1 Recall

Theorem 1.1 (Bezout's Identity)**.** Let $\gcd(a,b) = d$. Then there exist integers x and y such that $ax + by = d$. Moreover, integers of the form $as + bt$ (i.e. linear combinations of a, b) are exactly the multiples of d.

This theorem gives rise to an extremely important corollary:

Corollary 1.2. Integers a and b are relatively prime (i.e. $\gcd(a,b) = 1$) iff there exist $s, t \in \mathbb{Z}$ such that $as + bt = 1$.

Theorem 1.3. Let n, a be positive integers and let $d = \gcd(a,n)$. Then the equivalence

$$ax \equiv 1 \pmod{n}$$

has a solution if and only if $d = 1$.

Proof. We have

$$ax \equiv 1 \pmod{n} \iff \exists k \in \mathbb{Z},\ ax = kn + 1 \iff \gcd(a,n) = 1.$$

$\square$

Remark. We can consider x as the inverse of a under $U(n)$. Thus we can restate this as "a has an inverse x iff $\gcd(a,n) = 1$." This theorem justifies why the only members of $U(n)$ are those coprime to n.

Definition 1.4 (Euler's Totient Function)**.** Given a positive integer n, the function $\phi(n)$ counts the positive integers less than n that are relatively prime to n. Formally,

$$\phi(n) = \left|\{1 \leq k \leq n \mid \gcd(k,n) = 1\}\right|.$$

Theorem 1.5. Euler's Phi is a multiplicative function. That is, if $\gcd(m,n) = 1$ then $\phi(mn) = \phi(m)\phi(n)$.

Theorem 1.6. Let p be prime. Then $\phi(p^n) = p^n - p^{n-1}$.

2 Groups

Definition 2.1. Let G be a set. A *binary operation* on G is a function that assigns each ordered pair of elements of G to an element of G.

Definition 2.2. Let G be a set together with a binary operation that assigns to each ordered pair (a,b) of elements of G to an element of G denoted by ab. We say G is a *group* under this operation if the following three properties are satisfied.

1. *Associativity.* We have $(ab)c = a(bc)$ for all a, b, c in G.

2. *Identity.* There is an element e (called the *identity*) in G such that $ae = ea = a$ for all a in G.

3. *Inverses.* For each element a in G, there is an element b in G (called an *inverse* of a) such that $ab = ba = e$.

Example 2.3. The following are all examples of groups:

1. The sets $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all groups under addition. In all cases the identity is 0 and the inverse of a is $-a$.

2. The set of positive rationals $\mathbb{Q}^+_\times$ is a group under ordinary multipication.

3. The set $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ is a group under addition modulo n.

4. The set of 2×2 nonsingular matrices is called the *general linear group* of 2×2 matrices over $\mathbb{R}$, denoted $\mathrm{GL}(2, \mathbb{R})$. This group is non-commutative.

5. Let $\mathbb{F}$ be a field, such as $\mathbb{R}, \mathbb{C}$, or $\mathbb{Z}_p$. Then $\mathrm{GL}(n, \mathbb{F})$ is a group for any positive integer $n \geq 1$, prime .

6. For any positive integer n, we define $U(n)$ to be the set of all positive integers less than n and relatively prime to n. The operation is multiplication modulo n. This group is simply known as the *multiplicative group of integers modulo n.*

7. Notice that in $U(8) = \{1, 3, 5, 7\}$, we have the property $3 \cdot 5 = 7$, $5 \cdot 7 = 3$, and $7 \cdot 3 = 5$. Thus $U(8)$ exhibits the properties of (i.e. is isomorphic to) the Klein-4 group.

8. Consider the symmetries of a regular n-gon with $n \geq 3$. The corresponding group is denoted D_n and is called the *dihedral group of order* $2n$. For instance, a square has symmetries $D_4 = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$ and is called the dihedral group of order 8. This group is non-commutative.

Definition 2.4. A group with the property that $ab = ba$ for every pair of elements $a, b \in G$ is said to be *Abelian.*

Theorem 2.5. In a group, there is only one identity element.

Proof. Let e, e' be identities in G. Then

1. $ae = a$ for all $a \in G$, and

2. $e'b = b$ for all $b \in G$.

   Setting $a := e'$ and $b := e$ yields $e'e = e'$ and $e'e = e$, respectively, which proves the claim.

□

Theorem 2.6. In a group, right and left cancellation hold; that is, $ba = ca$ implies $b = c$, and $ab = ac$ implies $b = c$

Theorem 2.7. For each element a in a group G, there is a unique element a^{-1} in G such that $aa^{-1} = a^{-1}a = e$.

Definition 2.8. Let g be an element of a group G. If n is positive, then we define

$$g^n := \underbrace{gg\dots g}_{n \text{ factors}}.$$

if $n = 0$, then $g^0 := e$, and if n is negative,

$$g^n := (g^{-1})^{|n|}.$$

Example 2.9. For $(ab)^{-2}$ we have

$$(ab)^{-2} = [(ab)^{-1}]^2 = (b^{-1}a^{-1})^2 = b^{-1}a^{-1}b^{-1}a^{-1}.$$

using the socks-and-shoes principle described later.

