Abstract algebra

Krisztián Szabó

Source: Contemporary Abstract Algebra by Joseph A. Gallian

Content

1 Integers and Equivalence Relations

1.1 Properties of integers

Much of abstract algebra involves properties of integers and sets. In this chapter we collect the properties we need for future reference. An important property of the integers, which we will often use, is the so-called *Well ordering principle*. Since this property cannot be proved from the usual properties of arithmetic, we will take it as an axiom.

1.1.1 Well ordering principle

Every nonempty set of positive integers contains a smallest member.

1.1.2 Division algorithm

Theorem. Let a and b be integers with $b > 0$. Then there exists unique integers q and r with the property that $a = bq + r$, where $0 \leq r < b$.

Proof. We begin with the existence portion of the theorem. Consider the set $S = \{a - bk \mid k \text{ is and integer and } a - bk \geq 0\}$. If $0 \in S$, then b divides a and we may obtain the desired result with $q = \frac{a}{b}$ and $r = 0$. Now assume $0 \notin S$. Since S is nonempty $\big($if $a > 0$, $a - b \cdot 0 \in S$; if $a < 0$, $a - b(2a) = a(1 - 2b) \in S$; $a \neq 0$ since $0 \neq S\big)$, we may apply the Well ordering principle to conclude that S has a smallest member, say $r = a - bq$. Then $a = bq + r$ and $r \geq 0$, so all that remains to be proved that $r < b$.

If $r \geq b$, then $a - b(q + 1) = a - bq - b = r - b \geq 0$, so that $a - b(q + 1) \in S$. But $a - b(q + 1) < a - bq$, and $a - bq$ is the smallest member of S. So $r < b$.

To establish the uniqueness of q and r, let us assume that there are integers q, q', r, and r' such that

$$a = bq + r, \quad 0 \leq r < b \quad \text{and} \quad a = bq' + r', \quad 0 \leq r' < b.$$

For convenience, we may also suppose that $r' \geq r$. Then $bq + r = bq' + r'$ and $b(q - q') = r' - r$. So, b divides $r' - r$ and $0 \leq r' - r \leq r' < b$. It follows that $r' - r = 0$.

1.1.3 Greatest common divisor, relatively prime integers

Definition. The *greatest common divisor* of two nonzero integers a and b is the largest of all common divisors of a and b. We denote this integer by $gcd(a, b)$, when $gcd(a, b) = 1$, we say a and b are *realively prime*.

1.1.4 GCD is a linear combination

Theorem. For any nonzero integers a and b, there exists integers s and t such that $gcd(a, b) = as + bt$. Moreover, $gcd(a, b)$ is the smallest positive integer of the form $as + bt$.

Proof. Consider the set $S = \{am + bn \mid m, n \text{ are integeres and } am + bn > 0\}$. Since S is obviously nonempty, the Well ordering principle asserts that S has a smallest member, say, $d = as + bt$. We claim that $d = gcd(a, b)$. To verify this claim, use the division algorithm to write $a = dq + r$, where $0 \leq r < d$. If $r > 0$, then $r = a - dq = a - (as + bt)q = a - asq - btq = a(1 - sq) + b(-tq) \in S$, contradicting the fact that d is the smallest member of S.

So, $r = 0$ and d divides a. Analogously (or, better yet, by symmetry), d divides b as well. This proves that d is a common divisor of a and b. Now suppose d' is another common divisor of a nad b and write $a = d'h$ and $b = d'k$. Then $d = as + bt = (d'h)s + (d'k)t = d'(hs + kt)$, so that d' is a divisor of d. Thus, among all common divisors of a and b, d is the greatest.

Corollary. If a and b are relatively prime, than there exist integers s and t such that $as + bt = 1$.

1.1.5 Euclid's lemma

Lemma. If p is is prime that divides ab, then p divides a or p divides b.

Proof. Suppose p is a prime that divides ab but does not divide a. We must show that p divides b. Since p does not divide a, ther are integers s and t such that $1 = as + pt$. Then $b = abs + ptb$. and since p divides the right-hand side of the equation, p also divides b.

1.1.6 Fundamental theorem of arithmetic

Theorem. Every integer greater than 1 is a prime or a product of primes. This product is unique, except the order in which the factors appear. That is, if $n = p_1 p_2 \cdots p_r$ and $n = q_1 q_2 \cdots q_s$, where the p's and q's are primes, then $r = s$ and, after renumbering the q's, we have $p_i = q_i$ for all i.

Proof. Later.

1.1.7 Least common multiple

Definition. The *least common multiple* of two nonzero integers a and b is the smallest positive integer that is a multiple of both a and b. We will denote this integer by $lcm(a, b)$.

1.2 Mathematical induction

1.2.1 Fist principle of mathematical induction

Theorem. Let S be a set of integers containing a. Suppose S has the property that whenever some integer $n \geq a$ belongs to S, then the integer $n + 1$ also belongs to S. Then, S contains every integer greater than or equal to a.

Proof. S contains a. But if S contains an element $n \geq a$, then $n + 1$ is also in S. So $a + 1$ is also in S. But S contains the element $a + 1$, so $a + 2$ is also in S. This gives us the result, that S contains all the integers greater than or equal to a.

1.2.2 Second principle of mathematical induction

Theorem. Let S be a set of integers containing a. Suppose S has the property that n belongs to S whenever every integer less then n and greater than or equal to a belongs to S. Then, S contains every integer greater than or equal to a.

Proof. S contains a. Let n_1 be $a + 1$. All the numbers that are less than n_1 and greater than or equal to a is only a, and it is in S, so $a + 1$ is also in S. Let n_2 be $a + 2$. The numbers that are less than n_2 and greater than or equal to a are $n_2 = a + 2 > n_1 = a + 1 > a \geq a$. So n_2 is also in S. This, again gives us the result that all the integers that are greater than or equal to a are in S.

To use this form of induction, we first show that the statement is true for the integer a. We then assume that the statement is true for all integers that are greater than or equal to a and less then n, and use this assumption to prove that the statement is true for n.

Clarity. So what have just we proven? We prooved that **if** all integers that are less than n and greater than or equal to a are in S, **then** n is also in S. And most importantly, a is also in S. Look at $a+1$, the first half holds, because a is in S, so $a+1$ must be in S. Look at $a+2\ldots$

1.3 Equivalence relations

1.3.1 Equivalence relation

Definition. An *equivalence relation* on a set S is a set R of ordered pairs of elements of S such that

1. $(a, a) \in R$ for all $a \in S$ (reflexive property).
2. $(a, b) \in R$ implies $(b, a) \in R$ (symmetric property).
3. $(a, b) \in R$ and $(b, c) \in R$ imply $(a, c) \in R$ (transitive property).

