Groups

Contents

1 Introduction to Groups

Binary Operator

Definition 1.1. Let G be a set. A Binary Operator on G is a function that assigns each ordered pair of elements of G an element of G.

The most familiar binary operators on integers is addition, subtraction, and multiplication. Division is not an operator since it may not give a integer.

Group

Definition 1.2. Let G be a set together with a Binary Operator (1.1) (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 if these three properties are satisfied:

1. Associativity. $(ab)c = a(bc)$
2. Identity. That is there exists an identity denoted e such that $ae = ea = a$
3. Inverses. $\forall a \in G, \exists b \in G : ab = ba = e$

Examples
$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ under addition. Consider $\mathbb{Z}$ under addition.

$$a, b, c \in \mathbb{Z}$$

$(a + b) + c = a + (b + c)$ Hence there is Associativity

$a + 0 = 0 + a = a$ Hence there is a identity

$a + (-a) = (-a) + a = 0$ Hence every element has a inverse

Uniqueness of Identity Theorem

Theorem 1.1. In a Group there one and only one identity.

proof

Let G be a group and let $a \in G$. Assume e and e' are both identities of the group. Then,

$$ae = a \tag{1}$$

$$e'a = a \tag{2}$$

Now assume in (1) $a = e'$ and in (2) $a = e$ this means,

$$e'e = e$$

$$e'e = e'$$

$\implies e = e'$ since we can set them equal to each other.

We can now say "the identity".

Cancellation

Theorem 1.2. In a group the right and left cancellation laws hold; that is $ab = ac \implies b = c$ and $ba = ca \implies b = c$.

proof

Suppose $a, b, c, a^{-1} \in G$ and $ba = ca$ where a^{-1} is the inverse of a. Then we can multiply both sides by a^{-1} yielding,

$$(ba)a^{-1} = (ca)a^{-1}$$

Then by associativity,

$$b(aa^{-1}) = c(aa^{-1})$$

$$be = ce$$

$$b = c$$

by the identity axiom. Now supposed instead $ab = ac$ then

$$a^{-1}(ab) = a^{-1}(ac)$$

$$(a^{-1}a)b = (a^{-1}a)c$$

$$b = c$$

This is a implication of the fact that every row and column in a Cayley table, a element must only appear once.

Uniqueness of Inverses

Theorem 1.3. Each element in a Group has one and only one inverse.

proof Suppose $a, b, c \in G$ and b and c are both inverses of a. Then

$$ab = e = ac$$

So by the cancellation theorem

$$a = c$$

Thus this contradicts the assumption.

An important note is multiplicative notation is used. So if $g \in G$ then g^n could mean $ggggg$.. or $g+g+g+g+...$ depending on if the operator is multiplication or addition. We also define $g^0 = e$, $g^{-n} = (g^{-1})^{|n|}$ and require n be a integer. This also means $g^n g^m = g^{n+m}$ and $(g^n)^m = g^{nm}$ as would normally be. This does not work for two elements, that is, $g, f \in G, (gf)^n \neq g^n f^n$. But is instead $gfgfgf$.... When $n < 0$ we have $(gf)^{-n} = ((gf)^{-1})^{|n|} = (f^{-1}g^{-1})^n = f^{-1}g^{-1}f^{-1}g^{-1}f^{-1}g^{-1}...$

	Multiplicative Group		**Additive Group**
$a \cdot b$ or ab	Multiplication	$a + b$	Addition
e or 1	Identity or one	0	Zero
a^{-1}	Multiplicative inverse of a	$-a$	Additive inverse of a
a^n	Power of a	na	Multiple of a
ab^{-1}	Quotient	$a - b$	difference

Socks-Shoes Property

Theorem 1.4. $(ab)^{-1} = b^{-1}a^{-1}$

proof Assume $a, b \in G$. Now,

$$(ab)(ab)^{-1} = e$$

and

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = e$$

So

$$(ab)(ab)^{-1} = (ab)(b^{-1}a^{-1})$$

and using the Cancellation theorem

$$(ab)^{-1} = (b^{-1}a^{-1})$$

2 Finite Groups and Subgroups

Order of Group

Definition 2.1. Let G be a Group. The order, denoted $|G|$, is the number of elements in the group, which may be infinite.

Order of an Element in a Group

Definition 2.2. Let G be a Group and $a \in G$. The order of a, denoted $|a|$ is the smallest number such that $a^n = e$ (In additive notation this is $na = e$). If no n exists, then we say a has infinite order.

Subgroup

Definition 2.3. If a subset of a Group, G is also a group under the same operation, we say it is a subgroup of G.

We say that e is the trivial subgroup as it is a subgroup of every group. If H is a subgroup of G we write $H \leq G$. If we want to show H is a subgroup but not equal, we say $H < G$.

One Step Subgroup Test

Theorem 2.1. 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.)

proof Since H has the same operation of G it is associative. Next, since H is nonempty we may pick some $x \in H$ then $a = x, b = x^{-1} \implies xx^{-1} = e \in H$ so there is an identity element. Now we need to show the existence of inverses so $a = e, b = x$ then $ab^{-1} = ex^{-1} = x^{-1} \in H$. Finally to show closure assume $x, y \in H$ then $y^{-1} \in H$ and $a = x, b = y^{-1}$ so $ab^{-1} = xy \in H$ so if x and y are in H so is xy.

This proof is structured by assuming the conditions then proving it is a subgroup.

Two Step Subgroup Test

Theorem 2.2. Let G be a group and H a nonempty subset of G. If ab is in H whenever a and b are in H, and a^{-1} is in H whenever a is then H is a subgroup of G.

proof Since H has the same operation of G it is associative. Next, since H is nonempty we may pick some $x \in H$ then $a = x \implies x^{-1} \in H$. So $a = x, b = x^{-1} \implies ab = xx^{-1} = e \in H$ so we have a identity. Now we already have closure since whenever a, b and in H ab must be.

