Group Theory Part-1

Prep Smart. Stay Safe. go Gradeup

gradeup.co

Group Theory Part-1

Content:

1. **Group**
2. **Properties of Group**
3. **Auto orphism**
4. **Sub Group**
5. **COSET**
6. **Cyclic Group**

What is a group?

If G is a nonempty set, a binary operation μ on G is a function μ : G × G → G

For example + is a binary operation defined on the integers Z. Instead of writing +(3, 5) = 8 we instead write 3 + 5 = 8. Indeed the binary operation μ is usually thought of as multiplication and instead of μ(a, b) we use notation such as ab, a + b, a ◦ b and a ∗ b. If the set G is a finite set of n elements we can present the binary operation, say ∗, by an n by n array called the multiplication table. If a, b ∈ G, then the (a, b)-entry of this table is a ∗ b. text

$*$	a	b	c	d
a	a	b	c	a
b	a	c	d	d
c	a	b	d	c
d	d	a	c	b

width in in: 4.50089in Here is an example of a multiplication table for a binary operation ∗ on the set G = {a, b, c, d}.

Note that $(a * b) * c = b * c = d$ but $a * (b * c) = a * d = a$.

A binary operation $*$ on set G is associative if $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$

Subtraction − on Z is not an associative binary operation, but addition + is. Other examples of associative binary operations are matrix multiplication and function composition. A set G with a associative binary operation $*$ is called a semi group. The most important semi groups are groups.

A group $(G, *)$ is a set G with a special element e on which an associative binary operation $*$ is defined that satisfies: 1. $e * a = a$ for all $a \in G$;

2. for every $a \in G$, there is an element $b \in G$ such that $b * a = e$.

Example of groups:

1. The integers Z under addition +.

2. The set GL2(R) of 2 by 2 invertible matrices over the reals with matrix multiplication as the binary operation. This is the general linear group of 2 by 2 matrices over the reals R.

3. The set of matrices

$$G = \left\{ e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, a = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, b = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, c = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\}$$

under matrix multiplication. The multiplication table for this group is:

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

4. The non-zero complex numbers C is a group under multiplication.

WHAT IS A GROUP?

5. The set of complex numbers G = {1, i, −1, −i} under multiplication. The multiplication table for this group is:

$*$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

6. The set Sym (X) of one to one and onto functions on the n-element set X, with multiplication defined to be composition of functions. (The elements of Sym (X) are called permutations and Sym (X) is called the symmetric group on X. This group will be discussed in more detail later. If $\alpha \in$ Sym (X), then we define the image of x under α to be x α. If α, $\beta \in$ Sym (X), then the image of x under the composition $\alpha\beta$ is x $\alpha\beta$ = (x α) β .)

Some properties are unique.

Lemma 1.2.1. If $(G, *)$ is a group and $a \in G$, then $a*a = a$ implies $a = e$.

Lemma 1.2.2.

In a group $(G, *)$ (i) if $b * a = e$, then $a * b = e$ and

(ii) $a * e = a$ for all $a \in G$

Furthermore, there is only one element $e \in G$ satisfying (ii) and for all $a \in G$, there is only one $b \in G$ satisfying $b * a = e$.

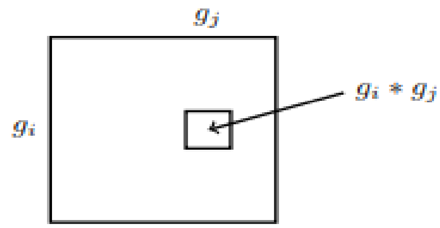
SOME PROPERTIES ARE UNIQUE.

Let $(G, *)$ be a group. The unique element $e \in G$ satisfying $e * a = a$ for all $a \in G$ is called the identity for the group $(G, *)$. If $a \in G$, the unique element $b \in G$ such that $b * a = e$ is called the inverse of a and we denote it by $b = a^{-1}$.

