PROOFS IN CHAPTER 6

Lemma 6.1 There are \( n! \) permutations of \( \{1, 2, \ldots, n\} \).

Proof Given a permutation in 2-line notation

\[
\begin{pmatrix}
1 & 2 & 3 & \ldots & n \\
a_1 & a_2 & a_3 & \ldots & a_n
\end{pmatrix}
\]

there are \( n \) choices for \( a_1 \), leaving \( n - 1 \) choices for \( a_2 \), \( n - 2 \) choices for \( a_3 \),..., 1 choice for \( a_n \). Hence there are \( n! \) choices in all.

Lemma 6.2 Let \( \alpha \) be a permutation (of \( \{1, 2, \ldots, n\} \)) then there exists a positive integer \( k \) such that \( \alpha^k = \iota \).

Proof \( \iota, \alpha, \alpha^2, \alpha^3, \ldots \) cannot all be different as there are only \( n! \) different permutations of \( \{1, 2, \ldots, n\} \). Hence there exist positive integers \( r < s \) with \( \alpha^r = \alpha^s \).

Since \( \alpha \) is a bijection it has an inverse \( \alpha^{-1} \). From the equation above we have:

\[ \alpha^r \alpha^{-1} = \alpha^s \alpha^{-1} \]

That is,

\[ \iota = \alpha^{s-r} \]

Thus \( \alpha^k = \iota \), where \( k = s - r \).

Lemma 6.3 Let \( m \) be the order of \( \alpha \). Then \( \alpha^k = \iota \) if and only if \( m \) divides \( k \).

Proof Suppose \( m | k \). Then \( k = qm \) for some \( q \). So

\[ \alpha^k = (\alpha^m)^q = \iota^q = \iota \]

Conversely suppose \( \alpha^k = \iota \). By the division algorithm, \( k = qm + r \) some \( 0 \leq r < m \). So

\[ \iota = \alpha^k = (\alpha^m)^q\alpha^r = \iota^q\alpha^r = \alpha^r \]

But \( m \) was chosen to be the smallest positive integer such that \( \alpha^m = \iota \). So \( r = 0 \). Hence \( m | k \).

Lemma 6.4 Every cycle of length \( r \) has order \( r \).

Proof Let \( \alpha = (a_1 \ a_2 \ldots \ a_r) \). Then \( \alpha^j \) sends each \( a_k \) to \( a_{k+j} \), where \( k + j \) is counted modulo \( r \). Hence when \( 0 < j < r \), \( \alpha^3 \neq \iota \), but for \( j = r \) we have \( \alpha^r = \iota \). So the order of \( \alpha \) is \( r \).

Lemma 6.5 Disjoint cycles commute, i.e. if \( \alpha = (a_1 \ldots a_r) \) and \( \beta = (b_1 \ldots b_s) \) are disjoint cycles then \( \alpha \beta = \beta \alpha \).

Proof Let \( \alpha = (a_1 \ldots a_r) \) and let \( \beta = (b_1 \ldots b_s) \), and let \( x \) be any \( a_i \) or \( b_i \).

If \( x = a_i \), then

\[ x\alpha\beta = a_i \alpha \beta = a_{i+1} \beta = a_{i+1} \]

and

\[ x\beta\alpha = a_i \beta \alpha = a_i \alpha = a_{i+1} \]

Similarly if \( x = b_i \), then

\[ x\alpha\beta = b_{i+1} = x\beta\alpha \]
Thus \( x\alpha \beta = x\beta \alpha \) for all \( x \) and hence \( \alpha \beta = \beta \alpha \).

**Proposition 6.6** Let \( \alpha \) be a permutation of \( S \) and let \( \sim \) be the relation on \( S \) defined by \( x \sim y \Leftrightarrow y = x\alpha^k \) for some \( k \in \mathbb{Z} \). Then \( \sim \) is an equivalence relation, and the equivalence classes are the orbits of \( \alpha \).

**Proof** For all \( x \in S \), \( x \sim x \) since \( x = x\alpha^0 \).
For all \( x, y \in S \), \( x \sim y \Rightarrow y = x\alpha^k \Rightarrow x = y\alpha^{-k} \Rightarrow x \sim y \).
For all \( x, y, z \in S \), \( x \sim y \) and \( y \sim z \Rightarrow y = x\alpha^k \) and \( z = y\alpha^l \Rightarrow z = x\alpha^{k+l} \Rightarrow x \sim z \).
Hence \( \sim \) is an equivalence relation. The equivalence class of \( x \) is \( \{x\alpha^k : k \in \mathbb{Z}\} \), in other words it is the orbit of \( x \).