Finite Subgroup Test

Theorem 2.3. 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 We only need to prove that $a^{-1} \in H$ whenever $a \in H$ since it is assumed that H is closed so the first part of the Two Step Subgroup Test is fulfilled. So if $a = e$ then $a = a^{-1}$ and we are done. If ae we can consider the sequence $a, a^2, a^3...$ which since H is closed these are all elements of H. Since H is also finite this sequence must repeat so considering $a^i = a^j \implies a^{i-j} = e \; with \; i > j$ but since $a \neq e$ we have $i - j > 1$. Thus, $e = a^{i-j} = aa^{i-j-1} = aa^{-1} \implies a^{-1} = a^{i-j-1}$. But $i - j > 1 \implies i - j - 1 > 0$ so $a^{i-j-1} \in \{a, a^2, a^3, ...\}$ which we already showed $\{a, a^2, a^3, ...\} \in H$ so $a^{i-j-1} = a^{-1} \in H$

Center of Group

Definition 2.4. The center of a group, denoted $Z(G)$ of G is the subset of elements in G that commute with every other element in G.

$$Z(G) = \{a \in G | ax = xa \; \forall x \in G\}$$

Center is a Subgroup

Theorem 2.4. The center of a group G is a subgroup of G.

proof We already know $Z(G)$ is associative. We know there is an identity element since $ex = xe$. Suppose $a, b \in Z(G)$ then $(ab)x = a(bx) = a(xb) = (ax)b = x(ab)$ hence when a, b are in $Z(G)$ so is ab. Now since $e \in Z(G)$ we can write

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

$$a^{-1}axa^{-1} = a^{-1}xaa^{-1}$$

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

So $a^{-1} \in Z(G)$ whenever $a \in Z(G)$.

Centralizer of Group

Definition 2.5. Let a be a fixed element of a group G. The centralizer of a in G, denoted $C(G)$, is the set of all elements in G that commute with a.

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

The center is the set of elements in G that commute with every other element in G whereas the centralizer is the is the set of all elements in G that commute with a specific element.

Centralize Is a Subgroup

Theorem 2.5. For a in a group G, the centralizer of a is a subgroup of G.

proof We already know $C(a)$ is associative since it has the same operation as G. We know there is an identity element since $ea = ae$. Suppose $b, c \in C(a)$ then $cba = c(ba) = c(ab) = (ca)b = acb \implies cb \in C(a)$. Now since $e \in C(a)$ we can write

$$c^{-1}(ca)c^{-1} = c^{-1}(ac)c^{-1}$$

$$c^{-1}cac^{-1} = c^{-1}acc^{-1}$$

$$ac^{-1} = c^{-1}a$$

So $c^{-1} \in C(a)$ whenever $c \in C(a)$.

3 Cyclic Groups

Cyclic Group

Definition 3.1. Let a cyclic group be denoted by $\langle a \rangle = \{a^n | n \in \mathbb{Z}\}$ where a is called the generator of the cyclic group.

Cyclic Group is a Subgroup

Theorem 3.1. Let G be a group and $a \in G$. Then, $\langle a \rangle$ is a subgroup of G.

proof We know $a \in \langle a \rangle$ so $\langle a \rangle$ is not empty. We know $\langle a \rangle$ is associative since it has the same operation as G. Now since all elements are $a^n : n \in \mathbb{Z}$ taking two $ab = a^n a^m = a^{n+m} \in \langle a \rangle$ where $n, m \in \mathbb{Z}$ so there is closure. Now pick a element $c = a^n$ since $n \in \mathbb{Z}$ we can write $c^{-1} = (a^n)^{-1} = a^{-n}$ which by definition $-n \in \mathbb{Z}$ so by the two step subgroup test this is a subgroup.

Criterion for $a^i = a^j$

Theorem 3.2. Let G be a group and $a \in G$. If a has infinite order, then $a^i = a^j$ iff $i = j$. If a has finite order, say n, then $\langle a \rangle = \{e, a, a^2, a^3, ..., a^{n-1}\}$ and $a^i = a^j$ iff n divides $i - j$.

proof If a has infinite order then there is no nonzero n such that $a^n = e$. So $a^i = a^j \implies a^{i-j} = e$ so we must have $i - j = 0$. Now consider $|a| = n$. We must prove the first statement that $\langle a \rangle = \{e, a, a^2, a^3, ..., a^{n-1}\}$. Obviously $\{e, a, a^2, a^3, ..., a^{n-1}\} \in \langle a \rangle$. If we pick a^k we can write $a^k = a^{nq+r} = a^{nq}a^r = a^{nq}a^r = a^r$ where $k = nq + r \; with \; 0 \leq r < n$. So $a^k \in \{e, a, a^2, a^3, ..., a^{n-1}\}$ and $\langle a \rangle = \{e, a, a^2, a^3, ..., a^{n-1}\}$. Now we want to prove the final statement $a^i = a^j$ iff n divides $i - j$. Assume $a^i = a^j \implies a^{i-j} = e$ using the division algorithm again $i - j = nq + r$ and we showed $a^{i-j} = a^r$ so $r = 0$ and therefore $i - j = nq$ so n divides $i - j$. Since this is a iff we prove the converse. Assume n divides $i - j$ then $a^{i-j} = a^r$ and r must be 0 since n divides $i - j$ so $a^{i-j} = e \implies a^i = a^j$.

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

Corollary 3.3. *For any group element a, $|a| = |\langle a \rangle|$*

$a^k = e$ Iff $|a|$ Divides k

Corollary 3.4. *For any group element a,$a^k = e$ iff $|a|$ divides k.*

proof We know from Criterion for $a^i = a^j$ that $a^k = e$ iff n divides $k - 0 = k$.

$a^k = e$ Iff k is a Multiple of $|a|$

Corollary 3.5. *$\forall a \in G$, $a^k = e$ iff k is a multiple of $|a|$.*

proof Suppose a^k. If k is a multiple of $|a|$ the by the division theorem we can write $a^k = a^{nq}$ where q is the order of a. Then this is equivalent to $(a^q)^n = e^n = e$. We already showed that for any k not that $a^k = a^{nq+r} = a^r$. Now the converse, suppose

Relationship Between $|ab|$ and $|a||b|$

Corollary 3.6. *If G is finite and abelian, then $\forall a, b \in G$,$|ab|$ divides $|a||b|$.*

proof Suppose $|a| = m$ and $|b| = n \implies |a||b| = mn$. Now if $(ab)^{mn} = a^{mn}b^{mn} = (a^n)^m(b^m)^n = ee = e$. From Corollary 3.4 we know $(ab)^k = e$ iff $|ab|$ divides k. In this case $k = mn$ so the result is clear.

