Math 210A, Exam 1, 2009

1. *Give an example of each of the following . You do not need to justify your answer.*
(a) *An element in S_5 of order 6.*

Answer: $(12)(345) \in S_5$ such that $\circ(12)(345) = 6$.

(b) A homomorphism from S_n onto $\mathbb{Z}_2$.

Answer: Define $f: S_n \to \mathbb{Z}_2$ by $f(\sigma) = \begin{cases} 0 \text{ if } \operatorname{sgn}(\sigma) = -1 \\ 1 \text{ if } \operatorname{sgn}(\sigma) = 1 \end{cases}$

(c) An infinite group in which all elements have finite order.

Answer: $\mathbb{Q}/\mathbb{Z}$ is an infinite group in which all elements have finite order.

2. *Let $\sigma = (25)(134) \in S_7$ and $\tau = (23)(567) \in S_7$.*
(a) *Find $\gamma \in S_7$ such that $\tau = \gamma\sigma\gamma^{-1}$.*

Answer: (1536)(47)(2)

Proof:
Since τ is a conjugate of σ and conjugate permutations have the same cycle structure, then $(\gamma(2)\gamma(5))(\gamma(1)\gamma(3)\gamma(4)) = (23)(567)$.

This gives us the following permutation $\begin{pmatrix} 1234567 \\ 5267314 \end{pmatrix}$, or equivalently, (1536)(47)(2).

We can verify that $\tau = \gamma\sigma\gamma^{-1}$ as $(2)(74)(6351)(25)(134)(1536)(47)(2) = (23)(567)$.

(b) *Determine, with explanation, the number of conjugates of σ in S_7.*

Answer: There are 420 conjugates of σ in S_7.

Proof:
The cycle structure of σ is (12)(345).

All conjugates in S_7 will have the same cycle structure.

$\therefore$ There are $\frac{\underline{7} \bullet \underline{6}}{2} \bullet \frac{\underline{5} \bullet \underline{4} \bullet \underline{3}}{3} = 21 \bullet 20 = 420$ conjugates of σ in S_7.

Math 210A, Exam 1, 2009

3. (a) *Let Z be the center of the group G. Prove that if G/Z is cyclic, then G is abelian.*

Proof:

Let $x, y \in G$. Since G/Z is cyclic, then $G/Z = \langle aZ \rangle$ for some $a \in G$.

And $xZ = a^iZ$, $yZ = a^jZ$ for some positive integers i, j.

Since $1 \in Z$, then $x \bullet 1 \in xZ$ and $y \bullet 1 \in yZ$.

Thus, $x = a^ic$ and $y = a^jd$ for some $c, d \in Z$.

Note that c and d commute with all elements of G by definition of center.

So then $xy = a^ic \bullet a^jd = a^ia^jcd = a^{i+j}dc = a^{j+i}dc = a^ja^idc = a^jda^ic = yx$.

$\therefore$ G is abelian.

(b) Let G be a nonabelian group of order pq, where p and q are primes.
Prove that $G \cong \text{Inn}(G)$, where $\text{Inn}(G)$ is the inner automorphism group of G.

Proof:

Let p, q be primes. Let G be a group such that $|G| = pq$.

We can conclude $p \neq q$, otherwise $|G| = p^2$ which would imply G is abelian.

Let $g \in G$. Define $\gamma_g: G \to G$ by $\gamma_g(x) = gxg^{-1}$.

By definition $\text{Inn}(G) = \{\gamma_g : g \in G\}$.

Define $\varphi: G \to \text{Inn}(G)$ by $\varphi(g) = \gamma_g$.

Claim: $G \cong \text{Inn}(G)$.

To show φ is a homomorphism, let $a, b \in G$ and note that

$\varphi(ab) = \gamma_{ab} = \gamma_a\gamma_b = \varphi(a)\varphi(b)$ since $\gamma_{ab} = abxb^{-1}a^{-1} = a\gamma_b a^{-1} = \gamma_a\gamma_b$.

