Chapter 5

8. Show that A_8 contains an element of order 15.

To get an element of order 15, take the product of a 3-cycle and a 5-cycle that are disjoint (there is just enough room to do this since $3+5=8$). This product will be even because the 3-cycle can be written as a product of 2 transpositions and the 5-cycle as a product of 4 transpositions, so the full product is a product of 6 transpositions, hence even.
An explicit element is $(123)(45678)$.

11. Determine whether the following permutations are even or odd:

(a) $(135) = (13)(35) \longrightarrow$ even

(b) $(1356) = (13)(35)(56) \longrightarrow$ odd

(c) $(13567) = (13)(35)(56)(67) \longrightarrow$ even

(d) $(12)(134)(152) = (15)(234) = (15)(23)(34) \longrightarrow$ odd

(e) $(1243)(3521) = (1)(2)(354) = (35)(54) \longrightarrow$ even

15. Let $n \in \mathbb{Z}^+$. If n is odd, an n-cycle is an <u>even</u> permutation since it can be written as a product of $n-1$ transpositions, and $n-1$ is even. If n is even, an n-cycle is an <u>odd</u> permutation since it can be written as a product of $n-1$ transpositions, and $n-1$ is odd.

17. The set of even permutations A_n is a subgroup of S_n.

<u>Proof</u> The identity is a product of 0 transpositions, and 0 is even, so $(1) \in A_n$. Let $\alpha \in A_n$ be written as a product of an even number of transpositions. Since the inverse of a transposition is itself, α^{-1} can be written as the same product of an even number of transpositions, so $\alpha^{-1} \in A_n$. Let $\alpha, \beta \in A_n$ where α is a product of m transpositions, β is a product of n transpositions, and m, n are both even. Then $\alpha\beta$ is a product of $m+n$ transpositions, and m, n even $\Rightarrow m+n$ is even. Thus, $\alpha\beta \in A_n$, and $A_n \leq S_n$. ▨

19. Let $\alpha, \beta \in S_n$. Prove that $\alpha\beta$ is even iff $\alpha + \beta$ are both even or both odd.

<u>Proof</u> Let α be a product of m transpositions and β be a product of n transpositions, so that $\alpha\beta$ is a product of $m+n$ transpositions. Then

$$\alpha\beta \text{ is even} \iff m+n \text{ is even} \iff m+n \text{ are either both even or both odd}$$
$$\iff \alpha + \beta \text{ are either both even or both odd.}$$ ▨

25. Give two reasons why the set of odd permutations in S_n is not a subgroup.

First, $(1) \in A_n$ so this set does not contain the identity (1) of S_n. Secondly, the set is not closed under products: if $\alpha, \beta \in S_n$ are odd, then $\alpha\beta$ is even by #19.

27. Use Table 5.1 to compute the following.

(a) Centralizer in A_4 of $\alpha_3 = (13)(24) = \{\alpha_i \in A_4 \mid \alpha_i\alpha_3 = \alpha_3\alpha_i\}$
$= \{(1), (12)(34), (13)(24), (14)(23)\}$

(b) Centralizer in A_4 of $\alpha_{12} = (124) = \{\beta \in A_4 \mid \beta\alpha_{12} = \alpha_{12}\beta\}$
$= \{(1), (142), (124)\}$

39. How many elements of order 5 are there in A_6?

The only elements of order 5 in A_6 are 5-cycles since there is not enough room to have two disjoint 5-cycles ($5+5=10>6$), and these are even since they can be written as a product of 4 transpositions. To count the number of 5-cycles, there are 6 choices for 1st cycle entry, 5 choices for 2nd entry, etc., but need to divide by 5 since there are 5 ways to choose the 1st entry of the same 5-cycle. So there are $\frac{6\cdot5\cdot4\cdot3\cdot2}{5} = 6\cdot4\cdot3\cdot2 = \boxed{144}$ elements of order 5 in A_6.

Chapter 6

1. Find an isomorphism $(\mathbb{Z}, +) \to (2\mathbb{Z}, +)$.

Let $\phi(x) = 2x$. Then $\phi(x) = \phi(y) \Rightarrow 2x = 2y \Rightarrow x = y$, so ϕ is injective, and given any $y \in 2\mathbb{Z}$, $\exists\, x \in \mathbb{Z}$ s.t. $y = 2x = \phi(x)$, so ϕ is surjective. ϕ also preserves the group operation since $\phi(x+y) = 2(x+y) = 2x + 2y = \phi(x) + \phi(y)$. Thus, ϕ is an isomorphism.