$\langle a^k \rangle = \langle a^{gcd(n,k)} \rangle$ and $|a^k| = \frac{n}{gcd(n,k)}$

Theorem 3.7. Let $a \in G : |a| = n$ and let $k \in \mathbb{Z}^+$, then $\langle a^k \rangle = \langle a^{gcd(n,k)} \rangle$ and $|a^k| = \frac{n}{gcd(n,k)}$.

proof First we will prove $\langle a^k \rangle = \langle a^{gcd(n,k)} \rangle$. Assume $gcd(n,k) = d$ and $k = dr$ where r is also a positive integer. Then since $a^k = a^{dr} = (a^d)^r \implies \langle a^k \rangle \subseteq \langle a^d \rangle$ since we know $a^k \in \{(a^d)^1, (a^d)^2, ..., (a^d)^r, ...\}$. Now we can write $d = ns + kt$ so $a^d = a^{ns+kt} = a^{ns}a^{kt} = (a^n)^s(a^k)^t = (a^k)^t \in \langle a^k \rangle$ so we now have that $\langle a^d \rangle \subseteq \langle a^k \rangle$ so $\langle a^d \rangle = \langle a^k \rangle$ proving the first statement. Now for the second we want to show that the order of $a^d = n/d$. First we notice $(a^d)^{\frac{n}{d}} = a^n = e \implies |a^d| \leq \frac{n}{d}$. Now consider a positive integer $i : i < \frac{n}{d}$, since $|a| = n, (a^d)^i \neq e$ as i cannot be $\frac{n}{d}$ so $|a^d| = \frac{n}{d}$ and using the fact that we proved $\langle a^k \rangle = \langle a^{gcd(n,k)} \rangle$ we can then say $|a^k| = |\langle a^k \rangle| = |\langle a^{gcd(n,k)} \rangle| = \frac{n}{gcd(n,k)}$

Order of Element in Cyclic Group

Corollary 3.8. *In a finite cyclic group, the order of an element divides the order of the group.*

proof This was proven in Theorem 3.7, that is for some element of a cyclic group $a^k, |a^k| = \frac{n}{gcd(n,k)}$

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

Corollary 3.9. *Let* $|a| = n$ *then* $\langle a^i \rangle = \langle a^j \rangle$ *iff* $gcd(n,i) = gcd(n,j)$ *and* $|a^i| = |a^j|$ *iff* $gcd(n,i) = gcd(n,j)$.

proof We know from Theorem 3.7 that $\langle a^k \rangle = \langle a^{gcd(n,k)} \rangle$ *so* $\langle a^i \rangle = \langle a^j \rangle \implies \langle a^{gcd(n,i)} \rangle = \langle a^{gcd(n,j)} \rangle$ *which can only be true if* $gcd(n,i) = gcd(n,j)$. *This is also true for the order.*

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

Corollary 3.10. *Let* $|a| = n$ *then* $\langle a \rangle = \langle a^j \rangle$ *iff* $gcd(n,j) = 1$ *and* $|a| = |a^j|$ *iff* $gcd(n,j) = 1$.

Generator of Z_n

Corollary 3.11. *An integer in Z_n is a generator of Z_n iff $gcd(n,k) = 1$*

proof This follows from Corollary 3.9.

Fundamental Theorem of Cyclic Groups

Theorem 3.12. Every subgroup of a cyclic group is cyclic. Moreover, if $|\langle a\rangle| = n$, for each positive divisor k of n, the group $\langle a\rangle$ has exactly one subgroup of order k namely $\langle a^{\frac{n}{k}}\rangle$.

proof Assume $G = \langle a\rangle$ and suppose that H is a subgroup of G.

Case 1: $H = \{e\}$ Then H is clearly cyclic by definition.

Case 2: $H \neq \{e\}$ Since every element of G has the form a^t this implies the form of elements in H are of the form a^t. Now by closure a^{-t} is in H. Let m be the least positive integer such that $a^m \in H$. By closure $\langle a^m\rangle \subseteq H$. Now let $b \in H \implies b = a^k$ by the division algorithm $k = mq + r, 0 \leq r < m$ which we can write as $a^k = a^{mq+r} = a^{mq}a^r \implies a^r = a^{-mq}a^k = a^{-mq}b = (a^m)^{-q}b$. Now since $(a^m)^{-q}, b \in H$ by closure $a^r \in H$. But since we said m in the least positive integer and $0 \leq r < m \implies r = 0$ so $a^k = (a^m)^q \in \langle a^m\rangle$ so since any element in H is in $\langle a^m\rangle, H = \langle a^m\rangle$ proving every subgroup of a cyclic group is cyclic.

Let there be two cyclic subgroups with order k $\langle a^i\rangle, \langle a^j\rangle$ then by corollary 3.9 $\langle a^i\rangle = \langle a^j\rangle$. Now $|a^{\frac{n}{k}}| = \frac{n}{gcd(n,\frac{n}{k})} = \frac{n}{\frac{n}{k}} = k$ so since there can only be one group of order k and the group $|\langle a^{\frac{n}{k}}\rangle| = k$ we prove the last part of the Theorem.

Subgroups of Z_n

Corollary 3.13. *For each positive divisor k of n, the set $\langle\frac{n}{k}\rangle$ is a unique subgroup of Z_n of order k; moreover, these are the only subgroups of Z_n*

Euler Phi Function

Definition 3.2. Let $\phi(n)$ be the number of positive integers relatively prime to n.

Number of Elements of Each Order in a Cyclic Group

Theorem 3.14. 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 3.11, the group has exactly one subgroup of order d, say $\langle a \rangle$. Then every element of order d also generates $\langle a \rangle$ and we know an element a^k generates $\langle a \rangle$ if and only if $gcd(k, d) = 1$, in other words only if k and d are relatively prime which is precisely the definition of the Euler Phi Function.

Number of Elements of Order d in a Finite Group

Corollary 3.15. *In a finite group, the number of elements of order d is a multiple of* $\phi(d)$

proof If the number of elements of order d is 0 then this holds since $0 = n\phi(d) \implies \frac{0}{\phi(d)} = n$. *Next suppose* $a \in G$, *then we can say by Theorem 3.13 the number of elements of order d in* $\langle a \rangle$ *is* $\phi(d)$. *If all the elements of order d are in* $\langle a \rangle$ *then the multiple is one. Now suppose there is also a* $b \in G$ *of order d that is not in* $\langle a \rangle$. *We can again construct* $\langle b \rangle$ *which, by Theorem 3.13 has* $\phi(d)$ *number of elements of order d. This means that there is* $2\phi(d)$ *elements in G which have order d. To show this assume there is a elements* $c \in G$ *of order d, that is in both* $\langle a \rangle$ *and* $\langle b \rangle$. *This means that we can write c as* a^j *and by the converse of Corollary 3.10* $gcd(d, j) = 1$ *iff* $|a| = |a^j|$ *which is true as both are d. So we may write by Corollary 3.10* $\langle a \rangle = \langle a^j \rangle = \langle c \rangle$. *Now since c can also be written as* b^i *we can write following the same logic* $\langle b \rangle = \langle c \rangle \implies \langle a \rangle = \langle b \rangle \implies b \in \langle a \rangle$ *which is a contradiction. Continuing in the same fashion we see that for a group G the number of elements of order d will be a multiple of* $\phi(d)$.