To show $\ker \varphi = \{e\}$, we will show that every element of $\ker \varphi$ is also an element of the center of G and that $|Z(G)| = 1$.

Note that $\ker \varphi = \{g \in G : \varphi(g) = \gamma_g = e_{\text{Inn}(G)}\}$.

And $\gamma_g = e_{\text{Inn}(G)} \Rightarrow \forall\, x \in G, \gamma_g(x) = gxg^{-1} = x$.

Let $k \in \ker \varphi$. Then $\forall\, x \in G$, $kxk^{-1} = x$.

That is, k commutes with every element of G. Thus, $k \in \text{Z}(G)$.

Since G is not abelian, then $\text{Z}(G) \neq G$.

Since $\text{Z}(G) \leq G$, then $|\text{Z}(G)| \mid |G| = pq$. Thus, $|\text{Z}(G)| = 1$, p, or q.

If $|\text{Z}(G)| = p$ or q, then $|G/\text{Z}(G)| = q$ or p, hence $G/(\text{Z}(G)$ is cyclic as p, q are prime.

Then by part (a) G is abelian, contrary to our assumption.

Thus, $|\text{Z}(G)| = 1$. Or equivalently, $\text{Z}(G) = \{e\} = \ker \varphi$.

$\therefore$ $\text{G} \cong \text{Inn}(G)$.

4. Let $\varphi: G \to G'$ be a homomorphism.
(a) Prove that if $g \in G$ and g has finite order, then $\circ(\varphi(g))$ divides $\circ(g)$.

Proof:
Let $g \in G$ such that $|g| = n < \infty$.

Then by homomorphism properties, $e_{G'} = \varphi(e_G) = \varphi(g^n) = (\varphi(g))^n$.

Since $a^n = 1 \Rightarrow \circ(a) \mid n$, then $\circ(\varphi(g)) \mid n = \circ(g)$.

(b) Prove that if $(|G|, |G'|) = 1$, then $\varphi(x) = 1$ for all $x \in G$.

Proof:
Let $x \in G$. Then by part (a) $\circ(\varphi(x)) \mid \circ(x)$.

By corollary to Lagrange's Theorem, $\circ(x) \mid |G|$ and $\circ(\varphi(x)) \mid |G'|$.

Hence $\circ(\varphi(x)) \mid |G|$ and $\circ(\varphi(x)) \mid |G'|$.

Since $(|G|, |G'|) = 1$ then $\circ(\varphi(x)) = 1$, by Euclid's Lemma.

Thus $1 = (\varphi(x))^1 = \varphi(x)$.

5. Let G be a finite group with $K \lhd G$. If $(|K|, [G:K]) = 1$, prove that K is the unique subgroup of G having order $|K|$.

Proof:
Suppose $\exists\, K'$ such that $K' \lhd G$ and $|K'| = |K|$.

Let $x \in K'$.

Since $K \lhd G$, G/K is a group and we can define $\pi: G \to G/K$ by $\pi(g) = gK$.

Then by 4(a) $\circ(xK) \mid \circ(x)$.

By corollary to Lagrange's Thm, $\circ(x) \mid |K'| = |K|$ and $\circ(xK) \mid |G/K| = [G:K]$.

Since $\circ(xK) \mid \circ(\text{x})$ and $\circ(x) \mid |K|$, we have $\circ(xK) \mid |K|$.

Thus $\circ(xK) \mid [G:K]$ and $\circ(xK) \mid |K|$.

By Euclid's Lemma, $(|K|, [G:K]) = 1 \Rightarrow \circ(xK) = 1$.

$\therefore$ $xK = K$, which implies $x \in K$. Hence $K' \subseteq K$. And since $|K'| = |K|$, then $K' = K$.

