Chapter 5

6. Let \( \alpha = (a_1 \ a_2 \ a_3) \) and \( \beta = (a_4 \ a_5 \ a_6 \ a_7 \ a_8) \) be disjoint cycles in \( A_8 \). (We know \( \alpha, \beta \in A_8 \) since \( \alpha \) and \( \beta \) each decompose into an even number of 2-cycles, for example, \( \alpha = (a_1 \ a_3)(a_1 \ a_2) \) and \( \beta = (a_4 \ a_8)(a_4 \ a_7)(a_4 \ a_6)(a_4 \ a_5) \).

Notice that \(|\alpha| = 3\), since
\[
\alpha^2 = (a_1 \ a_2 \ a_3)(a_1 \ a_2 \ a_3) = (a_1 \ a_3 \ a_2) \neq \varepsilon
\]
but
\[
\alpha^3 = (a_1 \ a_2 \ a_3)(a_1 \ a_2 \ a_3)(a_1 \ a_2 \ a_3) = (a_1 \ a_3 \ a_2)(a_1 \ a_2 \ a_3) = (a_1)(a_2)(a_3) = \varepsilon,
\]
where \( \varepsilon \) is the identity in \( A_8 \).

Also notice that \(|\beta| = 5\) since
\[
\beta^5 = (a_4 \ a_5 \ a_6 \ a_7 \ a_8)(a_4 \ a_5 \ a_6 \ a_7 \ a_8)(a_4 \ a_5 \ a_6 \ a_7 \ a_8)(a_4 \ a_5 \ a_6 \ a_7 \ a_8)(a_4 \ a_5 \ a_6 \ a_7 \ a_8)
\]
\[
= (a_4 \ a_5 \ a_6 \ a_7 \ a_8)(a_4 \ a_5 \ a_6 \ a_7 \ a_8)(a_4 \ a_5 \ a_6 \ a_7 \ a_8)(a_4 \ a_5 \ a_6 \ a_7 \ a_8)
\]
\[
\beta^5 \neq \varepsilon
\]
\[
= (a_4 \ a_5 \ a_6 \ a_7 \ a_8)(a_4 \ a_5 \ a_6 \ a_7 \ a_8)(a_4 \ a_5 \ a_6 \ a_7 \ a_8)
\]
\[
\beta^5 \neq \varepsilon
\]
\[
= (a_4)(a_5)(a_6)(a_7)(a_8) = \varepsilon
\]
By Theorem 5.3, then, \(|\alpha\beta| = \text{lcm}(3, 5) = 15\).

18. a) \( \alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 8 & 6 \end{bmatrix} = (1 \ 2 \ 3 \ 4 \ 5)(6 \ 7 \ 8) \)

and
\[
\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 8 & 7 & 6 & 5 & 2 & 4 \end{bmatrix} = (2 \ 3 \ 8 \ 4 \ 7)(5 \ 6),
\]
so \( \alpha\beta = (1 \ 2 \ 3 \ 4 \ 5)(6 \ 7 \ 8)(2 \ 3 \ 8 \ 4 \ 7)(5 \ 6) = (1 \ 2 \ 4 \ 8 \ 5 \ 7 \ 3 \ 6) \).

b) Here are two different ways of decomposing each of \( \alpha, \beta, \) and \( \alpha\beta \) into 2-cycles:
\[
\alpha = (1 \ 5)(1 \ 4)(1 \ 3)(1 \ 2)(6 \ 8)(6 \ 7) = (1 \ 2)(2 \ 3)(3 \ 4)(4 \ 5)(6 \ 7)(7 \ 8)
\]
\[
\beta = (2 \ 7)(2 \ 4)(2 \ 8)(2 \ 3)(5 \ 6) = (2 \ 3)(3 \ 8)(8 \ 4)(4 \ 7)(5 \ 6)
\]
\[
\alpha\beta = (1 \ 6)(1 \ 3)(1 \ 7)(1 \ 5)(1 \ 8)(1 \ 4)(1 \ 2) = (1 \ 2)(2 \ 4)(4 \ 8)(8 \ 5)(5 \ 7)(7 \ 3)(3 \ 6)
\]
22. Let \( r, s, t, \) and \( u \) be the number of 2-cycles into which \( \alpha, \beta, \alpha^{-1}, \) and \( \beta^{-1} \) decompose, respectively.

**Claim.** Either \( r \) and \( t \) are both even or \( r \) and \( t \) are both odd; either \( s \) and \( u \) are both even or \( s \) and \( u \) are both odd.