**Proposition 6.7** Every permutation can be written as a product of disjoint cycles.

**Proof** Let \( \alpha \) be a permutation of \( S \) and let \( E_1, \ldots, E_k \) be the orbits of \( \alpha \). Then, restricted to each \( E_i \), the permutation \( \alpha \) is a cycle \( C_i \). The \( E_i \)'s are disjoint by 6.6 (since \( \sim \) is an equivalence relation). Hence \( \alpha = C_1C_2 \ldots C_k \) (the product of the cycles \( C_1, \ldots, C_k \)).

**Proposition 6.8** The representation of any \( \alpha \) as a product of disjoint cycles is unique, up to the order in which the cycles are written down.

**Proof** Each cycle corresponds to an orbit, so we get a unique collection of cycles. But as these cycles are disjoint it does not matter the order in which we write them down.

**Proposition 6.9** Any permutation is a product of transpositions.

**Proof** It suffices to show that each cycle can be written as a product of transpositions. But \( (a_1 a_2 \ldots a_r) = (a_1 a_2)(a_1 a_3)\ldots(a_1 a_r) \).

**Proposition 6.10** Any permutation is a product of basic transpositions.

**Proof** By 6.9 we just have to show that any transposition \( (i j) \), with \( i < j \), can be written as a product of basic transpositions. But
\[
(i j) = (i i + 1)(i + 1 i + 2)(j - 2 j - 1)(j - 1 j)(j - 2 j - 1) \ldots (i + 1 i + 2)(i i + 1)
\]

**Proposition 6.11** \( sgn(\alpha \beta) = sgn(\alpha) sgn(\beta) \) for any permutations \( \alpha \) and \( \beta \).

**Proof** (Sketch only)
First we observe that if \( t \) is a basic transposition \( (i i + 1) \), then \( sgn(t) = -1 \), since \( t \) changes the order of just one pair of elements.
Next we observe that if \( \alpha \) is any permutation and \( t \) is a basic transformation, say \( t = (i i + 1) \), then
\[
(*) \quad l(t\alpha) = l(\alpha) + 1 \text{ if } i\alpha < (i + 1)\alpha \text{ and } l(t\alpha) = l(\alpha) - 1 \text{ if } i\alpha > (i + 1)\alpha.
\]
This is because the effect of \( t \) is to interchange just two of the columns in the 2-line representation of \( \alpha \).
Thus \( sgn(t\alpha) = -sgn(\alpha) = sgn(t) sgn(\alpha) \).
Since any permutation \( \alpha \) can be written as a product of basic permutations \( \alpha = t_1 \ldots t_p \) we may now deduce inductively (using \((*)\)) that
\[
sgn(\alpha) = sgn(t_1 \ldots t_p) = sgn(t_1) \ldots sgn(t_p) = (-1)^p
\]
If \( \beta \) is another permutation, written as a product of basic permutations \( \beta = s_1 \ldots s_q \) we also have
\[
sgn\beta = (-1)^q
\]
Since $\alpha \beta = t_1 \ldots t_p s_1 \ldots s_q$ as a product of basic permutations we also have

$$\text{sgn}(\alpha \beta) = (-1)^{p+q}$$

Thus $\text{sgn}(\alpha \beta) = \text{sgn}(\alpha)\text{sgn}(\beta)$.

**Corollary 6.12** A permutation $\alpha$ is even if and only if it can be written as a product of an even number of (not necessarily basic) transpositions.

**Proof** Suppose $\alpha = t_1 \ldots t_q$, where $t_1, \ldots, t_q$ are transpositions (not necessarily basic). For any transposition $t$ we have $\text{sgn}(t) = -1$, since $t$ can be written as a product of an odd number of basic transpositions (by the proof of 6.10). Now, by 6.11,

$$\text{sgn}(\alpha) = \text{sgn}(t_1) \ldots \text{sgn}(t_q) = (-1) \times \ldots \times (-1) = (-1)^q$$

which is $+1$ if and only if $q$ is even.