When R is an equivalence relation on a set S, it is customary to write aRb instead of $(a, b) \in R$. Also, since an equivalence relation is just a generalization of equality, a suggestive symbol such as $\approx$, $\equiv$, $\sim$. Using this notation, the three conditions for an equivalence relation become $a \sim a$; $a \sim b$ implies $b \sim a$; and $a \sim b$ and $b \sim c$ imply $a \sim c$. If $\sim$ is an equivalence relation on a set S and $a \in S$, then the set $[a] = \{x \in S \mid x \sim a\}$ is called the equivalence class of S containing a.

Example. Let S be the set of **all** polynomials with the real coefficients. If f, $g \in S$ define $f \sim g$ if $f' = g'$, where f' is the derivative of f. Then, $\sim$ is an equivalence relation on S. Since two polynomials with equal derivatives differ by a constant, we see that for any f in S, $[f] = \{f + c \mid c \text{ is real}\}$.

Example. Let S be the set of integers and let n be a positive integer. If a, $b \in S$, define $a \equiv b$ if $a \bmod n = b \bmod n$. (that is, if $a - b$ is divisible by n). Then, $\equiv$ is an equivalence relation on S. and $[a] = \{a + kn \mid k \in S\}$. Since this particular relation is important in abstract algebra, we will take the trouble to verify that it is indeed an equivalence relation. Certainly, $a - a$ is divisible by n, so that $a \equiv a$ for all a in S. Next, assume that $a \equiv b$, say, $a - b = rn$. Then $b - a = (-r)n$, and therefore $b \equiv a$. Finally, assume that $a \equiv b$ and $b \equiv c$, say $a - b = rn$ and $b - c = sn$. Then, we have $a - c = (a - b) + (b - c) = rn + sn = (r + s)n$, so that $a \equiv c$.

1.3.2 Partition

Definition. A *partition* of a set S is a collection of nonempty disjoint subsets of S whose union is S.

1.3.3 Equivalence classes partition

Theorem. The equivalence classes of an equivalence relation on a set S constitute a partition of S. Conversely, for any partition P of S, there is an equivalence relation on S whose equivalence classes are the element of P.

Proof. Let $\sim$ be an equivalence relation on a set S. For any $a \in S$, the reflexive property shows that $a \in [a]$. So, $[a]$ is a nonempty and the union of all equivalence classes is S. Now, suppose that $[a]$ and $[b]$ are distinct equivalence classes. We must show that $[a] \cap [b] = \emptyset$. On the contrary, assume $c \in [a] \cap [b]$. We will show that $[a] \subseteq [b]$. To this end, let $x \in [a]$. We then have $c \sim a$, $c \sim b$, and $x \sim a$. By the symmetric property, we also have $a \sim c$. Thus, by transitivity, $x \sim c$, and transitivity again, $x \sim b$. This proves $[a] \subseteq [b]$. Analogously, $[b] \subseteq [a]$. Thus, $[a] = [b]$, in contradiction to our assumption that $[a]$ and $[b]$ are distinc equivalence classes.

To prove the converse, let P be a collection of nonempty disjoint subsets of S whose union is S. Define $a \sim b$ if a and b belong to the same subset in the collection.

1.4 Functions (mappings)

Although the concept of a function plays a central role in nearly every branch of mathematics, the terminology and notation associated with functions vary quite a bit. In this section, we establish ours.

1.4.1 Function (mapping)

Definition. A *function* (or mapping) ϕ from a set A to a set B is a rule that assigns to each element a of A exactly one element b of B. The set A is called the *domain* of ϕ, and B is called the *range* of ϕ. If ϕ assigns b to a, then b is called the *image of a under ϕ*. The subset of B comprising all the images of elements of A is called the *image of A under ϕ*.

We use the shorthand $\phi : A \to B$ to mean that ϕ is a mapping from A to B. We will write $\phi(a) = b$ or $\phi : a \to b$ indicate that ϕ carries a to b.

1.4.2 Composition of functions

Definition. Let $\phi : A \to B$ and $\psi : B \to C$. The *composition* $\psi\phi$ is the mapping from A to C defines by $(\psi\phi)(a) = \psi(\phi(a))$ for all a in A.

1.4.3 One-to-one function

Definition. A function ϕ from a set A is called *one-to-one* if for every a_1, $a_2 \in A$, $\phi(a_1) = \phi(a_2)$ implies $a_1 = a_2$.

1.4.4 Function from A onto B

Definition. A function ϕ from A to a set B is said to be *onto B* if each element of B is the image of at least one element of A. In symbols, $\phi : A \to B$ is onto if for each b in B there is at least one a in A such that $\phi(a) = b$.

1.4.5 Properties of functions

Theorem. Given functions $\alpha : A \to B$, $\beta : B \to C$, and $\gamma : C \to D$, then

1. $\gamma(\beta\alpha) = (\gamma\beta)\alpha$ (associativity).
2. If α and β are one-to-one, then $\beta\alpha$ is one-to-one.
3. If α and B are onto, then $\beta\alpha$ is onto.
4. If α is one-to-one and oneto, then there is a function α^{-1} from B onto A such that $(\alpha^{-1}\alpha)(a) = a$ for all a in A and $(\alpha\alpha^{-1})(b) = b$ for all b in B.

Proof. we prove only part 1. The remaining parts are left as exercises. Let $a \in A$. Then $(\gamma(\beta\alpha))(a) = \gamma((\beta\alpha)(a)) = \gamma(\beta(\alpha(a)))$ On the other hand, $((\gamma\beta)\alpha)(a) = (\gamma\beta)(\alpha(a)) = \gamma(\beta(\alpha(a)))$.

2 Groups

2.1 Definition of groups

The term *group* was used by Galois around 1830 to describe sets of one-to-one functions on finite sets that could be grouped together to form a set closed under composition. As is the case with most fundamental concepts in mathematics, the modern definition of a group that follows is the result of a long evolutionary process. Although this definition was given by both Heinrich Weber and Walter von Dyck in 1882, it did not gain universal acceptance until the 20th century.

2.1.1 Binary operation

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

2.1.2 Group

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

1. *Associativity.* The operation is associative; that is, $(ab)c = a(bc)$ for all a, b, c in G.
2. *Identity.* There is an element e (called *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 $ab = ba = e$.

If a group has the property that $ab = ba$ for every pair of elements a and b, we say the group is *Abelian*.

2.2 Elementary properties of groups

2.2.1 Uniqueness of the identity

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

Proof. Suppose both e and e' are indentities of G. Then,

1. $ae = a$ for all a in G, and
2. $e'a = a$ for all a in G.

The choices of $a = e'$ in 1. and $a = e$ in 2. yield $e'e = e'$ and $e'e = e$. Thus, e and e' are both equal to $e'e$ and so are equal to each other.

2.3 Cancellation

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

Proof. Suppose $ba = ca$. Let a' be an inverse of a. Then, muliplying on the right by a' yields $(ba)a' = (ca)a'$. Associativity yields $b(aa') = c(aa')$. Then, $be = ce$ and, therefore, $b = c$ as desired. Simirarly, one can prove that $ab = ac$ implies $b = c$ by multiplying by a' on the left.