**Proof of Claim (by contradiction).** Suppose \( r \) is even and \( t \) is odd. Then \( \alpha \alpha^{-1} \) decomposes into \( r + t \) 2-cycles. Note that \( r + t \) is odd since ”even” + ”odd” = ”odd.” But \( \alpha \alpha^{-1} \) is the identity in \( S_n \), which is an even permutation, so this is a contradiction. The same proof works if we assume \( r \) is odd and \( t \) is even, since ”odd” + ”even” = ”odd” as well. If we replace \( r \) with \( s \) and \( t \) with \( u \), then we have proved the second half of the claim.

Now observe that \( \alpha^{-1} \beta^{-1} \alpha \beta \) decomposes into \( t + u + r + s \) 2-cycles. Since \( t \) and \( r \) are both even or both odd, \( t + r \) is even. Similarly, \( s + u \) is even. Thus, \( t + u + r + s \) is even, hence \( \alpha^{-1} \beta^{-1} \alpha \beta \) is an even permutation.

\[
(a_1 \ a_2 \ \cdots \ a_n)^{-1} = (a_1 \ a_n \ a_{n-1} \ \cdots \ a_2) \text{ since } (a_1 \ a_2 \ \cdots \ a_n)(a_1 \ a_n \ a_{n-1} \ \cdots \ a_2) = \]
\[
(a_1)(a_2) \cdots (a_{n-1})(a_n). 
\]

**Chapter 6.**

2. We will show that \( \text{Aut}(\mathbb{Z}) = \{ \varphi_1, \varphi_{-1} \} \), where \( \varphi_1 \) is the identity map from \( \mathbb{Z} \) to \( \mathbb{Z} \) and we define \( \varphi_{-1} : \mathbb{Z} \rightarrow \mathbb{Z} \) as

\[
\varphi_{-1}(k) = \begin{cases} 
-k, & \text{if } k \neq 0 \\
0, & \text{if } k = 0 
\end{cases}
\]

We know that the identity map is an automorphism, so we show that \( \varphi_{-1} \) is an automorphism.

Let \( k, \ell, m \in \mathbb{Z} \).

One-to-one: If \( \varphi_{-1}(k) = \varphi_{-1}(\ell) \), then \( -k = -\ell \Rightarrow k = \ell \).

Onto: If \( m \in \mathbb{Z} \), then \( \varphi_{-1}(m) = -(m) = m \).

Operation-preserving: \( \varphi_{-1}(k + \ell) = -(k + \ell) = (-k) + (-\ell) = \varphi_{-1}(k) + \varphi_{-1}(\ell) \).

Inverse-preserving: \( \varphi_{-1}(k^{-1}) = \varphi_{-1}(-k) = -(-k) = \varphi_{-1}(k)^{-1} \).

We now argue that there are no other automorphisms of \( \mathbb{Z} \). As seen in class, an automorphism of a cyclic group is determined by its image of a generator, so we need only consider the possible images of 1. Suppose that \( d : \mathbb{Z} \rightarrow \mathbb{Z} \) is an automorphism. Then \( 1 \in \langle d(1) \rangle \) if and only if \( d(1) \) divides 1, which is to say that \( d(1) = 1 \) or \( d(1) = -1 \). Thus, \( d = \varphi_1 \) or \( d = \varphi_{-1} \).

The multiplication in \( \text{Aut}(\mathbb{Z}) \) works as follows: \( \varphi_1 \circ \varphi_1 = \varphi_1 \), \( \varphi_1 \circ \varphi_{-1} = \varphi_{-1} \), \( \varphi_{-1} \circ \varphi_1 = \varphi_{-1} \), and \( \varphi_{-1} \circ \varphi_{-1} = \varphi_1 \). (All of these are straightforward to check.)

14. By Theorem 6.5, \( \text{Aut}(\mathbb{Z}_6) \) is isomorphic to \( U(6) = \{1,5\} \) via the correspondence \( \varphi_1 \leftrightarrow 1 \) and \( \varphi_5 \leftrightarrow 5 \). More specifically, \( \varphi_1(1) = 1 \), so that \( \varphi_1 \) is the identity map \( \mathbb{Z}_6 \rightarrow \mathbb{Z}_6 \), and \( \varphi_5(1) = 5 \).

The group structure of \( \text{Aut}(\mathbb{Z}_6) \) is as follows: \( \varphi_1 \circ \varphi_1 = \varphi_1 \), \( \varphi_1 \circ \varphi_5 = \varphi_5 \circ \varphi_1 = \varphi_5 \), and \( \varphi_5 \circ \varphi_5 = \varphi_1 \). To verify this last fact, notice that \( \varphi_6(\varphi_5(1)) = \varphi_5(5) = \varphi_5(1+1+1+1+1+1) = \varphi_5(1) + \varphi_5(1) + \varphi_5(1) + \varphi_5(1) + \varphi_5(1) = 5 + 5 + 5 + 5 + 5 = 1 \text{ (mod 6)} \), and so \( \varphi_5 \circ \varphi_5 \) is the identity isomorphism.