4 Permutation Groups

Permutation of A, Permutation Group of A

Definition 4.1. 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 is a set of permutations of A that forms a group under function composition.

We do not define function like in calculus, instead we explicitly write what each number in the domain corresponds to in the range. For example,

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

A more convenient way to write this is

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

Where each element in the bottom row corresponds to the output of alpha acting on the element in the top row of the same column. To compose functions we simply use regulation composition $(\alpha\gamma)(1) = \alpha(\gamma(1)) = \alpha(2) = 3$ or in matrix notation,

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

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

Remember the group here is the group of these functions under function composition. Another type of notation is cycle notation. Here we represent the "cycles" of the permutation. For example, consider the permutation,

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

Here we see there are cycles in the permutation, that is 1 maps to 2 and 2 maps to one, 5 maps to itself and 3 maps to 4 which maps to 6 which maps to 3. We can represent this as (12)(346)(5). We can compose to cycles by starting from right and going to left for example take,

$$\alpha = (13)(27)(456)(8)$$

$$\beta = (1237)(648)(5)$$

$$\alpha\beta = (13)(27)(456)(8)(1237)(648)(5)$$

We first start from 1 and proceed right to left. So (5) does nothing to 1, (648) does nothing to 1, (1237) maps 1 to 2, (8) does nothing to 2, (456) does nothing to 2, (27) maps 2 to 7, and (13) does nothing to 7 so we have the first component 1 maps to 7. We continue this for 2,3,4... until we have our desired permutation. We also consider the identity to be the permutation which is (1)(2)(3)....

Products of Disjoint Cycles

Theorem 4.1. Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.

proof Consider the set $A = \{1, 2, 3, .., n\}$. To write α in disjoint cycle form, we start by choosing an element of the set A say a_1 and suppose

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

and so on until we reach $a_1 = \alpha^m(a_1)$, which must exist since A is finite. We can write this then as

$$\alpha = (a_1, a_2, a_3, ..., a_m)...$$

But α may not be the only cycle so now assume we choose some other element b_1 not in α we can then repeat this process to get

$$\alpha = (a_1, a_2, a_3, ..., a_m)(b_1, b_2, b_3, .., b_k)...$$

We can do this until we have exhausted every element in A, hence we can write any permutation as a product of disjoint cycles.

Disjoint Cycles Commute

Theorem 4.2. If two pairs of cycles of a set S, say

$$\alpha = (a_1, a_2, a_3, ..., a_m)$$

and

$$\beta = (b_1, b_2, b_3, ..., b_k)$$

do not have any elements in common, then $\alpha\beta = \beta\alpha$

proof Consider the set $S = \{a_1, a_2, a_3, ..., a_m, b_1, b_2, b_3, .., b_k, c_1, c_2, c_3, .., c_n\}$ and permutations α and β. Then

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

Now we can show

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

We can also show

$$(\alpha\beta)(b_i) = (\beta\alpha)(b_i) = b_{i+1}$$

and also show

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

hence we have completed the proof since

$$(\alpha\beta)(x) = (\beta\alpha)(x)$$

Order of Permutation

Theorem 4.3. 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 Suppose α and β are disjoint cycles of lengths m and n, and let k be the least common multiple between them. It follows from Theorem 3.2 that $\alpha^k = \epsilon$ and $\beta^k = \epsilon$ since the least common multiple is a multiple of n and m. We also know disjoint cycles commute, so $(\alpha\beta)^k = \alpha^k\beta^k = \epsilon$. We also know the order of $\alpha\beta$ must divide k. So we have $|\alpha\beta| = t \implies (\alpha\beta)^t = \epsilon = (\alpha\beta)^k$. Now since $(\alpha\beta)^t = \alpha^t\beta^t = \epsilon$ it must fix values 1 through n, so t must be a multiple n and m to satisfy this condition and since k is the least common multiple $t = |\alpha\beta| = k$. This can be done for more disjoint cycles in a similar fashion.

Product of 2-Cycles

Theorem 4.4. Every permutation in S_n such that $n > 1$ is a product of 2-cycles.

proof We can express the identity permutation as (12)(21) since 2 maps to 1 and 1 maps to 2. Conversely, 1 maps to 2 and 2 maps to 1. Now for the rest of the elements we may write a permutation by Theorem 4.1 as

$$(a_1...a_k)(b_1...k_t)(c_1....c_s)$$

We may now write

$$(a_1a_k)(a_1a_{k-1})...(a_1a_2)(b_1b_t)(b_1b_{t-1})...(b_1b_2)(c_1c_s)(c_1c_{s-1})...(c_1c_2)$$

as a_1 maps to a_2, then a_2 maps to a_1 which maps to a_3 and so on so we arrive back to $(a_1a_2a_3...)$

Identity Lemma

Theorem 4.5. If the permutation $\beta_1\beta_2...\beta_r = \epsilon$ then r is even.

proof I will not complete this proof yet.

Always even or odd

Theorem 4.6. If a permutation α can be expressed as a product of an even or odd number of 2-cycles, then every decomposition of α into a product of 2-cycles must have an even or odd number of 2-cycles. That is,

$$\alpha = \beta_1\beta_2...\beta_r \; and \; \alpha = \gamma_1\gamma_2...\gamma_s$$

Where beta and gamma are 2-cycles, then r and s are either both even or odd. *proof* Since

$$\beta_1\beta_2...\beta_r = \alpha = \gamma_1\gamma_2...\gamma_s$$

we can write

$$\epsilon = \gamma_1\gamma_2...\gamma_s\beta_r^{-1}\beta_2^{-1}...\beta_1^{-1}$$

Since 2-cycles are there own inverse,

$$\epsilon = \gamma_1\gamma_2...\gamma_s\beta_r\beta_2...\beta_1$$

Now by Theorem 4.5 $s + r$ must be even and therefore r and s must either both be even or odd.

Even Permutations Form a Group

Theorem 4.7. The set of even permutations in S_n forms a subgroups of S_n *proof* Is left to the reader.

Alternating Group

Definition 4.2. The group of even permutations of n symbols denoted A_n is called the alternating group of degree n.