Remark. The order in which the -1 and the $|n|$ appears is not so important, since for positive n,

$$g^{-n} = (g^{-1})^n$$

but clearly

$$(g^{-1})^n g^n = e$$

and so

$$(g^{-1})^n = (g^n)^{-1}.$$

Theorem 2.10. The laws of exponents hold, that is, for integers m, n and any group element g, we have

1. $g^m g^n = g^{m+n}$
2. $(g^m)^n = g^{mn}$.

Remark. Note that in general, we **do not** have $(ab)^n = a^n b^n$. It is the case that

$$(ab)^n = \underbrace{abab\dots ab}_{n \text{ times}}.$$

Theorem 2.11 (Socks and Shoes)**.** For group elements a and b, $(ab)^{-1} = b^{-1}a^{-1}$.

Theorem 2.12 (Pants, Socks and Shoes)**.** For group elements a, b, c we have $(abc)^{-1} = c^{-1}b^{-1}a^{-1}$.

Definition 2.13 (Cayley Table)**.** A *Cayley table* for a group G with n elements is an $n \times n$ array where a row corresponds to an element a in G, a column corresponds to an element b in G, and the entry in the a-row and b-column is the product ab.

Theorem 2.14. In a Cayley table, each element in a group occurs exactly once in each row and each column.

Proof. If an element is in the a-row, then it is of the form ax for some $x \in G$. Suppose $ax = ay$, i.e. the entry in (a, x) is equal to the entry in (a, y). Then by cancellation, $x = y$, so every entry in the row is unique. The same argument mutatis mutandis can be used to prove the uniqueness for columns. $\square$

Theorem 2.15. Consider the Cayley table of G as an $n \times n$ matrix. Then G is Abelian iff its Cayley table is symmetric.

3 Finite Groups and Subgroups

Definition 3.1. The number of elements $|G|$ of a group G is called its *order*.

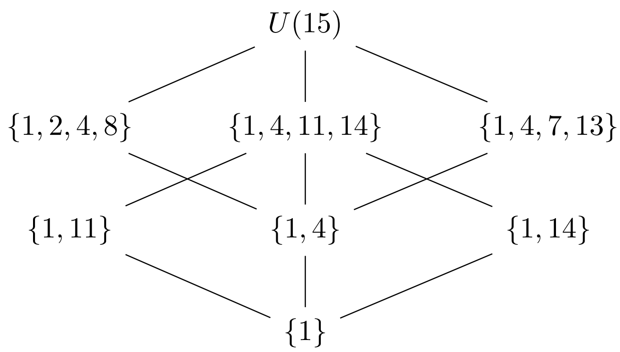
Definition 3.2. The *order* of an element g in a group G is the smallest positive integer n such that $g^n = e$. If no such integer exists, we set $g^n := \infty$. We denote the order of g as $|g|$.

Definition 3.3. If a subset H of a group G is itself a group under the operation of G, we say that H is a *subgroup* of G.

Definition 3.4. If H is a subgroup of G but $H \neq G$, we say that H is a *proper subgroup of* G.

Definition 3.5. The lattice of subgroups of a group G is the lattice whose elements are the subgroups of G, with the partial ordering being set inclusion $\subseteq$.

Example 3.6. For $U(15)$ we have the following lattice of subgroups:



Theorem 3.7 (One-Step Subgroup Test)**.** Let G be a group. Then a subset H is a subgroup of G if and only if the following hold:

1. H is nonempty

2. If $a, b \in H$ then $ab^{-1} \in H$.

Proof. Since the operation of H is the same as in G, it is clear that this operation is associative. Now we show that $e \in H$. Since H is nonempty, we can speak of an element $a \in H$. By premise, since $a \in H$ we know $aa^{-1} = e \in H$. Now let $x \in H$; we wish to show that $x^{-1} \in H$ as well. Take $a = e$ and $b = x$ in the premise: then $eb^{-1} = b^{-1} \in H$ as desired. □

Theorem 3.8 (Two-Step Subgroup Test)**.** Let G be a group. Then a subset H is a subgroup of G if and only if the following hold:

1. H is nonempty.
2. If $a, b \in H$ then $ab \in H$.
3. If $a \in H$ then $a^{-1} \in H$.

Proof. Notice we just need to show that $e \in H$. But this follows since H is nonempty and $aa^{-1} = e \in H$ by (2) and (3). □

Theorem 3.9 (Finite Subgroup Test)**.** Let H be a nonempty finite subset of a group G. If H is closed under the operation of G, then H is a subgroup of G.