2.3.1 Uniqueness of inverses

Theorem. For each element a in a group G, there is a unique element b in G such that $ab = ba = e$.

Proof. Suppose b and c are both inverses of a. Then $ab = e$ and $ac = e$, so that $ab = ac$. Canceling the a on both sides gives $b = c$, as desired.

We may unambiguously denote it by g^{-1}. This notation is suggested by that used for ordinary real numbers under multiplication. Similarly, when n is a positive integer, the associative law allows us to use g^n to deont the unambiguous product

$$\underbrace{gg\cdots g.}_{n \text{ factors}}$$

We define $g^0 = e$. When n is negative, we define $g^n = (g^{-1})^{|n|}$. Unlike for real numbers, in an abstract algebra group we do not permit noninteger exponents such as $g^{1/2}$. With this notation, the familiar laws of exponents hold for groups; that is, for all integers m and n and any group element g, we have $g^m g^n = g^{m+n}$ and $(g^m)^n = g^{mn}$. Although the laws of exponents fail to hold for expressions involving two group elements. Thus, for groups in general, $(ab)^n \neq a^n b^b$.
Also, one must be careful with this notation when dealing with a specific group whose binary

operation is addition and is denoted by "+". In this case, the definitions and group properties expressed in multiplicative notation must be translated to additive notation. For example, the inverse of g is written as $-g$. Likewise, for example, g^3 means $g + g + g$ and is usually written as $3g$, whereas g^{-3} means $(-g) + (-g) + (-g)$.

2.3.2 Socks-shoes property

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

Proof. Since $(ab)(ab)^-1 = e$ and $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$, we have by the theorem of uniqueness of inverses that $(ab)^-1 = b^{-1}a^{-1}$.

3 Finite groups; subgroups

3.1 Terminology and notation

As we will soon discover, finite groups - that is, groups with finitely many elements - have interesting arithmetic properties. To faciliate the study of finite groups, it is convenient to introduce some terminology and notation.

3.1.1 Order of a group

Definition. The number of elements of a group (finite or infinite) is called its *order*. We will use $|G|$ to denote the order of G.

Thus, the group Z of integers under addition has infinite order, whereas the group $U(10) = \{1, 3, 5, 7\}$ under multiplication modulo 10 has order 4.

3.1.2 Order of an element

Definition. The *order* of an element g in a group G is the smallest positive integer n such that $g^n = e$. (In additive notation, this would be $ng = 0$.) If no such integer exists, we say that g has *infinite order*. The order of an element g is denoted by $|g|$.

So, to find the order of a group element g, you need only compute the sequence of products g, g^2, g^3, ..., until you reach the indentity for the first time. The exponenet of this product (or coefficient if the operation is addition) is the order of g. If the indentity never appears in the sequence, then g has infinite order.

3.1.3 Subgroup

Definition. 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.

We use the notation $H \leq G$ to mean that H is a subgroup of G. If we want to indicate that H is a subgroup of G but is not equal to G itself, we write $H < G$. Such a subgroup is called a *proper subgroup*. The subgroup $\{e\}$ is called the *trivial subgroup* of G; a subgroup that is not $\{e\}$ is called a *nontrivial subgroup* of G.
Notice that Z_n under addition modulo n is not a subgroup of Z under addition, since addition modulo n is not the operation of Z.

3.2 Subgroup tests

When determining whether or not a subset H of a group G is a subgroup of G, one need not directly verify the group axioms. The next three results provide simple tests that suffice to show that a subset of a group is a subgroup.

3.2.1 One-step subgroup test

Theorem. Let G be a group and H a nonempty subset of G. If ab^{-1} is in H whenever a and b are in H, then H is a subgroup of G. (In additive notation, if $a - b$ is in H whenever a and b are in H, then H, is a subgroup of G.)

Meaning of whenever: if a and b are in H, then ab^{-1} is also in H.

Proof. Since the operation of H is the same as that of G, it is clear that this operation is associative. Next, we show that e is in H. Since H is nonempty, we may pick some x in H. Then, letting $a = x$ and $b = x$ in the hypothesis, we have $e = xx^{-1} = ab^{-1}$ is in H. To verify that x^{-1} is in H whenever x is in H, all we need to do is choose $a = e$ and $b = x$ in the statement of the theorem. Finally, the proof will be complete when we show that H is closed; that is, if x, y belong to H, we must show that xy is in H also. Well, we have already shown that y^{-1} is in H whenever y is; so, letting $a = x$ and $b = y^{-1}$, we have $xy = x(y^{-1})^{-1} = ab^{-1}$ is in H.

There are actually four steps involved in applying the theorem. Notice the similarity between the last three steps listed below and the three steps involved in the Principle of the mathematical induction.

1. Identify the property P that distinguishes the elements of H; that is, identify a defining condition.
2. Prove that the identity has property P. (This verifies that H is nonempty.)
3. *Assume* that two elements a and b have property P.
4. Use the assumption that a and b have property P to show that ab^{-1} has property P.

Example. Let G be an Abelian group with identity e. Then $H = \{x \in G \mid x^2 = e\}$ is a subgroup of G. Here, the defining property of H is the condifiton $x^2 = e$. So, we first note that $e^2 = e$, so that H is nonempty. Now assume that a and b belong to H. This means $a^2 = b^2 = e$. Finally, we must show that $(ab^{-1})^2 = e$. Since G is Abelian, $(ab^{-1})^2 = ab^{-1}ab^{-1} = a^2(b^{-1})^2 = a^2(b^2)^{-1} = ee^{-1} = e$. Therefore, ab^{-1} belongs to H and, by the One-step subgroup test, H is a subgroup of G.

3.2.2 Two-step subgroup test

Theorem. Let G be a group and let H be a nonempty subset of G. If ab is in H whenever a and b are in H (H is closed under the operation), and a^{-1} is in H (H is closed under taking inverses), then H is a subgroup of G.

Proof. By the One-step subgroup test theorem, it suffices to show that $a, b \in H$ implies $ab^{-1} \in H$. So, we suppose that $a, b \in H$. Since H is closed under taking inverses, we also have $b^{-1} \in H$. This, $ab^{-1} \in H$ by closure under multiplication.

When dealing with finite groups, it is easier to use the following subgroup test.

3.2.3 Finite subgroup test

Theorem. 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. In view of the Two-step subgroup test, we need only prove that $a^{-1} \in H$ whenever $a \in H$. If $a = e$, then $a^{-1} = a$ and we are done. If $a \neq e$, consider the sequence $a, a^2, \ldots$. By closure, all of these elments belong to H. Since H is finite, not all of these elements are distinct. Say $a^i = a^j$ and $i > j$. Then, $a^{i-j} = e$; and since $a \neq e$, $i - j > 1$. Thus, $aa^{i-j-1} = a^{i-j} = e$ and, therefore, $a^{i-j-1} = a^{-1}$. But, $i - j - 1 \geq 1$ implies $a^{i-j-1} \in H$ and we are done.