Let $[x_1\ x_2\ x_3 \cdots x_n]$ be the row labeled by g_i in the multiplication table. I.e. $x_j = g_i * g_j$. If $x_{j1} = x_{j2}$, then $g_i * g_{j1} = g_i * g_{j2}$. Now multiplying by g^{-1}_i on the left we see that $g_{j1} = g_{j2}$. Consequently $j1 = j2$. Therefore every row of the multiplication table contains every element of G exactly once a similar argument shows that every column of the multiplication table contains every

If $n > 0$ is an integer, we abbreviate $\underbrace{a * a * a * \cdots * a}_{n \text{ times}}$ by a^n. Thus $a^{-n} =$ $(a^{-1})^n = \underbrace{a^{-1} * a^{-1} * a^{-1} * \cdots * a^{-1}}_{n \text{ times}}$

Let $(G, *)$ be a group where $G = \{g_1, g_2, \ldots, g_n\}$. Consider the multiplication table of $(G, *)$.



element of G exactly once A table satisfying these two properties is called a Latin Square.

A latin square of side n is an n by n array in which each cell contains a single element form an n-element set S = {s1, s2, . . . , sn}, such that each element occurs in each row exactly once. It is in standard form with respect to the sequence s1, s2, . . . , sn if the elements in the first row and first column are occur in the order of this sequence.

The multiplication table of a group (G, ∗), where G = {e, g1, g2, . . . , gn−1} is a latin square of side n in standard form with respect to the sequence e, g1, g2, . . . , gn−1.

The converse is not true. That is not every latin square in standard form is the multiplication table of a group. This is because the multiplication represented by a latin square need not be associative.

A group (G, ∗) is abelian if a ∗ b = b ∗ a for all elements a, b ∈ G.

(a) Let (G, ∗) be a group in which the square of every element is the identity. Show that G is abelian.

(b) Prove that a group (G, ∗) is abelian if and only if f : G → G defined by f(x) = x $^{-1}$ is a homomorphism.

When are two groups the same?

When ever one studies a mathematical object it is important to know when two representations of that object are the same or are different. For example consider the following two groups of order 8.

$$G = \left\{ \begin{array}{lll} g_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, & g_2 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, & g_3 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \\ g_4 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, & g_5 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, & g_6 = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \\ g_7 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, & g_8 = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} & \end{array} \right\}$$

$(G, \cdot)$ is a group of 2 by 2 matrices under matrix multiplication.

$$H = \left\{ \begin{array}{l} h_1 : x \mapsto x, h_2 : x \mapsto ix, h_3 : x \mapsto -x, h_4 : x \mapsto -ix, \\ h_5 : x \mapsto \bar{x}, h_6 : x \mapsto -\bar{x}, h_7 : x \mapsto i\bar{x}, h_8 : x \mapsto -i\bar{x} \end{array} \right\}$$

(√ H, ◦) is a group complex functions under function composition. Here i = −1 and a + bi = a − bi. The

The multiplication tables for G and H respectively are:

	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8
g_1	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8
g_2	g_2	g_3	g_4	g_1	g_7	g_8	g_6	g_5
g_3	g_3	g_4	g_1	g_2	g_6	g_5	g_8	g_7
g_4	g_4	g_1	g_2	g_3	g_8	g_7	g_5	g_6
g_5	g_5	g_8	g_6	g_7	g_1	g_3	g_4	g_2
g_6	g_6	g_7	g_5	g_8	g_3	g_1	g_2	g_4
g_7	g_7	g_5	g_8	g_6	g_2	g_4	g_1	g_3
g_8	g_8	g_6	g_7	g_5	g_4	g_2	g_3	g_1

	h_1	h_2	h_3	h_4	h_5	h_6	h_7	h_8
h_1	h_1	h_2	h_3	h_4	h_5	h_6	h_7	h_8
h_2	h_2	h_3	h_4	h_1	h_7	h_8	h_6	h_5
h_3	h_3	h_4	h_1	h_2	h_6	h_5	h_8	h_7
h_4	h_4	h_1	h_2	h_3	h_8	h_7	h_5	h_6
h_5	h_5	h_8	h_6	h_7	h_1	h_3	h_4	h_2
h_6	h_6	h_7	h_5	h_8	h_3	h_1	h_2	h_4
h_7	h_7	h_5	h_8	h_6	h_2	h_4	h_1	h_3
h_8	h_8	h_6	h_7	h_5	h_4	h_2	h_3	h_1

Observe that these two tables are the same except that different names were chosen. That is the one to one correspondence given by:

WHEN ARE TWO GROUPS THE SAME?