Proof. By the Two-Step Subgroup Test, we only need to prove (3), that $a^{-1} \in H$ whenever $a \in H$. If $a = e$, we are done, so suppose $a \neq e$ and consider the sequence

$$a, a^2, \dots.$$

By closure, all of these elements belong to H, but since H is finite, not all of these elements are distinct. Say $a^i = a^j$ and WLOG $i > j$. Then $a^{i-j} = e$ and since $a \neq e$ we have $i - j > 1$. Therefore

$$aa^{i-j-1} = a^{i-j} = e \implies a^{i-j-1} = a^{-1}.$$

But $i - j - 1 \geq 0$ implies $a^{i-j-1} \in H$ and we are done. □

Definition 3.10. A group H is called *cyclic* iff there is an element $a \in H$ such that $H = \{a^n \mid n \in \mathbb{Z}\}$. Such an element a is called a *generator* of H.

Let G be a group and $a \in G$ a group element. We call $\langle a \rangle$ the *cyclic subgroup of G generated by a* defined by

$$\begin{aligned}\langle a \rangle :=& \{a^n : n \in \mathbb{Z}\} \\ =& \{\dots, a^{-2}, a^{-1}, e, a, a^2, \dots\}\end{aligned}$$

Theorem 3.11. For any $a \in G$, $\langle a \rangle$ is a subgroup of G.

Proof. We use the One-Step Subgroup Test. Clearly $a \in \langle a \rangle$, so it is nonempty. Let $a^i, a^j \in \langle a \rangle$. Then $a^i a^{-j} = a^{i-j} \in \langle a \rangle$ by laws of exponents. $\square$

Definition 3.12. Let S be a collection of elements from a group G. Then we call $\langle S \rangle$ the *subgroup generated by* S, defined as the smallest subgroup of G containing S. More precisely, $\langle S \rangle$ is the subgroup with the property that $S \subseteq \langle S \rangle$, and if $S \subseteq H$, then $\langle S \rangle \subseteq H$.

Remark. In linear algebra, this is simply the span.

Definition 3.13. The center $Z(G)$ of a group G is the subset of elements in G that commute with every element of G, that is,

$$Z(G) := \{a \in G : ax = xa \text{ for all } x \in G\}.$$

Theorem 3.14. The center of a group G is a subgroup of G.

Proof. We use the One-Step Subgroup Test. First, we have $ex = xe = x$ for all $x \in G$, so $e \in Z(G)$. Now let $a, b \in Z(G)$. Then for any $x \in G$

$$\begin{aligned}(ab^{-1})x &= b^{-1}(ax) \\ &= b^{-1}(ax)bb^{-1} \\ &= b^{-1}b(ax)b^{-1} \\ &= axb^{-1} \\ &= xab^{-1}\end{aligned}$$

and so $ab^{-1} \in Z(G)$, as desired. $\square$

Definition 3.15. Let a be a fixed element of a group G. The *centralizer of a in G*, denoted $C(a)$, is the set of all elements in G that commute with a. In other words,

$$C(a) := \{g \in G : ga = ag\}.$$

Theorem 3.16. For each $a \in G$, $C(a)$ is a subgroup of G.

Proof. We use the same proof as above, modified slightly. $\square$

3.1 Some Useful Theorems

Theorem 3.17. Let a, x be any group elements of G and $n \in \mathbb{Z}$. Then we have

$$(xax^{-1})^n = xa^n x^{-1}$$

4 Cyclic Groups

We have already defined cyclic groups in the previous section. Here are some of their properties.

Theorem 4.1. Let $a \in G$. If $|a| = \infty$, then $a^i = a^j$ iff $i = j$. If $|a| = n \in \mathbb{Z}^+$, then $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ and $a^i = a^j$ iff $n \mid i - j$.

Proof. Suppose first that $|a| = \infty$. Then if $a^i = a^j$, we must have $a^{i-j} = e$. Since a has infinite order, it must be that $i = j$.

Now suppose $|a| = n < \infty$. That $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ can be proven easily with the division algorithm. Now suppose $a^i = a^j$; we wish to show that $n \mid i - j$. Observe that $a^{i-j} = e$ and by the division algorithm, we can find integers q, r such that

$$i - j = nq + r, \qquad 0 \leq r < n.$$

Thus $a^{i-j} = a^{nq+r} = a^r$ But $a^{i-j} = e$ and since $r < n$, it must be that $r = 0$ (otherwise n is not the smallest integer such that $a^n = e$). Therefore, $i - j = nq$, that is, n divides $i - j$. □

Corollary 4.2. We have $a^k = e$ if and only if $|a| \mid k$.

Corollary 4.3. We have $|\langle a^k \rangle| = |a^k|$ for any integer k.

Corollary 4.4. If $a, b \in G$ where $|G| < \infty$ and $ab = ba$, then $|ab|$ divides $|a||b|$.

Proof. Let $|a| = m$ and $|b| = n$. Then $(ab)^{mn} = (a^m)^n (b^n)^m = e$ and so by the previous corollary, $|ab| \mid mn$. □

Remark. There is essentially only one cyclic group of each order. If $|a| = \infty$ then $\langle a \rangle \cong \mathbb{Z}$, and if $|a| = n < \infty$ then $\langle a \rangle \cong \mathbb{Z}_n$.