$|A_n|$

Theorem 4.8. For $n > 1$, A_n has order $\frac{n!}{s}$ *proof* For each odd permutation α, we can turn it into an even permutation by $(12)\alpha$. So since α can be any odd permutation and $(12)\alpha \neq (12)\beta$ when $\alpha \neq \beta$ the number of even to odd permutations must be $even \geq odd$. Now suppose α is an even permutation, by the same steps we see $odd \geq even \implies odd = even$. Now since $|S_n| = n!$ and we are taking half the permutations $|A_n| = \frac{n!}{2}$.

5 Isomorphisms

Isomorphism

Definition 5.1. An isomorphism ϕ from a group G to a group $\overline{G}$ is a one to one, onto, mapping from G to $\overline{G}$ that preserves the group operation

$$\phi(a \cdot b) = \phi(a) \diamond \phi(b) \ \forall a, b \in G$$

The operation $\cdot$ is that of G and the operation $\diamond$ is that of $\overline{G}$.

Isomorphic

Definition 5.2. If there is an isomorphism between two groups we say they are isomorphic.

To determine of a function is a isomorphism between groups we first prove the function is one to one by assuming $\phi(a) = \phi(b)$ and showing $a = b$. Then we prove it is onto by taking an element $a \in \overline{G}$ and finding an element $b \in G$ such that $\phi(b) = a$. Finally make sure it is a homomorphism.

Properties of Isomorphisms

Theorem 5.1. Suppose that ϕ is an isomorphism from a group G onto a group H.

1. ϕ maps the identity of G to to the identity of H.
2. For every integer n and for every group element $a \in G$, $\phi(a^n) = [\phi(a)]^n$. In additive notation this is equivalent to $\phi(na) = n\phi(a)$.
3. For elements $a, b \in G$, $ab = ba$ iff $\phi(a)\phi(b) = \phi(b)\phi(a)$.
4. $G = \langle a \rangle$ iff $H = \langle \phi(a) \rangle$
5. $|a| = |\phi(a)|, \forall a \in G$
6. For an integer k the equation $x^k = b, b \in G$ has the same number of solutions as $x^k = \phi(b)$ in H.
7. If G is finite then G and H have exactly the same number of elements of every order.

proof Property 1: Let e denote the identity in G and h denote the identity in H. We know,

$$e = ee$$

Now

$$h\phi(e) = \phi(e) = \phi(ee) = \phi(e)\phi(e)$$

Which

$$h\phi(e) = \phi(e)\phi(e) \implies h = \phi(e)$$

Property 2: We will break this into positive and negative cases. For the positive assume $n = 1$ then

$$\phi(a) = \phi(a)$$

Which is true. So now lets assume it holds for $n = k$ then I will show it holds for $n = k + 1$

$$\phi(a^{k+1}) = \phi(a^k a) = \phi(a^k)\phi(a)$$

Now since

$$a^k = aa...$$

and since an isomorphism is a homomorphism,

$$\phi(a^k)\phi(a) = \phi(a)\phi(a)\phi(a)... = \phi(a)^{k+1}$$

Thus

$$\phi(a^{k+1}) = \phi(a)^{k+1}$$

So by induction it must hold for $n \in \mathbb{N}$ Now for the case when $n = 0$

$$\phi(a^0) = \phi(e) = h = h^0 = \phi(e)^0 = \phi(a)^0$$

By property 1. Now suppose $n < 0$. We know already this property holds for the positive case so since $-n$ is positive,

$$h = \phi(e) = \phi(a^n a^{-n}) = \phi(a^n)\phi(a^{-n}) = \phi(a^n)\phi(a)^{-n}$$

Thus

$$h = \phi(a^n)\phi(a)^{-n}$$

So multiplying on the right both sides by $\phi(a)^n$ we have

$$h\phi(a)^n = \phi(a^n)\phi(a)^{-n}\phi(a)^n$$

$$\phi(a)^n = \phi(a^n)$$

Completing this proof.

Property 4: Assume $G = \langle a \rangle$ then since the mapping $\phi(a)$ must map to a element in H. Then every power of a maps to a element in H b Property 2. Thus $\langle \phi(a) \rangle \subseteq H$. Since ϕ is onto, every element $b \in H$ can be written $\phi(b) = \phi(a^k) = \phi(a)^k \implies H = \langle \phi(a) \rangle$ Now assume $H = \langle \phi(a) \rangle$. Pick some $b \in G$ then since for some $\phi(b) \in H$ we know $\phi(b) = \phi(a)^k = \phi(a^k) \implies b = a^k$ as ϕ is one to one and every element in G is therefore a power of a $\implies G = \langle a \rangle$.

Observe by property 2 $|a| = |\phi(a)|$ as $\phi(a^n) = [\phi(a)]^n$. So they will have the same number take each element to the identity and by property 1 the identity maps to the identity, so property 5 is proven. Property 5 also directly proves property 7.

Properties of Isomorphisms Acting on Groups

Theorem 5.2. Suppose that ϕ is an isomorphism from a group G onto a group H.

1. ϕ^{-1} is an isomorphism from H to G.
2. G is Abelian iff H is Abelian.
3. G is cyclic iff H is cyclic.
4. If K is a subgroup of G, then $\phi(K) = \{\phi(k)|k \in K\}$ is a subgroup of H.
5. If K is a subgroup of H, then $\phi^{-1}(K) = \{g \in G|\phi(g) \in K$ is a subgroup of G.
6. $\phi(Z(G)) = Z(H)$

These two Theorems provide several convenient ways to prove that two groups are not isomorphic,

1. $|G| \neq |H|$
2. One group is cyclic and the other is not
3. One group is Abelian and the other is not
4. Show the largest order of a element in group G is not the same as the largest order of any element of H
5. Show that the number of elements in G with a order of a specific number (Smallest number larger than 1 is usually a good choice) is not the same as the number of elements in H of the same order.

Automorphism

Definition 5.3. An isomorpism from a group G onto itself is called an automorphism of G.

Inner Automorphism Induced by a

Definition 5.4. Let G be a group, and let $a \in G$. The function ϕ_a defined by $\phi_a(x) = axa^{-1} \forall x \in G$ is called the inner automorphism of G induced by a.

When G is a group, we use $Aut(G)$ to denote the set of all automorphisms of G and $Inn(G)$ to denote the set of all inner automorphisms of G.