3.3 Example of subgroups

The proofs of the next few theorems show how our subgroup tests work. We first introduce an important notation. For any element a from a group, we let $\langle a \rangle$ denote the set $\{a^n \mid n \in Z\}$. In particular, observe that exponents of a include all negative integers as well as 0 and the positive integers (a^0 is defined to be the identity).

3.3.1 $\langle a \rangle$ is a subgroup

Theorem. Let G be a group, and let a be any element of G. Then, $\langle a \rangle$ is a subgroup of G.

Proof. Since $a \in \langle a \rangle$, $\langle a \rangle$ is not empty. Let a^n, $a^m \in \langle a \rangle$. Then, $a^n(a^m)^{-1} = a^{n-m} \in \langle a \rangle$; so, by the one-step subgroup test theorem, $\langle a \rangle$ is a subgroup of G.

The subgroup $\langle a \rangle$ is called the *cyclic subgroup of G generated by a*. In the case that $G = \langle a \rangle$, we say that G is *cyclic* and a is a *generator of G*. (A cyclic group may have many generators.) Notice that although the list $\ldots, a^{-2}, a^{-1}, a^0, a^1, a^2, \ldots$ has infinitely many entries, the set $\langle a \rangle = \{a^n \mid n \in Z\}$ might have only finitely many elements. Also note that, since $a^i a^j = a^{i+j} = a^{j+i} = a^j a^i$, every cyclic group is Abelian.

Example. In $U(10)$, $\langle a \rangle = \{3, 9, 7, 1\} = U(10)$, for

$$3^1 = 3,\ 3^2 = 9,\ 3^3 = 7,\ 3^4 = 1,\ 3^5 = 3^4 \cdot 3 = 1 \cdot 3;$$

$$3^{-1} = 7 \text{ (since } 3 \cdot 7 = 1),\ 3^{-2} = 9,\ 3^{-3} = 3$$

We next consider one of the most important subgroups.

3.3.2 Center of a group

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

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

3.3.3 Center is a subgroup

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

Proof. We will use the Two-step subgroup test theorem. Clearly, $e \in Z(G)$, so $Z(G)$ is nonempty. Now, suppose $a, b \in Z(G)$. We have to show that ab is in $Z(G)$; so that, ab commutes with every element $x \in G$. Then $(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$. (Since $a, b \in Z(G)$, so they commute with every x in G.)

Next, assume that $a \in Z(G)$. Then we have $ax = xa$ for all x in G. What we want is $a^{-1}x = xa^{-1}$ for all x in G.

$$a^{-1}(ax)a^{-1} = a^{-1}(xa)a^{-1}$$

$$(a^{-1}a)xa^{-1} = a^{-1}x(aa^{-1})$$

$$exa^{-1} = a^{-1}xe$$

$$xa^{-1} = a^{-1}x$$

This shows that $a^{-1} \in Z(G)$ whenever a is.

3.3.4 Centralizer of a in G

Let a be a fixed element of a group G. The *centralizer of a in G*, $C(a)$, is the set of all element in G that commute with a. In symbols

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

3.3.5 $C(a)$ is a subgroup

Theorem. For each a in G, the centralizer of a is a subgroup of G.

Proof. Similar to the proof of the "Center is a subgroup" theorem.

4 Cyclic groups

4.1 Properties of cyclic groups

Recall from chapter "Finite groups; subgroups" that a group G is cyclic if there is an element a in G such that $G = \langle a \rangle = \{a^n \mid n \in Z\}$. Such an element a is called a generator of G. In this chapter, we examine cyclic groups in detail and determine their important characteristics.

Example. The set of integers Z under ordinary addition is cyclic. Both 1 and -1 are generators. (Recall that, when the operation is addition, 1^n is interpreted as

$$\underbrace{1+1+\cdots+1}_{n \text{ terms}}$$

when n is positive, and as

$$\underbrace{(-1)+(-1)+\cdots+(-1)}_{|n| \text{ terms}}$$

when n is negative.)

Example. The set $Z_n = \{0, 1, \ldots, n-1\}$ for $n \geq 1$ is a cyclic group under addition modulo n. Again, 1 and $-1 = n-1$ are generators.

Example. $Z_8 = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle$. Te verify, for instance, that $Z_8 = \langle 3 \rangle = 3, 3+3, 3+3+3, \ldots$ is the set $\{3, 6, 1, 4, 7, 2, 5, 0\} = Z_8$. Thus, 3 is a generator of Z_8.

4.1.1 Criterion for $a^i = a^j$

Theorem. Let G be a group, and let a belong to G. If a has infinite order, then $a^i = a^j$ if and only if $i = j$. If a has finite order, say n, then

$$\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$$

and $a^i = a^j$ if and only if n divides $i - j$.

Proof. If a has infinite order, there is no nonzero n such that $a^n = e$. Since $a^i = a^j$ implies $a^{i-j} = e$, we must have $i - j = 0$, and the first statement of the theorem is proved.

Now assume that $|a| = n$. We will prove that $\langle a \rangle = \{e, a, a^2, a^3, \ldots, a^{n-1}\}$. Certainly, the elements $e, a, \ldots, a^{n-1}$ are in $\langle a \rangle$

Now, suppose that a^k is an arbitrary member of $\langle a \rangle$. By the division algorithm, there exist integers q and r such that

$$k = qn + r \quad 0 \leq r < n.$$

Then $a^k = a^{qn+r} = a^{qn}a^r = (a^n)^q a^r = e^q a^r = ea^r = a^r$, so that $a^k \in \{e, a, a^2, a^3, \ldots, a^{n-1}\}$.

Next, we assume that $a^i = a^j$ and prove that n divides $i - j$. We begin by observing that $a^i = a^j$ implies $a^{i-j} = e$. Again, by the division algorithm, there are integers q and r such that

$$i - j = qn + r \quad \text{with} \quad 0 \leq r < n.$$

Then $a^{i-j} = a^{qn+r}$, and therefore $e = a^{i-j} = a^{qn+r} = (a^n)^q a^r = e^q a^r = ea^r = a^r$. Since n is the least positive integer such that a^n is the identity, we must have $r = 0$, so that n divides $i - j$.

Conversely, if $i - j = nq$, then $a^{i-j} = a^{nq} = e^q = e$, so that $a^i = a^j$.

4.1.2 $|a| = |\langle a \rangle|$

Corollary. For any group element a, $|a| = |\langle a \rangle|$.

Proof. It comes from the fact that if $|a| = n$, then $\langle a \rangle = \{e, a, a^2, a^3, \ldots, a^{n-1}\}$.

One special case of the theorem "Criterion for $a^i = a^j$" occurs so often that it deserves singling out.