Theorem 4.5. Let $|a| = n$. Then $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ and $|a^k| = n/\gcd(n,k)$ for any integer k.

Proof. Write $d = \gcd(n, k)$ and let $k = dr$ for some integer r. Since $a^k = (a^d)^r$, we have $\langle a^k \rangle \subseteq \langle a^d \rangle$ by closure. By Corollary 1.2 we can find integers $s, t \in \mathbb{Z}$ such that $d = ns + kt$. So,

$$a^d = a^{ns+kt} = ea^{kt} = (a^k)^t \in \langle a^k \rangle$$

which shows that $\langle a^d \rangle \subseteq \langle a^k \rangle$. Therefore $\langle a^{\gcd(n,k)} \rangle = \langle a^k \rangle$.

For the second part, notice that

$$\begin{aligned} |a^k| &= \min\{m \in \mathbb{Z}^+ : (a^k)^m = e\} \\ &= \min\{m \in \mathbb{Z}^+ : n \mid km\} \\ &= \min\{m \in \mathbb{Z}^+ : km \text{ is a multiple of } n\} \end{aligned}$$

and so $k|a^k| = \text{lcm}(n, k)$. Multiplying both sides by $\gcd(n, k)$ gives

$$\begin{aligned} k \gcd(n,k)|a^k| &= \gcd(n,k)\text{lcm}(n,k) \\ &= nk \end{aligned}$$

and so $|a^k| = n/\gcd(n, k)$, as desired. □

Corollary 4.6. In a finite cyclic group $\langle a \rangle$, the order of an element divides the order of the group. In other words, if $|a| = n$ and $|a^k| = m$ then $m \mid n$.

Corollary 4.7. Let $|a| = n$. Then $\langle a^i \rangle = \langle a^j \rangle$ iff $\gcd(n, i) = \gcd(n, j)$.

Corollary 4.8. Let $|a| = n$. Then $\langle a \rangle = \langle a^j \rangle$ iff $\gcd(n, j) = 1$.

Corollary 4.9. An integer k in $\mathbb{Z}_n$ is a generator of $\mathbb{Z}_n$ iff $\gcd(n, k) = 1$.

4.1 Classification of Subgroups of Cyclic Groups

Theorem 4.10 (Fundamental Theorem of Cyclic Groups)**.** Every subgroup of a cyclic group is cyclic. Moreover, if $|a| = n$, then the order of any subgroup of $\langle a \rangle$ is a divisor of n, and for each positive divisor d of n, the group $\langle a \rangle$ has exactly one subgroup of order d — namely $\langle a^{n/d} \rangle$.

Proof. There are three claims in this theorem.

Claim 4.11. Every subgroup of a cyclic group is cyclic

Proof of Claim. Let $G = \langle a \rangle$ and suppose H is a subgroup of G. We want to show that H is cyclic. If $H = \{e\}$ then we are done, so suppose $a^t \in H$ for some $t \neq 0$. If $t < 0$ then $a^{-t} \in H$ as well since H is a (sub)group, so there is always an $a^t \in H$ such that $t > 0$.

Now let m be the least positive integer such that $a^m \in H$ (we needed to show that the set of such integers is nonempty). Let $a^k \in H$; we wish to show that $a^k \in \langle a^m \rangle$. Note that $k \geq m$ by minimality, so we can use the division algorithm to write $k = pm + r$ for integers $p, 0 \leq r < m$. Then

$$a^k = a^{pm}a^r = a^r.$$

But $r < m$, so we must have $r = 0$ (otherwise m is not minimal). So $a^k = (a^m)^p$, i.e. $a^k \in \langle a^m \rangle$. □

Claim 4.12. If $|a| = n$, then the order of any subgroup of $\langle a \rangle$ is a divisor of n.

Proof of Claim. By the above Claim 4.11, if H is a subgroup of $\langle a \rangle$ we can write $H = \langle a^m \rangle$ for some positive integer m. If $|H| = k$ then by Corollary 4.6 we have $k \mid n$. □

Claim 4.13. For each positive divisor d of $|a|$, the group $\langle a \rangle$ has exactly one subgroup of order d — namely $\langle a^{n/d} \rangle$.

Proof of Claim. If d is any positive divisor of n then by Theorem 4.5,

$$|\langle a^{n/d} \rangle| = \frac{n}{\gcd(n, n/d)} = \frac{n}{n/d} = d.$$

Thus there is at least one subgroup of order d. Suppose another subgroup H is of order d. By Claim 4.11 $H = \langle a^m \rangle$ for some positive $m \mid n$ and $|\langle a^m \rangle| = n/m = d$. So $m = n/d$, i.e. $H = \langle a^{n/d} \rangle$. □

□

Corollary 4.14. For each positive divisor d of n, the set $\langle a^{n/d} \rangle$ is the unique subgroup of $\mathbb{Z}_n$ of order d. Moreover, these are the only subgroups of $\mathbb{Z}_n$.

