(23), (132)\}$

The right cosets of H are:

- $H = \{(1), (12)\}$
- $H(13) = \{(1)(13), (12)(13)\} = \{(13), (132)\}$
- $H(23) = \{(1)(23), (12)(23)\} = \{(23), (123)\}$

H is **not** a normal subgroup since $(12)H \neq H(12)$ (not all of the left and right cosets are equal).

(b) Explain why A_n (the even permutations) is a normal subgroup of S_n. [Hint: You may either briefly explain *why it is a subgroup* **and** *why it is normal*, or you can find a homomorphism with kernel A_n.]

A_n is a finite (non-empty) subset of S_n (for example, $(1) \in A_n$). So to check it's a subgroup we only need to check closure (checking inverses is unnecessary since A_n is finite). Recall that even with even is even. Thus A_n is closed under the operation and thus is a subgroup. Next, let $\sigma \in S_n$ and $\tau \in A_n$. If σ is odd, then so is σ^{-1} so that $\sigma\tau\sigma^{-1}$ is odd with even with odd which is even. Thus $\sigma\tau\sigma^{-1} \in A_n$. Similarly for σ even. Thus A_n absorbs conjugates and so $A_n \lhd S_n$.

Alternately, $\text{sgn} : S_n \to \{\pm 1\}$ defined by $\text{sgn}(\sigma) = 1$ if σ is even and -1 if σ is odd — this is the sign homomorphism. It's kernel is all permutations with sign equal to 1 which is exactly the even permutations. So long story short $\text{Ker}(\text{sgn}) = A_n$ and thus $A_n \lhd S_n$.

(c) Consider the quotient group S_n/A_n. It this a cyclic group? Why or why not?

Yes. Notice that the index of A_n in S_n is 2 (one coset is the even permutations and one coset is the odd permutations, or $n!/(n!/2) = 2$) — by the way — index $= 2$ implies normal, so yet another reason A_n is a normal subgroup. Thus the quotient group has order 2 (which is prime) thus is cyclic (and isomorphic to $\mathbb{Z}_2$).

Alternatively you could write down the Cayley table for the quotient and see that you get a cyclic group of order 2 or using the first isomorphism theorem we know that $S_n/A_n = S_n/\text{Ker}(\text{sgn}) \cong \{\pm 1\} = \langle -1 \rangle$ which, again, is cyclic (order 2).

8. (12 points) D_{10}. $n = 10$ really? why oh why?

(a) Let G be a **non-abelian** group of order 20. What are possible orders of elements of G? What does "non-abelian" rule out and why?

Lagrange's theorem says that the order of an element must divide the order of the group. So Lagrange alone says that the possible orders are 1, 2, 4, 5, 10, and 20. However, if there were any elements of order 20, we would have a cyclic group which would imply that we have an abelian group. Since our group is non-abelian, we must not have any elements of order 20.

Answer: The possible orders of elements are 1, 2, 4, 5, and 10. 20 is ruled out by "non-abelian" (hence "not cylic").

(b) Half of the elements of D_{10} are reflections and half are rotations. In fact, the **rotations** in D_{10} form a **cyclic subgroup**. Without worrying about the cyclic part, **briefly** explain why the rotations do form a subgroup and why the reflections do not.

Since the reflections form a finite (non-empty) subset of D_{10} we just need to check closure to confirm that the rotations form a subgroup. But we know that a rotation composed with a rotation is a rotation. Thus the rotations in D_{10} form a subgroup of D_{10}.

On the other hand, a reflection composed with a reflection is a rotatation (not a reflection), so the set of reflections is **not closed** under the operation. Thus reflections do not form a subgroup.

Remark: Why do the rotations form a **cyclic** subgroup? Well, suppose that $R_\theta \in D_n$ is a rotation of θ degrees where θ is as small as possible (without being zero). Then take any other rotation, say $R_\alpha \in D_n$ (a rotation of α degrees). We can divide α by θ so we get $\alpha = m\theta + r$ where $m \in \mathbb{Z}$ and $0 \leq r < \theta$. Now since D_n is closed under composition, $R_r = R_\alpha \circ (R_\theta)^{-m} \in D_n$. But R_θ was a rotation of smallest (non-zero) degree. Therefore, $r = 0$ and so $\alpha = m\theta$ and thus $R_\alpha = (R_\theta)^m$. So all of the rotations are generated by R_θ.

(c) Use the description of D_{10} given in part (b) to determine the number of elements of each order in D_{10}.

D_{10} has 20 elements. Half of them are reflections. We know that reflections are their own inverses, so these 10 elements all have order 2.

Next, the rotations form a cyclic subgroup of order 10. Thus the rotations are isomorphic to $\mathbb{Z}_{10}$. We know that there is 1 identity. Then $2 - 1 = 1$ element of order 2. 1 and 5 are the only divisors of 5, so there are $5 - 1 = 4$ elements of order 5. And finally, 1, 2, 5, and 10 all divide 10, so there are $10 - 4 - 1 - 1 = 4$ elements of order 10. Putting this together we have that...

Element order =	1	2	5	10	20
Number of elements with that order =	1	11	4	4	0