2. Find $\mathrm{Aut}(\mathbb{Z})$.

Since $\mathbb{Z}$ is a cyclic group with 2 generators, any automorphism must send a generator to another generator. Therefore, $\mathrm{Aut}(\mathbb{Z})$ has two elements: the identity map (sending $1 \mapsto 1$) and the map ϕ given by $\phi(a) = -a \;\; \forall a \in \mathbb{Z}$ (sending $1 \mapsto -1$).

4. Show that $U(8) \ncong U(10)$.

Note that $U(10) = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\} = \langle\bar{3}\rangle$ is cyclic, but $U(8) = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ is not cyclic since every nonidentity element has order 2. Thus, there cannot be an isomorphism between $U(8)$ and $U(10)$.

5. Show that $U(8) \cong U(12)$.

Recall $U(8) = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ and $U(12) = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}\}$. Let ϕ be the map sending $\phi(\bar{1}) = \bar{1}$, $\phi(\bar{3}) = \bar{5}$, $\phi(\bar{5}) = \bar{7}$, and $\phi(\bar{7}) = \bar{11}$. This map is clearly a bijection, so we show it preserves the group operation. If $K = 3, 5,$ or 7, then $\phi(\bar{K}) = \phi(\bar{K}\cdot\bar{1}) = \phi(\bar{K})\cdot\phi(\bar{1}) = \phi(\bar{K})\cdot\bar{1} = \phi(\bar{K})$. Since the groups are abelian, there are only 3 other products to check:

$\phi(\bar{3}\cdot\bar{5}) = \phi(\overline{15}) = \phi(\bar{7}) = \bar{11}$ and $\phi(\bar{3})\phi(\bar{5}) = \bar{5}\cdot\bar{7} = \overline{35} = \bar{11}$ ✓

$\phi(\bar{3}\cdot\bar{7}) = \phi(\overline{21}) = \phi(\bar{5}) = \bar{7}$ and $\phi(\bar{3})\phi(\bar{7}) = \bar{5}\cdot\bar{11} = \overline{55} = \bar{7}$ ✓

$\phi(\bar{5}\cdot\bar{7}) = \phi(\overline{35}) = \phi(\bar{3}) = \bar{5}$ and $\phi(\bar{5})\phi(\bar{7}) = \bar{7}\cdot\bar{11} = \overline{77} = \bar{5}$ ✓ ▨

6. Prove that isomorphism is an equivalence relation.

Proof Let G be a group and define $\phi: G \to G$ by $\phi(g) = g \ \forall g \in G$. It is clear that ϕ is a bijection, and if $g, h \in G$ then $\phi(gh) = gh = \phi(g)\phi(h)$, so ϕ is an isomorphism. Thus, $G \cong G$ and $\cong$ is reflexive.

Let G, H be groups with $G \cong H$. Then there is an isomorphism $\phi: G \to H$. By Thm 6.3 (1) [see HW #31 below], $\phi^{-1}: H \to G$ is also an isomorphism. Thus, $H \cong G$ and $\cong$ is symmetric.

Let G, H, K be groups with $G \cong H$ and $H \cong K$. Then there exist isomorphisms $\phi: G \to H$ and $\psi: H \to K$. Now $\psi\phi: G \to K$ is a map; by Thm 0.7(2) it is injective since ϕ & ψ are, and by Thm 0.7(3) it is surjective since ϕ and ψ are. Thus, $\psi\phi$ is a bijection. To show it preserves the group operations, let $g_1, g_2 \in G$. Then $\psi\phi(g_1 g_2) = \psi(\phi(g_1 g_2)) = \psi(\phi(g_1)\phi(g_2)) = \psi(\phi(g_1))\psi(\phi(g_2))$

$$= \psi\phi(g_1) \cdot \psi\phi(g_2).$$

Thus, $\psi\phi$ is an isomorphism, so $G \cong K$ and $\cong$ is transitive. Hence, $\cong$ is an equivalence relation. ▨

7. Prove that $S_4 \ncong D_{12}$.

Note that D_{12} has an element of order 12, the 30° CCW rotation that generates the subgroup of all rotations of D_{12}. However, S_4 has $\frac{4 \cdot 3 \cdot 2 \cdot 1}{4} = 6$ elements of order 4, $\frac{4 \cdot 3 \cdot 2}{3} = 8$ elements of order 3, $\frac{4 \cdot 3}{2} + \frac{6}{2} = 9$ elements of order 2, and the identity of order 1, so S_4 has no element of order 12. Thus, there cannot be an isomorphism between S_4 and D_{12}.