Corollary 4.15. The number of elements of order d in a cyclic group of order n is $\phi(d)$.

Proof. By Theorem 4.10 the group has a unique subgroup of order d, which we call $\langle a \rangle$. Note that an element $g \in G$ has order d iff $|\langle g \rangle| = d$ and so $|g| = d \iff \langle g \rangle = \langle a \rangle$. By Corollary 4.8 an element a^k generates $\langle a \rangle$ iff $\gcd(k, d) = 1$. There are exactly $\phi(d)$ such elements. □

Remark. The fundamental theorem can be used to exhaustively list all the subgroups of a finite cyclic group: they are exactly $\langle a^d \rangle$ where d is a divisor of $n = |a|$.

Corollary 4.16. In a finite group (not necessarily cyclic!), the number of elements of order d is a multiple of $\phi(d)$.

Proof. If a finite group has no elements of order d then the statement is true, so let $a \in G$ with $|a| = d$. By Corollary 4.15 we know $\langle a \rangle$ has $\phi(d)$ elements of order d. If all elements of order d in G are in $\langle a \rangle$, then we are done, so suppose there is some $b \in G$ not in $\langle a \rangle$. Then $\langle b \rangle$ has $\phi(d)$ elements of order d and we have found $2\phi(d)$ elements of order d, provided that $\langle a \rangle$ and $\langle b \rangle$ have no elements of order d in common.

But this must be the case, otherwise if c is such an element then $\langle a \rangle = \langle c \rangle = \langle b \rangle$ (recall that elements of order d generate the cyclic subgroup they are members of). Continuing in this fashion we see that the number of elements of order d in a finite group is a multiple of $\phi(d)$. □

5 Permutation Groups

Definition 5.1. A *permutation* of a set A is a bijection $f : A \to A$. A *permutation group* of a set A is a set of permutations of A that forms a group under function composition.

Definition 5.2. For a permutation f of $\{1, \ldots, n\}$ we sometimes express f in array form. So if $f(1) = 2$, $f(2) = 3$, $f(3) = 1$, and $f(4) = 4$, we write

$$f = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix}.$$

Definition 5.3. Let $A = \{1, \ldots, n\}$. The set of all permutations of A is called the *symmetric group of degree* n and is denoted by S_n. Clearly $|S_n| = n!$.

Theorem 5.4. The symmetric group S_n is non-Abelian if $n \geq 3$.

Definition 5.5. We can represent certain permutations $\alpha : \{1, \ldots, n\} \to \{1, \ldots, n\}$ in cycle form. If $\alpha(1) = 2, \alpha(2) = 3, \ldots, \alpha(n) = 1$, then we write

$$\alpha = (123 \ldots n)$$

Definition 5.6. Cycles of length 2 are often called *transpositions*.

Theorem 5.7. Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.

Proof. Note that in this case, the product refers to function composition. For a permutation α of $\{1, \ldots, n\}$ choose any member, say, a_1, and observe that

$$(a_1, \alpha(a_1), \alpha^2(a_1), \ldots)$$

is a finite cycle. Then simply choose an element b_1 not appearing in this cycle and continue the process, after which we obtain another cycle. These must be disjoint, otherwise we would have $\alpha^i(a_1) = \alpha^j(b_1)$ and so $b_1 = \alpha^{i-j}(a_1)$ which contradicts the way b_1 was chosen. Continuing in this manner we obtain a product of disjoint cycles. □

Theorem 5.8 (Disjoint Cycles Commute)**.** If the pair of cycles $\alpha = (a_1, \ldots, a_m)$ and $\beta = (b_1, \ldots, b_n)$ have no entries in common, then $\alpha\beta = \beta\alpha$.

Theorem 5.9. The order of a permutation of a finite set written in disjoint cycle form is the least common multiple of the lengths of the cycles.

Proof. Observe that a cycle of length n has order n (clearest seen with a diagram). Let $|\alpha| = m$ and $|\beta| = n$ and set $k := \text{lcm}(m, n)$. It follows from Theorem 4.1 that both α^k and β^k are the identity permutation ε and, since α and β commute, $(\alpha\beta)^k = \alpha^k\beta^k$ is also the identity.

Let $t = |\alpha\beta|$; we wish to show that $t = k$. By Corollary 4.2 we know that $t \mid k$, so $k \geq t$. Now observe that since α and β are disjoint, we know α^t fixes elements of β and β^t fixes elements of α. Thus $\alpha^t\beta^t$ fixes 1 through n only when $\alpha^t = \beta^t = \varepsilon$. But this implies that t is a multiple of both m and n. Since $k = \text{lcm}(m, n)$, we have $k \leq t$, and so we've shown that $k = t$, as desired.

We've actually only proved the case for two disjoint cycles, but this can be readily extended to the general case by a quick induction. □

Example 5.10. Determine all the orders of the 6! elements of S_6.