9 carries the entries in the table for G to the entries in the table for H. More precisely we have the following definition.

Two groups (G, ∗) and (H, ◦) are said to be isomorphic if there is a one to one correspondence θ : H → G such that

x	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8
$\theta(x)$	h_1	h_2	h_3	h_4	h_5	h_6	h_7	h_8

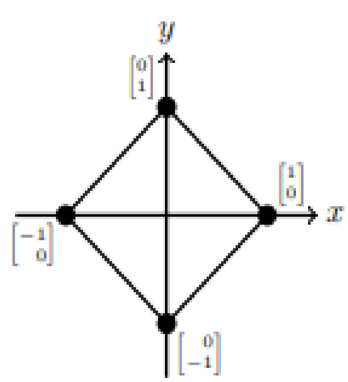
θ(g1 ∗ g2) = θ(g1) ◦ θ(g2)

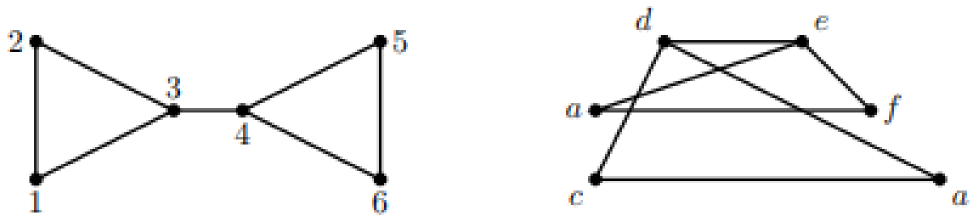
for all g1, g2 ∈ G. The mapping θ is called an isomorphism and we say that G is isomorphic to H. This last statement is abbreviated by G ∼= H.

If θ satisfies the above property but is not a one to one correspondence, we say θ is homomorphism. These will be discussed later

A geometric description of these two groups may also be given. Consider the square drawn in the[x/y]-plane with vertices the vectors in the set:

$$\mathcal{V} = \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} -1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ -1 \end{bmatrix} \right\}.$$





$\Gamma_1 = (\mathcal{V}_1, \mathcal{E}_1)$ $\Gamma_2 = (\mathcal{V}_2, \mathcal{E}_2)$

The auto orphism group of a graph

For another example of what is meant when two mathematical objects are the same consider the graph.

A graph is a pair Γ = (V, E) where 1. V is a finite set of vertices and

2. E is collection of unordered pairs of vertices called edges.

If {a, b} is an edge we say that a is adjacent to b. Notice that adjacent to is a symmetric relation on the vertex set V. Thus we also write a adj b for {a, b} ∈ E

Two graphs Γ1 = (V1, E1) and Γ2 = (V2, E2) are isomorphic graphs if there is a one to one correspondence θ : V1 → V2 such that

a adj b if and only if θ(a) adj θ(b)

A one to one correspondence from a set X to itself is called a permutation on X. The set of all permutations on X is a group called the symmetric group and is denoted by Sym (X). The multiplication is function composition.

The automorphism group of a graph Γ = (V, E) is that set of all permutations on V that fix as a set the edges E.

Example:

The set of isomorphisms from a graph Γ = (V, E) to itself is called the automorphism group of Γ. We denote this set of mappings by Aut(Γ).

Before proceeding with an example let us make some notational conventions. Consider the one to one correspondence $\theta : x \to x^{\theta}$ given by

THE AUTOMORPHISM GROUP OF A GRAPH

x	1	2	3	4	5	6	7	8	9	10	11
x^{θ}	11	2	4	1	6	5	8	9	7	10	3

A simpler way to write θ is:

$$\theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 11 & 2 & 4 & 1 & 6 & 5 & 8 & 9 & 7 & 10 & 3 \end{pmatrix}$$

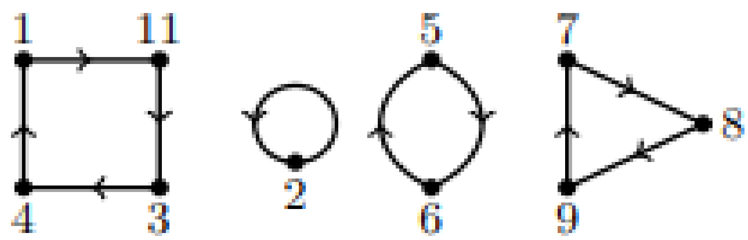
THE AUTOMORPHISM GROUP OF A GRAPH

The image of x under θ is written in the bottom row. below x in the top row. Although this is simple an even simpler notation is cycle notation. The cycle notation for θ is