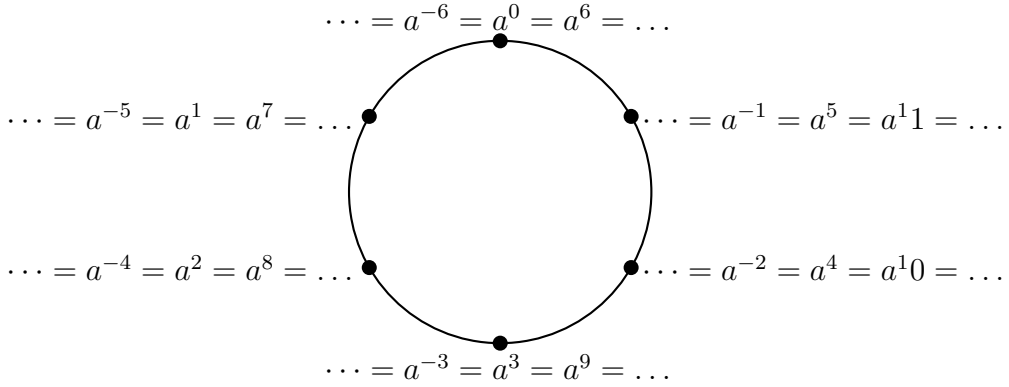
4.1.3 $a^k = e$ implies that $|a|$ divides k

Corollary. Let G be a group and let a be an element of order n in G. If $a^k = e$, then n divides k.

Proof. Since $a^k = e = a^0$, we know by the theorem "Criterion for $a^i = a^j$" that n divides $k - 0 = k$.

The theorem "Criterion for $a^i = a^j$" and its corollaries for the case $|a| = 6$ are illustrated in the figure below.

What is important about the theorem in the finite case is that it says that multiplication in $\langle a \rangle$ is essentially done by *addition* modulo n. That is, if $(i + j) \bmod n = k$, then $a^i a^j = a^k$. This, no matter what group G os, or how the element a is chosen, multiplication in $\langle a \rangle$ works the same as addition in Z_n whenever $|a| = n$. Simirarly, if a has infinite order, then multiplication in $\langle a \rangle$ works the same as addition in Z, since $a^i a^j = a^{i+j}$ ano no modular arithmetic is done.



For these reasons, the cyclic groups Z_n and Z serve as prototypes for all cyclic groups, and algebraists say that there is essentially only one cyclic group of each order. What is meant by this is that, although there may be many different sets of the form $\{a^n \mid n \in Z\}$, there is essentially only one way to operate on these sets. Algebraists do not really care what the elements of a set are; they care only about the algebraic properties of the set- that is, the ways in which the elements of a set can be combined.

The next theorem provides a simple method for computing $|a^k|$ knowing only $|a|$, and its first corollary provides a simple way to tell when $\langle a^i \rangle = \langle a^j \rangle$.

4.2 $\langle a^k \rangle = \langle a^{\mathbf{gcd}(n,k)} \rangle$

Theorem. Let a be an element of order n in a group and let k be a positive integer. Then $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ and $|a^k| = \frac{n}{\gcd(n,k)}$

Proof. To simplify the notation, let $d = \gcd(n, k)$ and let $k = dr$. Since $a^k = a^{dr} = (a^d)^r$, we have by clouse that $\langle a^k \rangle \subseteq \langle a^d \rangle$. By the gcd theorem, there are integers s and t such that $d = ns + kt$. So, $a^d = a^{ns+kt} = a^{ns} a^{kt} = (a^n)^s a^{kt} = e(a^k)^t = (a^k)^t \in \langle a^k \rangle$. This proves $\langle a^d \rangle \subseteq \langle a^k \rangle$. So, we have verified that $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$.

We prove the second part of the theorem by showing first that $|a^d| = \frac{n}{d}$ for any divisor d of n.

Clearly, $(a^d)^{n/d} = a^n = e$, so that $|a^d| \leq \frac{n}{d}$. On the other hand, if i is a positive integer less then $\frac{n}{d}$, then $(a^d)^i \neq e$ by definition of $|a|$. We now apply this fact with $d = \gcd(n, k)$ to obtain $|a^k| = |\langle a^k \rangle| = |\langle a^{\gcd(n,k)} \rangle| = |a^{\gcd(n,k)}| = \frac{n}{\gcd(n,k)}$.

The advantage of the 4.2 theorem is that it allows us to replace one generator of a cyclic subgroup with a more convenient one. For example, if $|a| = 30$, we have $\langle a^{26} \rangle = \langle a^2 \rangle$, $\langle a^{22} \rangle = \langle a^2 \rangle$, $\langle a^{21} \rangle = \langle a^3 \rangle$. From this we can easily see that $|a^{23}| = 30$ and $|a^{22}| = 15$. Moreover, if one wants to list the elements of, say, $\langle a^{21} \rangle$, it is easier to list the elements of $\langle a^3 \rangle$ instead. Theorem 4.2 establishes an important relationship between the order of an element in a finite cyclic group and the order of the group.

4.2.1 Orders for elements in finite cyclic groups

Corollary. In a finity cyclic group, the order of an element divides the order of the group.

4.2.2 Criterion for $\langle a^i \rangle = \langle a^j \rangle$ and $|a^i| = |a^j|$

Corollary. Let $|a| = n$. Then $\langle a^i \rangle = \langle a^j \rangle$ if and only if $\gcd(n, j) = \gcd(n, i)$ and $|a^i| = |a^j|$ if and only if $\gcd(n, j) = \gcd(n, i)$.

Proof. Theorem 4.2 shows that $\langle a^i \rangle = \langle a^{\gcd(n,i)} \rangle$ and $\langle a^j \rangle = \langle a^{\gcd(n,j)} \rangle$, so that the proof reduces to proving that $\langle a^{\gcd(n,i)} \rangle = \langle a^{\gcd(n,j)} \rangle$ if and only if $\gcd(n, i) = \gcd(n, j)$. Certainly, $\gcd(n, i) = \gcd(n, j)$ implies that $\langle a^{\gcd(n,i)} \rangle = \langle a^{\gcd(n,j)} \rangle$. On the other hand, $\langle a^{\gcd(n,i)} \rangle = \langle a^{\gcd(n,j)} \rangle$ implies that $|a^{\gcd(n,i)}| = |a^{\gcd(n,j)}|$, so that by the second conclusion of Theorem 4.2, we have $n/\gcd(n, i) = n/\gcd(n, j)$, and therefor $\gcd(n, i) = \gcd(n, j)$.

4.3 Generators of finite cyclic groups

Corollary. Let $|a| = n$. Then $\langle a \rangle = \langle a^j \rangle$ if and only if $\gcd(n, j) = 1$ and $|a| = |\langle a^j \rangle|$ if and only if $\gcd(n, j) = 1$.

4.3.1 Generators of Z_n

Corollary. An integer k in Z_n is a generator of Z_n if and only if $\gcd(n, k) = 1$.