Solution. We simply write out the possible disjoint cycle structures of the elements of S_6. We have

$$\begin{aligned}(6)\\(5)(1)\\(4)(2)\\(4)(1)(1)\\(3)(3)\\(3)(2)(1)\\(3)(1)(1)(1)\\(2)(2)(2)\\(2)(2)(1)(1)\\(2)(1)(1)(1)(1)\\(1)(1)(1)(1)(1)(1).\end{aligned}$$

From the above theorem we see that the orders of the elements of S_6 are $7, 5, 4, 3, 6, 2, 1$. □

Theorem 5.11. Every permutation in S_n, $n \geq 2$, is a product of 2-cycles (or *transpositions*).

Proof. Observe that $(a_1 a_2 \dots a_n)$ is equal to $(a_1 a_k)(a_1 a_{k-1}) \dots (a_1 a_2)$. Note that the identity can be written as $(12)(12)$. □

Remark. This is not the only way to write a permutation as a product of 2-cycles. Observe that

$$(12345) = (54)(53)(52)(51)$$

$$(12345) = (54)(52)(21)(25)(23)(13)$$

so even the number of 2-cycles may vary.

There is one aspect of a decomposition that never varies. To prove this we will prove a preliminary lemma.

Lemma 5.12. If $\varepsilon = \beta_1 \beta_2 \dots \beta_r$, where the β_i's are 2-cycles, then r is even.

Proof. The book's proof is rather convoluted. Here is a "standard" proof according to Gemini.

Consider a polynomial in n variables $x_1, x_2, \ldots, x_n$ defined as the product of all differences $(x_i - x_j)$ where $i < j$:

$$P(x_1, x_2, \ldots, x_n) := \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

(The astute observer may recognize this as the determinant of a Vandermode matrix). For any permutation $\sigma \in S_n$ we define the action of σ on the polynomial P by permuting the indices of the variables:

$$\sigma(P) := \prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

Since the set of factors in $\sigma(P)$ is the same as in P except perhaps for its sign, we have $\sigma(P) = \pm P$. Now consider the effect of a transposition, say, $\tau = (k, l)$ with $k < l$, on P.

1. The factor $(x_k - x_l)$ becomes $(x_l - x_k)$ and so its sign is flipped.
2. For a fixed $m \neq k, l$ the factors $(x_m - x_k)$ and $(x_m - x_l)$ are a pair, possibly with inside terms ordered differently, come in pairs. Then τ merely swaps x_k and x_l, leaving the sign unchanged.
3. The rest of the factors are unaffected by τ, leaving the sign unchanged.

Thus a transposition τ has the effect $\tau(P) = -P$. We are given that

$$\varepsilon = \beta_1 \beta_2 \ldots \beta_r$$

with each β a transposition. Then applying this to the polynomial P:

$$\begin{aligned} P = \epsilon(P) &= (\beta_1 \beta_2 \ldots \beta_r)(P) \\ &= (-1)^r P \end{aligned}$$

and so r must be even. □

Remark. The argument may not seem so convincing since we're using a specific case to find a property of the general S_n group. It may help to think of the counterfactual: if we could express the identity as a product of an odd number of transpositions, apply it to the Vandermode polynomial and we would get a contradiction.

Now the main theorem is easily proven.

Theorem 5.13. If a permutation α can be expressed as a product of an even (odd) number of transpositions, then every decomposition of α into a product of transpositions must have an even (odd) number of transpositions. In symbols, if

$$\alpha = \beta_1 \beta_2 \ldots \beta_r \quad \text{and} \quad \alpha = \gamma_1 \gamma_2 \ldots \gamma_s$$

where the β's and γ's are transpositions, then r and s have the same parity.

Proof. Observe that $\beta_1\beta_2\dots\beta_r = \gamma_1\gamma_2\dots\gamma_s$ implies that

$$\begin{aligned}\varepsilon &= \gamma_1\gamma_2\dots\gamma_s\beta_r^{-1}\dots\beta_2^{-1}\beta_1^{-1}\\ &= \gamma_1\gamma_2\dots\gamma_s\beta_r\dots\beta_2\beta_1\end{aligned}$$

since a transposition is its own inverse. Thus by Lemma 5.12, $s+r$ is even. It follows that r and s are both even or both odd. □

Definition 5.14. A permutation that can be expressed as a product of an even (odd) number of transpositions is called an *even (odd)* permutation.

Theorem 5.15. The set of even permutations in S_n forms a subgroup of S_n.

Proof. We use the One-Step Subgroup Test. We can write $\varepsilon = (12)(12)$, so it is in the set of even permutations. Let α and β be even permutations. Note that β^{-1} is even as well, so $\alpha\beta^{-1}$ must be even. □

Definition 5.16. The group of even permutations of n symbols is denoted by A_n and is called the *alternating group of degree n.*

Theorem 5.17. For $n \geq 2$, A_n has order $n!/2$.

Proof. Let B_n denote the set of odd permutations in S_n. For an odd permutation α, consider the function $f : B_n \to A_n$ defined by $f(\alpha) = (12)\alpha$. By cancellation properties we have $(12)\alpha = (12)\beta$ implies $\alpha = \beta$, so f is an injection; in other words $|B_n| \leq |A_n|$.