$\theta = (1, 11, 3, 4)(2)(5, 6)(7, 8, 9)(10)$

To see how this notation works we draw the diagram for the graph with edges: $\{x, x\theta\}$ for each x. But instead of drawing a line from x to x θ we draw a directed arc: $x \to \theta(x)$.

The resulting graph is a union of directed cycles. A sequence of vertices enclosed between parentheses in the cycle notation for the permutation θ is called a cycle of θ. In the above example the cycles are:



The resulting graph is a union of directed cycles. A sequence of vertices enclosed between parentheses in the cycle notation for the permutation θ is called a cycle of θ. In the above example the cycles are:

(1, 11, 3, 4), (2), (5, 6), (7, 8, 9), (10)

If the number of vertices is understood the convention is to not write the cycles of length one. (Cycles of length one are called fixed points. In our example 2 and 10 are fixed points.) Thus we write for θ

θ = (1, 11, 3, 4)(5, 6)(7, 8, 9)

Now we are in good shape to give the example. The automorphism group of Γ1 is.

$$\mathrm{Aut}(\Gamma_1) = \left\{ \begin{array}{l} e, (1,2), (5,6), (1,2)(5,6), (1,5)(2,6)(3,4), \\ (1,6)(2,5)(3,4), (1,5,2,6)(3,4), (1,6,2,5)(3,4) \end{array} \right\}$$

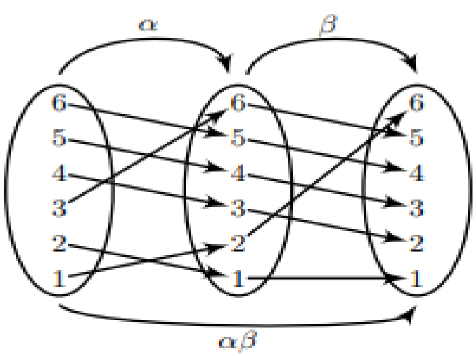
e is used above to denote the identity permutation.

The product of two permuations α and β is function composition read from left to right. Thus

$x^{\alpha\beta} = (x^{\alpha})^{\beta}$

Write the permutation that results from the product

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 11 & 2 & 4 & 1 & 6 & 5 & 8 & 9 & 7 & 10 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 3 & 6 & 4 & 11 & 9 & 7 & 8 & 10 & 5 & 2 & 1 \end{pmatrix}$$



in cycle notation.

2. Show that Aut(Γ1) is isomorphic to the group of symmetries of the square given in Section 1.3. 3.

3. What is the automorphism group of the graph $\Gamma = (V, E)$ for which

$V = \{1, 2, 3, 4, 5, 6\}$; and

$E = \{\{1, 2\}, \{2, 3\}, \{1, 3\}, \{4, 5\}, \{4, 6\}, \{5, 6\}, \{1, 4\}, \{2, 5\}, \{3, 6\}\}$

Subgroups

A nonempty subset S of the group G is a subgroup of G if S a group under binary operation of G. We use the notation $S \leq G$ to indicate that S is a subgroup of G.

Theorem : A subset S of the group G is a subgroup of G if and only if

(i) $1 \in S$;

(ii) $a \in S \Rightarrow a^{-1} \in S$;

(iii) $a, b \in S \Rightarrow ab \in S$.

Although the above theorem is obvious it shows what must be checked to see if a subset is a subgroup. This checking is simplified by the next two theorems.

Theorem: If S is a subset of the group G, then S is a subgroup of G if and only if S is nonempty and whenever $a, b \in S$, then $ab^{-1} \in S$.

Theorem: If S is a subset of the finite group G, then S is a subgroup of G if and only if S is nonempty and whenever $a, b \in S$, then $ab \in S$.

Examples of subgroups.

1. Both {1} and G are subgroups of the group G. Any other subgroup is said to be a proper subgroup. The subgroup {1} consisting of the identity alone is often called the trivial subgroup.