29. If ϕ and γ are isomorphisms from the cyclic group $\langle a \rangle$ to some group G and $\phi(a) = \gamma(a)$, prove that $\phi = \gamma$.

Proof Let $b \in \langle a \rangle$. Then $\exists K \in \mathbb{Z}$ s.t. $b = a^K$. Then since ϕ and γ are isomorphisms, we have

$$\phi(b) = \phi(a^K) = \phi(a)^K = \gamma(a)^K = \gamma(a^K) = \gamma(b).$$ Therefore, $\phi = \gamma$. ▨

31. Suppose that $\phi: G \to H$ is an isomorphism. Then $\phi^{-1}: H \to G$ is an isomorphism.

Proof If $h_1, h_2 \in H$ with $h_1 = h_2$, then $\exists g_1, g_2 \in G$ s.t. $\phi(g_1) = h_1 = h_2 = \phi(g_2)$ since ϕ is surjective. Then $g_1 = g_2$ since ϕ is injective. Thus, $\phi^{-1}(h_1) = \phi^{-1}(h_2)$, so ϕ^{-1} is a well-defined map.

Suppose now that $\phi^{-1}(h_1) = \phi^{-1}(h_2)$ for some $h_1, h_2 \in H$. Since ϕ is surjective, $\exists g_1, g_2 \in G$ s.t. $\phi(g_1) = h_1$, $\phi(g_2) = h_2$. Thus, $\phi^{-1}(\phi(g_1)) = \phi^{-1}(\phi(g_2)) \Rightarrow g_1 = g_2 \Rightarrow \phi(g_1) = \phi(g_2) \Rightarrow h_1 = h_2$. So ϕ^{-1} is injective. Let $g \in G$. Then $\phi^{-1}(\phi(g)) = g$, so ϕ^{-1} is surjective.

Finally, let $h_1, h_2 \in H$. Then by surjectivity of ϕ, $\exists g_1, g_2 \in G$ s.t. $\phi(g_1) = h_1$, $\phi(g_2) = h_2$. Thus, $\phi^{-1}(h_1 h_2) = \phi^{-1}(\phi(g_1)\phi(g_2)) = \phi^{-1}(\phi(g_1 g_2)) = g_1 g_2 = \phi^{-1}(h_1)\phi^{-1}(h_2)$.

Thus, ϕ^{-1} is an isomorphism. ▨

32. If $\phi: G \to H$ is an isomorphism and $K \leq G$, then $\phi(K) = \{\phi(k) \mid k \in K\} \leq H$.

Proof Note that $e_G \in K$ since $K \leq G$, and thus $e_H = \phi(e_G) \in \phi(K)$.

Assume that $\phi(k_1), \phi(k_2) \in \phi(K)$ for some $k_1, k_2 \in K$. Then $\phi(k_1)\phi(k_2) = \phi(k_1 k_2) \in \phi(K)$ since $K \leq G \Rightarrow k_1 k_2 \in K$. Finally, let $\phi(k) \in \phi(K)$ for some $k \in K$. Then $k^{-1} \in K$, so $\phi(k)^{-1} = \phi(k^{-1}) \in \phi(K)$. Hence, $\phi(K) \leq H$. ▨

48. Let $\phi: G \to H$ be an isomorphism and let $a \in G$. Prove that $\phi(C_G(a)) = C_H(\phi(a))$.

Proof Let $x \in C_G(a)$ so that $\phi(x) \in \phi(C_G(a))$. Then $xa = ax$, which implies $\phi(x)\phi(a) = \phi(xa) = \phi(ax) = \phi(a)\phi(x)$. Therefore, $\phi(x) \in C_H(\phi(a))$ and $\phi(C_G(a)) \subseteq C_H(\phi(a))$.