Similarly the function $g : A_n \to B_n$ defined by $g(\beta) = (12)\beta$ is an injection and so $|A_n| \leq |B_n|$. From this we conclude $|A_n| = |B_n|$ and since $A_n \cap B_n = \emptyset$, we obtain $|A_n| = n!/2$. □

Remark. The name *alternating* of A_n comes from polynomials where transpositions change (alternate) its sign, exactly as in the proof for Lemma 5.12.

6 Isomorphisms

Definition 6.1. A homomorphism $\phi : G \to \overline{G}$ is a mapping that preserves the group operation. That is,

$$\phi(ab) = \phi(a)\phi(b) \qquad \text{for all } a, b \text{ in } G.$$

There are names for special kinds of homomorphisms.

1. An injective homomorphism is also called a *monomorphism*
2. A surjective homomorphism is also called an *epimorphism*
3. A bijective homomorphism is also called an *isomorphism*

4. An isomorphism from a group onto itself is also called an *automorphism*

Definition 6.2. If there is an isomorphism $\phi : G \to \overline{G}$, we say that G and $\overline{G}$ are *isomorphic* and write $G \cong \overline{G}$.

Example 6.3. Let $G = \langle a \rangle$. If $|a| = \infty$ then $G \cong \mathbb{Z}$ via the isomorphism $\phi(a^k) = k$. On the other hand if $|a| = n < \infty$ then $G \cong \mathbb{Z}_n$ via the isomorphism $\phi(a^k) = k \pmod{n}$.

Theorem 6.4 (Properties of Isomorphisms on Elements)**.** Let $\phi : G \to \overline{G}$ be an isomorphism. Then:

1. $\phi(e)$ is the identity of $\overline{G}$.
2. $\phi(a^n) = [\phi(a)]^n$.
3. $ab = ba$ iff $\phi(a)\phi(b) = \phi(b)\phi(a)$....
4. $G = \langle a \rangle$ iff $\overline{G} = \langle \phi(a) \rangle$.
5. $|a| = |\phi(a)|$.
6. The equation $x^k = b$ has the same number of solutions in G as does the equation $x^k = \phi(b)$ in $\overline{G}$.
7. G and $\overline{G}$ have the same number of elements of each order.

Theorem 6.5 (Properties of Isomorphisms on Groups)**.** Let $\phi : G \to \overline{G}$ be an isomorphism. Then:

1. ϕ^{-1} is an isomorphism from $\overline{G}$ onto G.
2. G is Abelian iff $\overline{G}$ is Abelian.
3. G is cyclic iff $\overline{G}$ is cyclic.
4. If K is a subgroup of G, then $\phi(K)$ is a subgroup of $\overline{G}$.
5. $\phi(Z(G)) = Z(\overline{G})$

Theorem 6.6 (Cayley's Theorem)**.** Every finite group G is isomorphic to a group of permutations. In particular,

$$G \cong \{\pi_g : g \in G\}$$

Where $\pi_g(x) := gx$.

Proof. We will show that $\phi : G \to \overline{G}$ defined by

$$\phi(g) = \pi_g(x) \equiv gx$$

(i.e. $g \mapsto \pi_g$) is an isomorphism. Firstly, note that for any $g \in G$, π_g is indeed a permutation (i.e. a bijection), as for all $x, y \in G$,

$$\pi_g(x) = \pi_g(y) \implies gx = gy \implies x = y$$

and hence π_g is an injection. And for any $x \in G$ we have $\pi_g(g^{-1}x) = x$, so π_g is surjective.

Now let us show that $\overline{G} = \{T_g : g \in G\}$ is a group under function composition:

1. Function composition is associative.
2. Let $T_g \in \overline{G}$. Then for all x we have $T_g T_e(x) = gex = gx = egx = T_e T_g(x) = T_g(x)$ and so T_e is a proper identity.
3. Let $T_g \in \overline{G}$. Then
$$T_g T_{g^{-1}}(x) = gg^{-1}x = x = g^{-1}gx = T_{g^{-1}} T_g(x) = T_e(x)$$
for all x and hence each element has an inverse.

We have shown that $\overline{G}$ is indeed a group of permutations. We now proceed to show that $\phi : G \to \overline{G}$ is an isomorphism. By construction, ϕ is onto. And ϕ is one-to-one since

$$T_g = T_h \implies T_g(e) = T_h(e) \implies g = h.$$

We are left to show that ϕ is a homomorphism. Let $a, b \in G$. Then

$$\phi(ab) = T_{ab} = T_a T_b = \phi(a)\phi(b).$$

□

Definition 6.7. The group $\overline{G} = \{\pi_g : g \in G\}$ acting on the set G in Cayley's Theorem is called the *left regular representation of* G.

Remark. This $\overline{G}$ can be identified as a subgroup of $S_{|G|}$. Hence each π_g can be represented in disjoint cycle form.