Aut(G) and Inn(G) are Groups

Theorem 5.3. The set of automorphisms of a group and the set of inner automorphisms of a group are both groups under the operation of function composition.

proof

Automorphisms

The identity automorphism is $\phi(x) = x$ since for any automorphism $\alpha \circ \phi = \alpha(\phi(x)) = \alpha(x)$ and $\phi \circ \alpha = \phi(\alpha(x)) = \alpha(x)$. Each automorphism has a inverse by Theorem 5.3 property 1, ϕ^{-1}. Suppose we have unique Automorphisms ϕ, α, β. Then suppose $(\phi \circ \alpha) \circ \beta = \phi(\alpha(\beta(x)))$. Now $\phi \circ (\alpha \circ \beta) = \phi(\alpha(\beta(x)))$, which shows associativity holds, hence the set of Automorphisms is a group.

Inner Automorphisms

The identity inner automorphism is $\phi(x) = \epsilon x \epsilon^{-1} = \epsilon x \epsilon = x, \forall x$. Consider two inner automorphisms $\phi(x) = axa^{-1}, \alpha(x) = a^{-1}xa$ then $\phi \circ \alpha = \phi(a^{-1}xa) = a(a^{-1}xa)a^{-1} = aa^{-1}xaa^{-1} = x$, the same steps can be used for $\alpha \circ \phi$. For associativity, function composition is associative as shown in the last proof.

$\mathbf{Aut}(Z_n) \approx U(n)$

Theorem 5.4. For every positive integer n, Aut(Z_n) is isomorphic to U(n).

proof

The permutation is determined by $\alpha(1)$. Since the order of Z_n is n, $\alpha(1) \in U(n)$. Now consider a transformation from the group of automorphisms to U(n) $T : \alpha \longrightarrow \alpha(1)$. Since we know $\alpha(k) = k\alpha(1)$ T is one to one. Consider $\alpha, \beta \in Aut(Z_n)$ and $\alpha(1) = \beta(1)$ then $\alpha(k) = k\alpha(1) = k\beta(1) = \beta(k) \forall k$ therefore $\alpha = \beta$. Next to prove T is onto, let $r \in U(n)$ and consider the mapping α defined by $\alpha(s) = sr \ mod \ n$. Now since $T : \alpha \longrightarrow \alpha(1)$ T is $\alpha(1) = 1 * r \ mod \ n = r$, T is onto. Finally, consider $\alpha, \beta \in Aut(Z_n)$ then

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

So T is operation preserving and an isomorphism.

6 Cosets and Lagrange's Theorem

Cosets of H in G

Definition 6.1. Let G be a group and H be a non-empty subset of G. For any $a \in G$, the set $\{ah|h \in H\}$ is denoted by aH. Similarly, we can define Ha by $\{ha|h \in H\}$ along with $aHa-1$. If H is a subgroup of G, aH is the left coset of H in G containing a and Ha the right coset H in G containing a. The element a would then be called the representative of the coset. $|aH|$ denotes the number of elements in the set aH, and following this definition the same can be said for $|Ha|$.

Some quick examples to help solidify the idea,

Consider $G = S_3 = \{(1), (23), (12), (123), (132), (13)\}$ and $H = \{(1), (13)\}$, then we may write the left cosets of H in G,

$$(1)H = H$$

$$(12)H = \{(12), (12)(13)\} = \{(12), (132)\} = (132)H$$

Notice that since the element of the group (132) appeared in the result $(12)H$ and $(132)H$ are the same coset. This is a precursor to a property later.

$$(13)H = \{(13), (1)\} = H$$

$$(23)H = \{(23), (23)(13)\} = \{(23), (123)\} = (123)H$$

Another example consider $H = \{0, 3, 6\}$ and $G = Z_9$ under addition.

$$0 + H = 3 + H = 6 + H$$

$$1 + H = \{1, 4, 7\} = 4 + H = 7 + H$$

$$2 + H = \{2, 5, 8\} = 5 + H = 7 + H$$

Properties of Cosets

Theorem 6.1. Let H be a subgroup of G, and let a and b be elements of G. Then,

1. $a \in aH$.
2. $aH = H$ if and only if $a \in H$.
3. $(ab)H = a(bH)$ and $H(ab) = (Ha)b$.

4. $aH = bH$ if and only if $a \in bH$.
5. $aH = bH$ or $aH \cap bH = \emptyset$
6. $aH = bH$ if and only if $a^{-1}b \in H$.
7. $|aH| = |bH|$.
8. $aH = Ha$ if and only if $H = aHa^{-1}$.
9. aH is a subgroup of G if and only if $a \in H$.

proof

1. $a = ae \in H$.
2. Suppose $aH = H$. Then since $a = ae$ and $e \in H$ by definition we have $a \in aH$ and since we defined $aH = H$ we have $a \in H$. Now assume that $a \in H$. We will show $aH \subseteq H$ and $H \subseteq aH$. $aH \subseteq H$ since a subgroup must be closed. Next let $h \in H$ and since $a \in H$ by Theorem 2.1 we have if H is a subgroup with $a \in H$ and $h \in H$ then $a^{-1}h \in H$. Thus $h = eh = (aa^{-1})h = a(a^{-1}h) \in aH$ and $H \subseteq aH \implies H = aH$.
3. This follows directly from associativity.
4. If $aH = bH$, then $a \in aH = bH$. Conversely, if $a \in bH$ we have $a = bh$ where $H \in H$ then we can write $(bh)H = b(hH) = bH$.
5. Suppose an element c is in $aH \cap bH$. Then we have that $aH = bH$ by property 4 as $cH = aH$ but $bH = cH$ therefore $aH = bH$.
6. Since $aH = bH$ if $H = a^{-1}bH$ then by property 2 $a^{-1}b \in H$.
7. Define a map $ah \to bh$. This obviously maps aH onto bH. To show that it is one to one and thus has the same order suppose $h_1, h_2 \in H$ then denote the map by ϕ. Now suppose $\phi(ah_1) = \phi(ah_2) \implies bh_1 = bh_2 \implies h_1 = h_2$, thus one to one.
8. $aH = Ha$ if and only if $(aH)a^{-1} = (Ha)a^{-1} = h(aa^{-1}) = H$ thus $H = aHa^{-1}$.
9. If aH is a subgroup $e \in aH$ and by property 5 $aH = eH = H$ thus $a \in H$. Now if $a \in H$ then by property 2 $aH = H$ and H is already a subgroup of G.

Lagrange's Theorem

Theorem 6.2. If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$. Moreover the number of distinct left (right) cosets of H in G is $\frac{|G|}{|H|}$

proof

Let $a_1H, a_2H, ..., a_rH$ be left cosets of H in G. We know from property 1 $a_i \in a_iH$ thus for every element in G it is an element of some coset a_iH. Then,

$$G = a_1H \cup a_2H \cup ... \cup a_rH$$

Then since these are disjoint by property 5, since $aH = a_iH$, thus

$$|G| = |a_1H| + |a_2H| + ... + |a_rH|$$

but by property 7 we can say

$$|G| = r|H|$$

Thus $\frac{|G|}{|H|} = r$.