4.4 Classification of subgroups of cyclic groups

4.4.1 Fundamental theorem of cyclic groups

Theorem. Every subgroups of a cyclic groups is cyclic. Moreover, if $|\langle a\rangle| = n$, then the order of any subgroup of $\langle a\rangle$ is a divisor of n; and, for each positive divisor k of n, the group $\langle a\rangle$ has exactly one subgroup of order k, namely, $\langle a^{\frac{n}{k}}\rangle$.

Before we prove this theorem, let's see what it means. Suppose $G = \langle a\rangle$ and G has order 30. The first and second parts of the theorem say that if H is any subgroup of G, then H has the form $\langle a^{\frac{30}{k}}\rangle$ for some k that is divisor of 30. The third part of the theorem says that G has one subgroup of each of the orders 1, 2, 3, 5, 6, 10, 15, and 30-and no others. The proof will also show how to find these subgroups.

Proof. Let $G = \langle a\rangle$ and suppose that H is a subgroup of G. We must show that H is cyclic. If it consists of the identity alone, then clearly H is cyclic. So we may assume that $H \neq \{e\}$. We now claim that, H contains an element of the form a^t, where t is positive. Since $G = \langle a\rangle$, every element of H has the form of a^t; and when a^t belongs to H with $t < 0$, then a^{-t} belongs to H also and $-t$ is positive. Thus, our claim is verified. Now let m be the least positive integer such that $a^m \in H$. By closure, $\langle a^m\rangle \subseteq H$. We next claim that $H = \langle a^m\rangle$. To prove this claim, if suffices to let b be an arbitrary member of H and show that b is in $\langle a^m\rangle$. Since $b \in G = \langle a\rangle$, we have $b = a^k$ for some k. Now, apply the division algorithm to k and m to obtain integers q and r such that $k = mq + r$ where $0 \leq r < m$. Then $a^k = a^{mq+r} = a^{mq}a^r$, so that $a^r = a^{-mq}a^k$. Since $a^k = b \in H$ and $a^{-mq} = (a^m)^{-q}$ is in H also, $a^r \in H$. But, m is the least positive integer such that $a^m \in H$, and $0 \leq r < m$, so r must be 0. Therefore, $b = a^k = a^{mq} = (a^m)^q \in \langle a^m\rangle$. This proves the assertion of the theorem that every subgroup of a cyclic group is cyclic.

To prove the next portion of the theorem, suppose that $|\langle a\rangle| = n$ and H is any subgroup of $\langle a\rangle$. We have already shown that $H = \langle a^m\rangle$, where m is the least positive integer such that $a^m \in H$. Using $e = b = a^n$ as in the preceding paragraph, we have $n = mq$.

Finally, let k be any positive divisor of n. We will show that $\langle a^{\frac{n}{k}}\rangle$ is the one and only subgroup of $\langle a\rangle$ order k. From Theorem 4.2 we see that $\langle a^{\frac{n}{k}}\rangle$ has order $\frac{n}{\gcd\left(n, \frac{n}{k}\right)} = \frac{n}{\frac{n}{k}} = k$. Now let H be any subgroup of $\langle a\rangle$ order k. We have already shown above that $H = \langle a^m\rangle$, where m is a divisor of n. Then $m = \gcd(n, m)$ and $k = |a^m| = |a^{\gcd(n,m)}| = \frac{n}{\gcd(n,m)} = \frac{n}{m}$. Thus, $m = \frac{n}{k}$ and $H = \langle a^{\frac{n}{k}}\rangle$.

Returning for a moment to our discussion of the cyclic group $\langle a \rangle$, where a has order 30, we may conclude from Theorem 4.3 that the subgroups of $\langle a \rangle$ are precisely those of the form $\langle a^m \rangle$, where m is a divisor of 30. Moreover, if k is a divisor of 30, the subgroup of order k is $\langle a^{\frac{30}{k}} \rangle$. So the list of subgroups of $\langle a \rangle$ is:

$$\begin{array}{ll}
\langle a \rangle = \{e,\, a,\, a^2,\, \ldots,\, a^{30}\} & |a| = |\langle a \rangle| = 30, \\
\langle a^2 \rangle = \{e,\, a^2,\, a^4,\, \ldots,\, a^{28}\} & |a^2| = |\langle a^2 \rangle| = 15, \\
\langle a^3 \rangle = \{e,\, a^3,\, a^6,\, \ldots,\, a^{27}\} & |a^3| = |\langle a^3 \rangle| = 10, \\
\qquad\vdots & \qquad\vdots \\
\langle a^{15} \rangle = \{e,\, a^{15}\} & |a^{15}| = |\langle a^{15} \rangle| = 2, \\
\langle a^{30} \rangle = \{e\} & |a^{30}| = |\langle a^{30} \rangle| = 1.
\end{array}$$

4.4.2 Subgroups of Z_n

Corollary. For each positive divisor k of n, the set $\langle \frac{n}{k} \rangle$ is the unique subgroup of Z_n order k; moreover, these are the only subgroups of Z_n.

By combining Theorems 4.2 and 4.3, we can easily count the number of elements of each order in a finite cyclic group. For convenience, we introduce an important number-theoretic function called the *Euler phi function*. Let $\phi(1) = 1$, and for any integer $n > 1$, let $\phi(n)$ denote the number of positive integers less than n and relatively prime to n. Notice that by definition of the group $U(n)$, $|U(n)| = \phi(n)$. The first 12 values of $\phi(n)$ are given in table below.

n	1	2	3	4	5	6	7	8	9	10	11	12
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

4.4.3 Number of elements of each order in a cyclic group

Theorem. If d is a positive divisor of n, the number of elements of order d in a cyclic group of order n is $\phi(d)$.

Proof. By Theorem 4.3, the group has exactly one subgroup of order d- call it $\langle b \rangle$. Then every element of order d also generates the subgroup $\langle b \rangle$ and, by Corollary 3 of Theorem 4.2, and element b^k generates $\langle b \rangle$ if and only if $\gcd(k, d) = 1$. The number of such elements is precisely $\phi(d)$.

Comment. Let G be a cyclic group and $G = \langle a \rangle$. $n := |a| = |\langle a \rangle|$. Let $0 < d \mid n$. By Theorem 4.3 $\langle a \rangle$ has exactly one subgroup of order d, that is $\langle a^{\frac{n}{d}} \rangle$. So $|a^{\frac{n}{d}}| = |\langle a^{\frac{n}{d}} \rangle| = d$. Let $\langle b \rangle := \langle a^{\frac{n}{d}} \rangle$. Every element of order d in $\langle a \rangle$ also generates $\langle b \rangle$. So, all the elements of order d in a are in $\langle b \rangle$, and are generators. We need to find the number of generators in $\langle b \rangle$.

4.5 Number of elements of order d in a finite group

Corollary. In a finite group, the number of elements of order d is divisible by $\phi(d)$.