Example 6.8. The left regular representation for $U(12) = \{1, 5, 7, 11\}$ can be obtained by writing the permutations of $U(12)$ in array form (much like a Cayley table):

$$T_1 = \begin{bmatrix} 1 & 5 & 7 & 11 \\ 1 & 5 & 7 & 11 \end{bmatrix}, \quad T_5 = \begin{bmatrix} 1 & 5 & 7 & 11 \\ 5 & 1 & 11 & 7 \end{bmatrix}$$

$$T_7 = \begin{bmatrix} 1 & 5 & 7 & 11 \\ 7 & 11 & 1 & 5 \end{bmatrix}, \quad T_{11} = \begin{bmatrix} 1 & 5 & 7 & 11 \\ 11 & 7 & 5 & 1 \end{bmatrix}$$

In cycle form we obtain:

$$T_1 = (1), \quad T_5 = (1,5)(7,11), \quad T_7 = (1,7)(5,11), \quad T_{11} = (1,11)(5,7)$$

Example 6.9. Let G be a group of order $2n$ where n is odd. Prove that if G has an element of order 2, then G has a subgroup of order n.

Proof. Let $a \in G$ with $|a| = 2$. Viewing G as a group of permutations, observe that since $\pi_a^2 = e$, the permutation π_a written in disjoint cycle form consists solely of transpositions. We cannot have a 1-cycle, since that would imply π_a sends an element to itself, which means $a = e$, a contradiction.

Thus, π_a consists of n transpositions, which means it is an odd permutation. Define $A := \{\sigma \in \overline{G} : \sigma \text{ is even}\}$ and $B := \{\tau \in \overline{G} : \tau \text{ is odd}\}$, the sets of odd and even permutations in $\overline{G}$. Then the mapping $\sigma \mapsto \pi_a\sigma$ is an injection from A to B and $\tau \mapsto \pi_a\tau$ is an injection from B to A. Therefore, $|A| = |B| = n$ and in fact A is a subgroup of order n, as desired. □

Definition 6.10. Let $g \in G$ be a group element. The map α_g defined by

$$\alpha_g(x) := gxg^{-1} \qquad \text{for all } x \text{ in } G$$

is called the *conjugation of* G or the *inner automorphism of* G *induced by* g.

Theorem 6.11. α_g is indeed an automorphism.

Definition 6.12. When G is a group, we use $\operatorname{Aut}(G)$ to denote the set of all automorphisms of G. We use $\operatorname{Inn}(G)$ to denote the set of all inner automorphisms of G.

Theorem 6.13. The sets $\operatorname{Aut}(G)$ and $\operatorname{Inn}(G)$ are groups under the operation of function composition.

Theorem 6.14. Let α be an automorphism of a cyclic group $\langle a\rangle$. Then α is completely determined by $\alpha(a)$.

Proof. Observe that for any $g^k \in \langle g\rangle$,

$$\alpha(g^k) = \underbrace{\alpha(g)\alpha(g)\ldots\alpha(g)}_{k\text{ terms}} = [\alpha(g)]^k.$$

□

Theorem 6.15. For every $n \in \mathbb{Z}^+$, we have $\operatorname{Aut}(\mathbb{Z}_n) \cong U(n)$.

Proof. By Theorem 6.14, any automorphism α of $\mathbb{Z}_n$ is determined by the value of $\alpha(1)$, and $\alpha(1) \in U(n)$ since only elements of $U(n)$ function as generators. Let us show that $T : \operatorname{Aut}(\mathbb{Z}_n) \to U(n)$ determined by

$$T(\alpha) = \alpha(1)$$

is an isomorphism. It is injective, for if $\alpha, \beta \in \operatorname{Aut}(\mathbb{Z}_n)$ and $\alpha(1) = \beta(1)$, then $\alpha(k) = k\alpha(1) = k\beta(1) = \beta(k)$. It is surjective, since for any $r \in U(n)$ take the function $\alpha : \mathbb{Z}_n \to \mathbb{Z}_n$ defined by

$$\alpha(s) := sr \pmod{n}$$

which is indeed an automorphism because we recognize $\alpha^{-1} := sr^{-1} \pmod{n}$ is its inverse (it is important here that $r \in U(n)$ so that r^{-1} is well-defined.) We have $T(\alpha) = \alpha(1) = r$, showing that T is onto.

Finally we establish that T is operation-preserving. Let $\alpha, \beta \in \mathrm{Aut}(\mathbb{Z}_n)$. We then have

$$\begin{aligned}
T(\alpha\beta) &= (\alpha\beta)(1) \\
&= \alpha(\beta(1)) \\
&= \alpha(\underbrace{1 + 1 + \cdots + 1}_{\beta(1)}) \\
&= \underbrace{\alpha(1) + \alpha(1) + \cdots + \alpha(1)}_{\beta(1)} \\
&= \alpha(1)\beta(1) \\
&= T(\alpha)T(\beta).
\end{aligned}$$

□