An important point is that this Theorem gives us a list of candidates for the subgroups of G since they must be a factor of $|G|$. It is important to note however just because a group has order equal to a factor of the group it is not necessarily a subgroup and it is not a requirement for any group to have a subgroup of order equal to one of its factors.

Next, the notation $|G : H|$ is introduced to mean the number of cosets of H in G.

$|G : H| = \frac{|G|}{|H|}$

Corollary 6.3. *If G is a finite group and H is a subgroup of G then $|G : H| = \frac{|G|}{|H|}$.*

proof

View the proof of Lagrange's Theorem.

$|a|$ Divides $|G|$

Corollary 6.4. *If G is a finite group the order of each element divides the order of the group.*

proof

Recall the order of a element is the order of the subgroup generated by that element.

Groups of Prime Order Are Cyclic

Corollary 6.5. *Every group of prime order is isomorphic to Z_p.*

proof

Suppose $|G|$ is a prime number p and $a \in G$ with $a \neq e$. Then $|\langle a \rangle|$ divides p but it can only be 1 or p and we already said $a \neq e \implies |\langle a \rangle| = p = |G|$. Then consider the map $\phi : G \to Z_p$ where $\phi(a^k) = k \bmod p$. This is clearly onto and one to one. Now finally $\phi(a^i a^j) = \phi(a^{i+j}) = (i+j) \bmod p = (\phi(a^i) + \phi(a^j)) \bmod p = ((i \bmod p) + (j \bmod p)) \bmod p = (i+j) \bmod p$ thus this is isomorphic.

$$a^{|G|} = e$$

Corollary 6.6. *Let G be a finite group and $a \in G$ then $a^{|G|} = e$.*

proof

By Corollary 6.4 we know $|a|$ divides $|G|$ thus $r|a| = |G|$ and since the order of a by definition is a number such that a raised to this number is e and $|G|$ is multiples of this number $a^{|G|} = e$.

Fermat's Little Theorem

Corollary 6.7. *For every integer a and every prime p, $a^p \bmod p = a \mod p$.*

proof

By the division algorithm we know $a = pm + r$. Then $a \bmod p = r$ so we must show $r^p \bmod p = r$. Since $0 \leq r \leq p-1$ we can say $r \in U(p)$. Then by the preceding Corollary $r^{|U(p)|} = r^{p-1} \bmod p = 1 \bmod p = 1 \implies rr^{p-1} \bmod p = r^p \bmod p = r$.

$$|HK| = |H||K|/|H \cap K|$$

Theorem 6.8. Suppose H, K are two finite subgroups of a group and define the set $HK = \{hk : h \in H, k \in K\}$. Then $|HK| = |H||K|/|H \cap K|$.

proof

Although the set HK has $|H||K|$ products, not all of these need to be distinct elements of G. To determine the order of HK we must know the extent to which this occurs. Consider $hk = h'k'$ then we may write $hh'^{-1} = k'k^{-1}$, clearly $hh'^{-1} \in H$ and $k'k^{-1} \in K$. Since these are equal in different subgroups it is in the intersection of H and K. Now for every element in the intersection of H and K, $t = h_t = k_t$ can be written as $h_t e = k_t e$ thus every element of the intersection is in HK. We can also say that each element in HK must be at least $|H \cap K|$ big since for each element in the intersection t we can write $(ht^{-1})(tk)$. Thus each element is represented by exactly $|H \cap K|$ products. So $|HK| = |H||K|/|H \cap K|$.

Stabilizer Point

Definition 6.2. Let G be a group of permutations of a set S. For each i in S let $stab_G(i) = \{\phi \in G | \phi(i) = i\}$. We call $stab_G(i)$ the stabilizer of i in G.

Orbit of a Point

Definition 6.3. Let G be a group of permutations of a set S. For each i in S let $orb_G(i) = \{\phi(i) | \phi \in G\}$. The set $orb_G(i)$ is a subset of S called the orbit of i under G. We use $|orb_G(i)|$ to denote the number of elements in $orb_G(i)$.

Orbit-Stabilizer Theorem

Theorem 6.9. Let G be a finite group of permutations of a set S. Then, for any i from S, $|G| = |orb_G(i)||stab_G(i)|$.

proof

By Lagrange's Theorem we know $|G|/|stab_G(i)|$ is the number of distinct left cosets of $stab_G(i)$ in G. Now since we are hypothesizing that $|G|/|stab_G(i)| = |orb_G(i)|$ and we know $|G|/|stab_G(i)|$ is the number of distinct cosets of $|stab_G(i)|$ in G we could find a one to one correspondence between the left and cosets of $|stab_G(i)|$ in G and $|orb_G(i)|$ to show they have equal order. To do this we use the map T $\phi Stab_G(i)$ to $\phi(i)$ where ϕ is an element of the group of permutations and $Stab_G(i)$ is a set of permutations from G. This maps the coset $\phi Stab_G(i)$ to $\phi(i)$. To show this map is well defined consider two different cosets and show, $\alpha Stab(i) = \beta Stab(i)$ implies $\alpha(i) = \beta(i)$. $\alpha Stab(i) = \beta Stab(i) \implies \alpha^{-1}\beta \in Stab(i)$ by property 6 so $(\alpha^{-1}\beta)(i) = i \implies \alpha(i) = \beta(i)$. Reversing this shows that the map is one to one. Lastly, showing this map is onto consider $\alpha(i) = j$ for some $\alpha \in G$ and clearly $T(\alpha Stab(i)) = \alpha(i) = j$ so T is onto.

7 External Direct Products

Definition 7.1. Let $G_1, G_2, G_3, ..., G_n$ be a finite collection of groups. The external direct products of $G_1, G_2, G_3, ..., G_n$, written as $G_1 \oplus G_2 \oplus G_3 \oplus ... \oplus G_n$, the set of all n-tuples for which the i^{th} component is an element of G_i and the operation is component-wise. In symbols, $G_1 \oplus G_2 \oplus G_3 \oplus ... \oplus G_n = \{(g_1, g_2, g_3, ..., g_n) : g_i \in G_i\}$. We define $(g_1, g_2, g_3, ..., g_n)(g_1', g_2', g_3', ..., g_n') = (g_1 g_1', g_2 g_2', g_3 g_3', ..., g_n g_n')$. When G_i is finite we also define $|G_1 \oplus G_2 \oplus G_3 \oplus ... \oplus G_n| = |G_1||G_2|...|G_n|$.