Proof. If a finite group has no elements of order d, the statement is true, since $\phi(d)$ divides 0. Now suppose that $a \in G$ and $|a| = d$. By Theorem 4.4, we know that $\langle a \rangle$ has $\phi(d)$ elements of order d. If all elements of order d in G are in $\langle a \rangle$, we are done. So, suppose that there is an element b in G of order d that is not in $\langle a \rangle$. Then, $\langle b \rangle$ also has $\phi(d)$ elements of order d. This means that we have found $2\phi(d)$ elements of order d. provided that $\langle a \rangle$ and $\langle b \rangle$ have no elements or order d in common. If there is an element c of order d that belongs to both $\langle a \rangle$ and $\langle b \rangle$, then we have $\langle a \rangle = \langle c \rangle = \langle b \rangle$, so that $b \in \langle a \rangle$, which is contradiction. 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

Wigner's discovery about the electron permutation group was just the beginning. He and others found many similar applications and nowadays group theoretical methods—especially those involving characters and representations—pervade all branches of quantum mechanics.

5.1 Definition and notation

5.1.1 Permutation of A, permutation group of A

Definition. A *permutation* of a set A is a function from A to A that is both one-to-one and onto. A *permutation group* of a set A is a set of permutations of A that forms a group under function composition.

We will focus on the case where A is finite. Furthermore, it is customary, as well as convenient, to take A to be a set of the form $\{1, 2, 3, \ldots, n\}$ for some positive integer n. Permutations of finite sets are usually given by an explicit listing of each element of the domain and its corresponding functional value. For example, we define a permutation α of the set $\{1, 2, 3, 4\}$ by specifying

$$\alpha(1) = 2, \quad \alpha(2) = 3, \quad \alpha(3) = 1, \quad \alpha(4) = 4.$$

A more convenient way to express this correspodence is to write α in array form as

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

Example. Symmetric group of S_3 Let S_3 denote the set of all one-to-one functions from $\{1, 2, 3\}$ to itself. Then S_3, under function composition, is a group with six elements. The six elements are

$$\varepsilon = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \quad \alpha = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \quad \alpha^2 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix},$$

$$\beta = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}, \quad \alpha\beta = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}, \quad \alpha^2\beta = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}.$$

Note that

$$\beta\alpha = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} = \alpha^2\beta \neq \alpha\beta$$

, so that S_3 is non-Abelian.

5.2 Cycle notation

There is another notation commonly used to specify permutations. It is called *cycle notation* and was first introduced by the great French mathematician Cauchy in 1815. Cycle notation has theoretical advantages in that certain important properties of the permutation can be readily determined when cycle notation is used.

Let us consider the permutation

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{bmatrix}$$

In cycle notation: (1, 2)(3, 4, 6)(5).
Second example:

$$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{bmatrix}.$$

In cycle notation: (1, 5, 2, 3)(4, 6).
An expression of the form $(a_1, a_2, \ldots, a_m)$ is called a *cycle of length* m or an *m-cycle*.

5.3 Properties of permutations

5.3.1 Products of disjoint cycles

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

Proof. Let α be a permutation on $A = \{1, 2, \ldots, n\}$. To write α in disjoint cycle form, we start by choosing any member of A, say a_1, and let

$$a_2 = \alpha(a_1), \quad a_3 = \alpha(\alpha(a_1)) = \alpha^2(a_1),$$

and so on, until we arrive at $a_1 = \alpha^m(a_1)$ for some m. We know that such m exists because the sequence $a_1, \alpha(a_1), \alpha^2(a_1), \ldots$ must be finite; so there must eventually be a repetition, say $\alpha^i(a_1) = \alpha^j(a_1)$ for some i and j with $i < j$. Then $a^1 = \alpha^m(a_1)$, where $m = j - i$. We express this relationship among $a_1, a_2, \ldots, a_m$ as

$$\alpha = (a_1, a_2, \ldots, a_m) \cdots .$$

The three dots at the end indicate the possibility that we may not have exhausted the set A in this process. In such case, we merely choose any element b_1 of A not appearing in the first cycle and proceed to create a new cycle before. That is, we let $b_2 = \alpha(b_1)$, $b_3 = \alpha^2(b_1)$, and so on, until we reach $b_1 = \alpha^k(b_1)$ for some k. This new cycle will have no elements in common with the previously constructed cycle. For, if so, then $\alpha^i(a_1) = \alpha^k(b_1)$ for some i and j. But then $\alpha^{i-j}(a_1) = b_1$, and therefore $b_1 = a_t$ for some t.

This contradicts the way b_1 was chosen. Continuing this process until we run out of elements of A, our permutation will appear as

$$\alpha = (a_1, a_2, \ldots, a_m)(b_1, b_2, \ldots, b_k) \cdots (c_1, c_2, \ldots, c_s).$$

In this way, we see that every permutation can be written as a product of disjoint cycles.

5.3.2 Disjoint cycles commute

If the pair of cycles $\alpha = (a_1, a_2, \ldots, a_m)$ and $\beta = (b_1, b_2, \ldots, b_n)$ have no entries in common, then $\alpha\beta = \beta\alpha$.

Proof. For definiteness, let us say that α and β are permutations of the set

$$S = \{a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, c_1, c_2, \ldots, c_k\}$$

where the c's are the members of S left fixed by both α and β (there may not be any c's). To prove that $\alpha\beta = \beta\alpha$, we must show that $(\alpha\beta)(x) = (\beta\alpha)(x)$ for all x in S. If x is one of the a elements, say a_i, then

$$(\alpha\beta)(a_i) = \alpha(\beta(a_i)) = \alpha(a_i) = a_{i+1},$$

since β fixes all a elements. (We interpret a_{i+1} as a_1 if $i = m$.) For the same reason,

$$(\beta\alpha)(a_i) = \beta(\alpha(a_i)) = \beta(a_{i+1}) = a_{i+1}.$$

Hence, the functions of $\alpha\beta$ and $\beta\alpha$ agree on the a elements. A similar argument shows that $\alpha\beta$ and $\beta\alpha$ agree on the b elements as well. Finally, suppose that x is a c element, say c_i. Then, since both α and β fix c elements, we have

$$(\alpha\beta)(c_i) = \alpha(\beta(c_i)) = \alpha(c_i) = c_i$$

and

$$(\beta\alpha)(c_i) = \beta(\alpha(c_i)) = \beta(c_i) = c_i.$$

This completes the proof.

The next theorem shows that the disjoint cycle form has the enormous advantage of allowing us to "eyeball" the order of the permutation.

5.3.3 Order of a permutation

Theorem. 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. First, observe that a cycle of length n has order n. Let G be a permutation group of the set $A = \{1, 2, 3, 4, 5\}$ and $\alpha \in G$.