6. Prove that there does not exist a homomorphism from S_3 onto $\mathbb{Z}_3$.

Proof:
Note that the elements S_3 and $\mathbb{Z}_3$ and orders of each are

S_3	Order	$\mathbb{Z}_3$	Order
(1)	1	0	1
(12)	2		
(23)	2		
(13)	2		
(123)	3	1	3
(132)	3	2	3

Suppose $\exists\ \varphi: S_3 \to \mathbb{Z}_3$ such that φ is surjective.

Let $A = \langle(12)\rangle$. Then $A \leq S_3$ and $|A| = 2$.

Since $\varphi(A) \leq \mathbb{Z}_3$, then Lagrange's Theorem gives us that $|\varphi(A)| \mid |\mathbb{Z}_3| = 3$.

Since $|A| = 2$, then $|\varphi(A)| = 1$ (otherwise φ would not be well-defined.)

Thus $\varphi(A) = 1$ (as $(1) \in A$ and $\varphi(1) = 1$ by homomorphism properties).

So then $\varphi((12)) = 1$. Thus $\varphi((132)) = \varphi((12)(13)) = \varphi((12))\varphi((13)) = \varphi((13))$.

By 4(a) above $\circ(\varphi(13))|\circ(13) = 2$ and $\circ(\varphi(132))|\circ(132) = 3$.

So then $\varphi((132)) = \varphi((13)) \Rightarrow \circ\varphi(13) = \circ\varphi(132) = 1$.

And since $(123) = (23)(13)$, we have $\circ\varphi(23) = \circ\varphi(123) = 1$ by similar argument.

Thus $\varphi(S_3) = 1$, contrary to our assumption that φ is surjective.

$\therefore$ There is no homomorphism from S_3 onto $\mathbb{Z}_3$.

7. *Let $H \leq S_n$. Let $K = \{\sigma \in H \mid \sigma \text{ is even}\}$.*

(a) *Prove that $K \leq S_n$.*

Proof:

$(1) \in K$ as (1) is even.

Let $\alpha, \beta \in K$ where α is an r-cycle and β is a t-cycle.

Then $\beta^{-1} \in K$ as β^{-1} has the same cycle structure as β.

Since α and β are even, then $\text{sgn}(\alpha) = (-1)^{n-r} = (-1)^{2j}$ where $2j = n - r$ and

$\text{sgn}(\beta) = (-1)^{n-t} = (-1)^{2k}$ where $2k = n - t$.

So $\text{sgn}(\alpha\beta^{-1}) = \text{sgn}(\alpha)\text{sgn}(\beta^{-1}) = (-1)^{2j}(-1)^{2k} = 1$, hence $\alpha\beta^{-1} \in K$.

$\therefore\ K \leq S_n$.

(b) *Prove that $K \lhd H$.*

Proof:

Let $\alpha \in H$. Let $\beta \in K$.

Since $\alpha\beta\alpha^{-1}$ has the same cycle structure as β, then $\alpha\beta\alpha^{-1}$ is even.

Thus $\alpha\beta\alpha^{-1} \in K$.

$\therefore\ K \lhd H$.

(c) *Prove that if $K \neq H$, then $|K| = \frac{1}{2}|H|$.*

Proof:

Assume $K \neq H$. Let $\alpha \in H - K$.

Since $\alpha \notin K$, then K and αK are disjoint.

Let $\gamma \in H$. If γ is even, then $\gamma \in K$.

If γ is odd, then $\alpha^{-1}\gamma$ is even (as α and α^{-1} have the same parity), hence $\alpha^{-1}\gamma \in K$.

This gives us that $\gamma \in \alpha K$.

Note that $\alpha K \subseteq H$ by closure.

Thus $H = K \cup \alpha K$. Hence $|H| = |K| + |\alpha K| = 2|K|$ (as $|K| = |\alpha K|\ \forall\ \alpha \in H$).

$\therefore\ |K| = \frac{1}{2}|H|$.