As an example consider $U(8) \oplus U(10)$, we can write this as

$$= \{(1,1),(1,3),(1,7),(1,9),(3,1),(3,3),(3,7),(3,9),(5,1),(5,3),$$

$$(5,7),(5,9),(7,1),(7,3),(7,7),(7,9)\}$$

The product of $(3,7)(7,9) = (5,3)$ where the first component using multiplication mod 8 and the second component using multiplication mod 10. The order of the group is $4 * 4 = 16$

Order of an element in a Direct Product

Theorem 7.1. The order of an element in a direct product of a finite number of finite groups is the least common multiple of the orders of the components of the element. In symbols,

$$|(g_1, g_2, g_3, .., g_n)| = lcm(|g_1|, |g_2|, |g_3|, ..., |g_n|)$$

proof

Let e_i be the identity of of the group G_i. Let $s = lcm(|g_1|, |g_2|, |g_3|, ..., |g_n|)$ and $t = |(g_1, g_2, g_3, .., g_n)|$. Clearly, $(g_1, g_2, g_3, .., g_n)^s = (e_1, e_2, e_3, ..., e_n)$ so we know $t \leq s$. We also clearly see $(g_1^t, g_2^t, g_3^t, .., g_n^t) = (g_1, g_2, g_3, .., g_n)^t = (e_1, e_2, e_3, ..., e_n)$ so $s = t$.

Criterion for $G \oplus H$ to be Cyclic

Theorem 7.2. Let G and H be finite cyclic groups. Then $G \oplus H$ is cyclic iff $|G|$ and $|H|$ are relatively prime.

proof

Let $|G| = m$ and $|H| = n$, so that $|G \oplus H| = mn$. Assume $G \oplus H$ is cyclic and $gcd(m, n) = d$ and (g, h) is a generator of $G \oplus H$. Then $(g, h)^{mn/d} = ((g^m)^{n/d}, (h^n)^{m/d}) = (e, e)$ so we have $mn = |(g, h)| \leq mn/d \implies d = 1$ so m and n are relatively prime.

Now let $G = \langle g \rangle$, $H = \langle h \rangle$ and $gcd(m, n) = 1$. Then $|(g, h)| = lcm(m, n) = mn = |G \oplus H|$ so (g, h) is a generator of $|G \oplus H|$.

Criterion for $G_1 \oplus G_2 \oplus G_3 \oplus ... \oplus G_n$ to be Cyclic

Corollary 7.3. *An external direct product of n groups is cyclic iff $|G_i|$ and $|G_j|$ are relatively prime when $i \neq j$.*

Criterion for $Z_{n_1 n_2 n_3 .. n_k} \approx Z_{n_1} \oplus Z_{n_2} \oplus ... \oplus Z_{n_k}$

Corollary 7.4. *Let $m = n_1 n_2 n_3 .. n_k$ then Z_m is isomorphic to $Z_{n_1} \oplus Z_{n_2} \oplus ... \oplus Z_{n_k}$ iff n_i and n_j are relatively prime when $i \neq j$.*

$U_k(n)$

Definition 7.2. $U_k(n) = \{x \in U(n) : x \ mod \ k = 1\}$.

$U(n)$ as an External Direct Product

Theorem 7.5. Suppose s and t are relatively prime. Then $U(st)$ is isomorphic to the external direct product of $U(s)$ and $U(t)$,

$$U(st) \approx U(s) \oplus U(t)$$

Moreover, $U_s(st) \approx U(t)$ and $U_t(st) \approx U(s)$.

Corollary 7.6. *Let $m = n_1 n_2 n_3 ... n_k$ where $gcd(n_i, n_j) = 1$ for $i \neq j$. Then,*

$$U(m) \approx U(n_1) \oplus U(n_2) \oplus ... \oplus U(n_k)$$

8 Normal Subgroups and Factor Groups

Normal Group

Definition 8.1. A subgroup H of a group G is called a normal subgroup of G if $aH = Ha$ for all $a \in G$. We denote this $H \triangleleft G$.

Normal Subgroup Test

Theorem 8.1. A subgroup H of G is normal if and only if $xHx^{-1} \subseteq H$ for all $x \in H$

proof

If H is normal in G then for any $g \in G$ and $h \in H$ there is an $h' \in H$ such that $xh = h'x$. Thus, $xhx^{-1} = h'$ and therefore $xHx^{-1} \subseteq H$.

Conversely, if $xHx^{-1} \subseteq H$ for all x, then, letting $x = a$, we have $aHa^{-1} \subseteq H$ or $aH \subseteq Ha$. On the other hand, letting $x = a^{-1}$ have $a^{-1}H(a^{-1})^{-1} = a^{-1}HaH$ or $Ha \subseteq aH$ thus $xH = Hx$ for all x since we have, $aH \subseteq Ha$ and $Ha \subseteq aH$.

Factor/Quotient Groups

Theorem 8.2. Let G be a group and let H be a normal subgroup of G. The set $G/H = \{aH : a \in G\}$ is a group under the operation $(aH)(bH) = abH$. This is a group of cosets. *proof*

We need to show that this is indeed a well defined operation. That is the result needs to be independent of the representatives we pick. So suppose $aH = bH$ and $cH = dH$ for $a, b, c, d \in G$. Then we want to show $aHcH = bHdH$. This says that two cosets, no matter what representative we choose from them, will produce the same result. Now notice since H is normal we can write,

$$(aH)(cH) = a(Hc)H = a(cH)H = acH$$

and similarly,

$$(bH)(dH) = b(Hd)H = b(dH)H = bdH$$

So we want to show,

$$acH = bdH$$

Now since $aH = bH$ and $cH = dH$ there is some, $h_1, h_1 \in H$ such that, $a = bh_1$ and $c = dh_2$. So,

$$acH = bh_1dh_2H = bh_1dH$$

Now since H is normal,

$$bh_1dH = bh_1Hd = bHd$$

Now since H is normal,

$$bHd = bdH$$

Thus this operation is well defined. Notice that $e \in G$ causes $(eH)(aH) = aH$, if $b^{-1}b = e$ then, $(b^{-1}H)(bH) = b^{-1}bH = eH = H$ and $((aH)(bH))(cH) = (abH)(cH) = abcH = (aH)(bcH) = (aH)((bH)(cH))$. Finally it is clear that $|G/H| = |G : H|$.

The converse of this statement is actually true, that is if $aHbH = abH$ defines a group operation on the set of left cosets of H in G and H is normal is G.