To show the reverse inclusion, let $h \in C_H(\phi(a))$. Since ϕ is surjective, $\exists g \in G$ s.t. $\phi(g) = h$. Then $h\phi(a) = \phi(a)h \Rightarrow \phi(g)\phi(a) = \phi(a)\phi(g) \Rightarrow \phi(ga) = \phi(ag)$. Since ϕ is injective, this implies $ga = ag$. Thus, $g \in C_G(a) \Rightarrow h = \phi(g) \in \phi(C_G(a))$. Therefore, $C_H(\phi(a)) \subseteq \phi(C_G(a))$. Combined with the above, we have $\phi(C_G(a)) = C_H(\phi(a))$. ▨

10. Let G be a group. Prove that $\alpha(g) = g^{-1}$ is an automorphism iff G is abelian.

Proof Suppose first that α is an automorphism, and let $x, y \in G$. Then $\alpha(xy) = \alpha(x)\alpha(y) \Rightarrow (xy)^{-1} = x^{-1}y^{-1} \Rightarrow e = x^{-1}y^{-1}xy \Rightarrow yx = xy$, so G is abelian.

Suppose now that G is abelian. Let $x, y \in G$ and assume $\alpha(x) = \alpha(y)$. Then $x^{-1} = y^{-1} \Rightarrow x^{-1}y = e \Rightarrow y = x$, so α is injective. If $x \in G$, then $\alpha(x^{-1}) = (x^{-1})^{-1} = x$, so α is surjective. Finally, for $x, y \in G$ we have

$$\begin{aligned} \alpha(xy) &= (xy)^{-1} = (yx)^{-1} && \text{since } G \text{ is abelian} \\ &= x^{-1}y^{-1} && \text{by Shoes-Socks} \\ &= \alpha(x)\alpha(y). && \text{Thus, } \alpha \text{ is an automorphism.} \end{aligned}$$ ▨

11. If $g, h \in G$, prove that $\phi_g \phi_h = \phi_{gh}$.

Proof To show that two functions are equal, we show they take an arbitrary element to the same image. Let $x \in G$. Then $\phi_g\phi_h(x) = \phi_g(\phi_h(x)) = \phi_g(hxh^{-1}) = g(hxh^{-1})g^{-1} = ghxh^{-1}g^{-1}$ and $\phi_{gh}(x) = ghx(gh)^{-1} = ghxh^{-1}g^{-1}$, so $\phi_g\phi_h = \phi_{gh}$. ▨

12. Find two groups G and H s.t. $G \ncong H$ but $\mathrm{Aut}(G) \cong \mathrm{Aut}(H)$.

Let $G = \mathbb{Z}_8$ and $H = \mathbb{Z}_{12}$. Certainly $G \ncong H$ since $|G| = 8 \neq 12 = |H|$. We know that $\mathrm{Aut}(\mathbb{Z}_8) \cong U(8)$ and $\mathrm{Aut}(\mathbb{Z}_{12}) \cong U(12)$. By problem #5, $U(8) \cong U(12)$, and since $\cong$ is an equivalence relation by #6, $\mathrm{Aut}(\mathbb{Z}_8) \cong U(8) \cong U(12) \cong \mathrm{Aut}(\mathbb{Z}_{12}) \Rightarrow \mathrm{Aut}(\mathbb{Z}_8) \cong \mathrm{Aut}(\mathbb{Z}_{12})$. (Other examples are possible.)

22. Let ϕ be an automorphism of the group G. Prove that $H = \{x \in G \mid \phi(x) = x\} \leq G$.

Proof Since $\phi: G \to G$ is an isomorphism, we know that $\phi(e) = e$. Thus, $e \in H$. Suppose $x, y \in H$. Then $\phi(x) = x$ and $\phi(y) = y$. Therefore, $\phi(xy) = \phi(x)\phi(y) = xy$, which implies $xy \in H$. Finally, suppose $x \in H$. Then $\phi(x) = x$ and $\phi(x^{-1}) = [\phi(x)]^{-1} = x^{-1}$, so $x^{-1} \in H$. Thus, $H \leq G$. ▨

35. Show that $\phi(a+bi) = a - bi$ is an automorphism of $(\mathbb{C}, +)$, and that ϕ also preserves complex multiplication.