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{bmatrix}$$

In disjoint cycle form: $\alpha = (132)(45)$.
α can be written as $\alpha' \circ \alpha''$ or $\alpha'' \circ \alpha'$, where

$$\alpha' = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{bmatrix}, \quad \alpha'' = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{bmatrix}$$

$\alpha' = (132)$, $\alpha'' = (45)$. Let us see the order of these functions:

$$(\alpha')^1 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{bmatrix}, \quad (\alpha')^2 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{bmatrix}, \quad (\alpha')^3 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{bmatrix}.$$

$$(\alpha'')^1 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{bmatrix}, \quad (\alpha'')^2 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{bmatrix}.$$

We can see that $|\alpha'| = 3$, $|\alpha''| = 2$, that are equal with the lengths of the cycles.

Next, suppose that α and β are disjoint cycles of lengths m and n, and let k be the least common multiple of m and n. It follows from Theorem 4.1 that both α^k amd β^k are the identity permutation $\mathcal{E}$ ($\alpha^m = \alpha^k \iff m \mid m - k$) and, since α and β commute, $(\alpha\beta)^k = \alpha^k\beta^k$ is also the identity. Thus, we know by Corollary 2 to Theorem 4.1 ($a^k = e \iff |a| \mid k$) that the order of $\alpha\beta$ -let us call it t- must divide k. But then $(\alpha\beta)^t = \alpha^t\beta^t = \mathcal{E}$, so that $\alpha^t = \beta^{-t}$. However, it is clear that if α and β have no common symbol, the same is true for α^t and β^{-t}, since raising a cycle to a power does not introduce new symbols. But if α^t and β^{-t} are equal and have no common symbol, they must both be the identity, because every symbol in α^t is fixed by β^{-t} and vice versa. It follows, then, that both m and n divides t also. ($\alpha^t = e \iff m \mid t$). This means that k, the least common multiple of m and n, divides t also. This shows that $k = t$.

Thus far, we have proved that the theorem is true in the cases where the permutation is a single cycle or a product of two disjoint cycles. The general case involving more than two cycles can be handled in an analogous way.

As we will soon see, a particularly important kind of permutation is a cycle of length 2-that is, a permutation of the form (ab) where $a \neq b$. Many authors call these permutations *transpositions*, since the effect of (ab) is to interchange or transpose a and b.

5.3.4 Product of 2-cycles

Theorem. Every permutation in S_n, $n > 1$, is a product of 2-cycles.

Proof. First, note that the identity can be expressed as $(12)(12)$, and it is a product of 2-cycles. By Theorem 5.1, we know that every permutation can be written in the form

$$(a_1 a_2 \cdots a_k)(b_1 b_2 \cdots b_t) \cdots (c_1 c_2 \cdots c_s).$$

A direct computation shows that this is the same as

$$(a_1 a_k)(a_1 a_{k-1}) \cdots (a_1 a_2)(b_1 b_t)(b_1 b_{t-1}) \cdots (b_1 b_2)(c_1 c_s)(c_1 c_{s-1}) \cdots (c_1 c_2).$$

This completes the proof.

Example.

$$(12345) = (15)(14)(13)(12)$$
$$(1632)(457) = (12)(13)(16)(47)(45)$$

The decomposition of a permutation into a product of 2-cycles given in the proof of Theorem 5.4 is not the only way a permutation can be written as a product of 2-cycles. Although the next example shows that even the *number* of 2-cycles may vary from one decomposition to another, we will prove in Theorem 5.5 (first proved by Cauchy) that there is one aspect of a decomposition that never varies.

We isolate a special case of Theorem 5.5 as a lemma.

Lemma. If $\mathcal{E} = \beta_1 \beta_2 \cdots \beta_r$, where the β's are 2-cycles, then r is even.

Proof. Clearly, $r \neq 1$, since a 2-cycle is not the identity. If $r = 2$, we are done. So, we suppose that $r > 2$, and we proceed by induction. Since $(ij) = (ji)$, the product $\beta_{r-1}\beta_r$ can be expressed in one of the following forms shown on the right:

$$\mathcal{E} = (ab)(ab)$$
$$(ab)(bc) = (ac)(ab)$$
$$(ac)(cb) = (bc)(ab)$$
$$(ab)(cd) = (cd)(ab).$$

If the first case occurs, we may delete $\beta_{r-1}\beta_r$ from the original product to obtain $\mathcal{E} = \beta_1\beta_2\cdots\beta_{r-2}$. In the other three cases, we replace the form of $\beta_{r-1}\beta_r$ on the right by its counterpart in the left to obtain a new product of r 2-cycles that is still the identity, but where the rightmost occurence of the integer a is in the second-from-the-rightmost 2-cycle of the product instead of the rightmost 2-cycle. We now repeat the procedure just described with $\beta_{r-2}\beta_{r-1}$, and, as before, we obtain a product of $(r-2)$ 2-cycles equal to the identity or a new product of r 2-cycles, where the rightmost occurence of a is in the third 2-cycle from the right. Continuing this process, we must obtain a product of $(r-2)$ 2-cycles equal to the identity, because otherwise we have a product equal to the identity in which the only occurence of the integer a is in the leftmost 2-cycle, and such product does not fix a, whereas the identity does. Hence, by the *Second principle of mathematical induction*, $r-2$ is even, and r is even as well.

5.3.5 Always even or always odd

Theorem. If a permutation α can be expressed as a product of an even (odd) number of 2-cycles, then every decomposition of α into a product of 2-cycles must have an even (odd) number of 2-cycles. In symbols, if

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

where the β's and the γ's are 2-cycles, then r and s are both even or both odd.

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

$$\mathcal{E} = \gamma_1\gamma_2\cdots\gamma_s\beta_1^{-1}\beta_2^{-1}\cdots\beta_r^{-1} = \gamma_1\gamma_2\cdots\gamma_s\beta_1\beta_2\cdots\beta_r$$

since a 2-cycle is its own inverse. Thus, the lemma on page 104 guarantees that $s+r$ is even. It follows that r and s are both even or both odd.

5.3.6 Even and odd permutations

Definition. A permutation that can be expressed as a product of an even number of 2-cycles is called an *even permutation*. A permutation that can be expressed as a product of an odd number of 2-cycles is called an *odd permutation*.

Theorems 5.4 and 5.5 together show that every permutation can be unambigously classified as either even or odd. The significance of this observation is given in Theorem 5.6.

5.3.7 Even permutations form a group

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

Proof. This proof is left to the reader.

5.3.8 Alternating group of degree n

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

5.3.9 Order of the alternating group of degree n

Theorem. For $n > 1$, A_n has order $\frac{n!}{2}$.

Proof. For each odd permutation α, the permutation $(12)\alpha$ is even and $(12)\alpha \neq (12)\beta$ when $\alpha \neq \beta$. Thus, there are at least as many even permutation as there are odd ones. On the other hand, for each even permutation α, the permutation $(12)\alpha$ is odd and $(12)\alpha \neq (12)\beta$ when $\alpha \neq \beta$. Thus, there are at least as many odd permutations as there are even ones. It follows that there are equal members of even and odd permutations. Since $|S_n| = n!$, we have $|A_n| = \frac{n!}{2}$.