Proof Let $a+bi, c+di \in \mathbb{C}$ and assume $\phi(a+bi) = \phi(c+di)$. Then $a - bi = c - di \Rightarrow a = c$ and $b = d$, so $a+bi = c+di$ and ϕ is injective. Let $a+bi \in \mathbb{C}$. Then $\phi(a-bi) = a - (-b)i = a+bi$, so ϕ is surjective. Let $a+bi, c+di \in \mathbb{C}$. Then

$$\phi(a+bi) + \phi(c+di) = a - bi + c - di = (a+c) - (b+d)i = \phi((a+c) + (b+d)i)$$
$$= \phi[(a+bi) + (c+di)], \text{ so } \phi \text{ preserves the operation.}$$

Hence, ϕ is an automorphism of $(\mathbb{C}, +)$. To show that ϕ preserves complex multiplication, let $a+bi, c+di \in \mathbb{C}$. Then $(a+bi)(c+di) = (ac - bd) + (ad + bc)i$ and

$$\phi(a+bi) \cdot \phi(c+di) = (a-bi)(c-di) = (ac - bd) - (ad+bc)i = \phi[(ac-bd) + (ad+bc)i]$$
$$= \phi[(a+bi)(c+di)], \text{ so } \phi \text{ also preserves multiplication.}$$ ▨

53. Let $a \in G$ and $|a| < \infty$. Let $\phi_a(x) = axa^{-1}$. Show that $|\phi_a|$ divides $|a|$, and find an element a from a group for which $1 < |\phi_a| < |a|$.

Proof Let $|a| = n$. To show that $|\phi_a|$ divides n, it suffices to show that ϕ_a^n is the identity map. For any $x \in G$, we have $\phi_a^n(x) = \phi_a^{n-1}(axa^{-1}) = \phi_a^{n-2}(a^2xa^{-2})$
$= a^n x a^{-n} = exe = x$, so $\phi_a^n = id.$ and $|\phi_a|$ divides n.

Let $G = D_4$ and $a = R_{90}$. Then $1 < |\phi_a| = 2 < |a| = 4$. (Other examples possible.) ▨

55. Suppose ϕ is an automorphism of D_4 s.t. $\phi(R_{90}) = R_{270}$ and $\phi(V) = V$. Find $\phi(D)$ and $\phi(H)$.

Note that $\phi(D) = \phi(R_{90}V) = \phi(R_{90})\phi(V) = R_{270}V = \underline{D'}$, and $\phi(H) = \phi(R_{90}D) = \phi(R_{90})\phi(D)$
$= R_{270}D' = \underline{H}$.

56. In $\mathrm{Aut}(\mathbb{Z}_9)$, let α_i denote the automorphism that sends $\bar{1}$ to $\bar{i}$ where $\gcd(i, 9) = 1$. Write $\alpha_5 + \alpha_8$ as permutations of $\{0, 1, \ldots, 8\}$ in disjoint cycle form.

We have $\alpha_5(\bar{1}) = \bar{5}$, $\alpha_5(\bar{5}) = \overline{25} = \bar{7}$, $\alpha_5(\bar{7}) = \overline{35} = \bar{8}$, $\alpha_5(\bar{8}) = \overline{40} = \bar{4}$, $\alpha_5(\bar{4}) = \overline{20} = \bar{2}$, $\alpha_5(\bar{2}) = \overline{10} = \bar{1}$, and $\alpha_5(\bar{3}) = \overline{15} = \bar{6}$, $\alpha_5(\bar{6}) = \overline{30} = \bar{3}$, so $\boxed{\alpha_5 = (0)(157842)(36)}$.

Similarly, $\alpha_8(\bar{1}) = \bar{8}$, $\alpha_8(\bar{8}) = \overline{64} = \bar{1}$; $\alpha_8(\bar{2}) = \overline{16} = \bar{7}$, $\alpha_8(\bar{7}) = \overline{56} = \bar{2}$; $\alpha_8(\bar{3}) = \overline{24} = \bar{6}$, $\alpha_8(\bar{6}) = \overline{48} = \bar{3}$; $\alpha_8(\bar{4}) = \overline{32} = \bar{5}$, $\alpha_8(\bar{5}) = \overline{40} = \bar{4}$, so $\boxed{\alpha_8 = (0)(18)(27)(36)(45)}$.