2. If a is an element of the group G, then
   $(a) = \{. . . , a^{-3}, a^{-2}, a^{-1}, 1, a, a^2, a^3, a^4, . . .\}$
   are all the powers of a. This is a subgroup and is called the cyclic subgroup generated by a.

3. If $\theta : G \to H$ is a homomorphism, then

   $\text{kernel}(\theta) = \{x \in G : \theta x = 1\}$

   and

   $\text{image}(\theta) = \{y \in H : \theta x = y \text{ for some } x \in G\}$

   are subgroups of G and H respectively.

Theorem: Let X be a subset of the group G, then there is a smallest subgroup S of G that contains X. That is if T is any other subgroup containing X, then $T \supset S$.

Cosets

f S is a subgroup of G and $a \in G$, then

$Sa = \{xa : x \in S\}$

is a right coset of S.

If S is a subgroup of G and $a, b \in G$, then it is easy to see that $Sa = Sb$ whenever $b \in Sa$. An element $b \in Sa$ is said to be a coset representative of the coset Sa.

Theorem: Let S be a subgroup of the group Gand let $a, b \in G$. Then $Sa = Sb$ if and only if $ab-1 \in S$.

Theorem: Cosets are either identical or disjoint.

The number of elements in the finite group G is called the order of G and is denoted by $|G|$.

If S is a subgroup of the finite group G it is easy to see that $|Sa| = |S|$ for any coset Sa. Also because cosets are identical or disjoint we can choose coset representatives $a_1, a_2, \ldots, ar$ so that

$G = S_{a1} \dot\cup\ S_{a2} \dot\cup\ S_{a3} \cup \cdots \dot\cup\ S_{ar}$.

Thus G can be written as the disjoint union of cosets and these cosets each have size |S|. The number r of right cosets of S in G is denoted by |G : S|and is called the index of S in G. This discussion establishes the following important result of Lagrange (1736-1813).

If $x \in G$ and G is finite, the order of x is $|x| = |(x) |$.

Corollary: If $x \in G$ and G is finite, then |x| divides |G|.

Corollary: If |G| = p a prime, then G is cyclic.

Cyclic groups

Among the first mathematics algorithms we learn is the division algorithm for integers. It says given an integer m and an positive integer divisor d there exists a quotient q and a remainder r < d such that m/ d = q + r/ d . This is quite easy to prove and we encourage the reader to do so. Formally the division algorithm is.

(Division Algorithm) Given integers m and d > 0, there are uniquely determined integers d and r satisfying

$m = dq + r$

and

$0 \leq r < d$

Theorem: Every subgroup of a cyclic group is cyclic.

Theorem: Let G = hai have order n. Then for each k dividing n, G has a unique subgroup of order k, namely $(a^{n/k})$.

How many generators?

Let G be a cyclic group of order 12 generated by a. Then

$G = \{1, a^1, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^{10}, a^{11}\}$

Observe that

$\langle a^5 \rangle = \{1, a^5, a^{10}, a^3, a^8, a, a^6, a^{11}, a^4, a^9, a^2, a^7\} = G$

Thus a^5 also generates G. Also, a^7, a^{11} and a generate G. But, the other elements do not. Indeed:

$$\begin{aligned}
\langle 1 \rangle &= \{1\} \\
\langle a^6 \rangle &= \{1, a^6\} \\
\langle a^4 \rangle = \langle a^8 \rangle &= \{1, a^4, a^8\} \\
\langle a^3 \rangle = \langle a^9 \rangle &= \{1, a^3, a^6, a^9\} \\
\langle a^2 \rangle = \langle a^{10} \rangle &= \{1, a^2, a^4, a^6, a^8, a^{10}\}
\end{aligned}$$

The Euler phi function or Euler totient is

$\varphi(n) = |\{x : 1 \leq x \leq n \text{ and } \gcd(x, n) = 1\}|$

the number of positive integers $x \leq n$ that have no common divisors with n.

theorem: Let G be a cyclic group of order n generated by a. Then G has $\varphi(n)$ generators.

Corollary: Let G be a cyclic group of order n. If d divides n, the number of elements of order d in G is $\varphi(d)$. It is 0 otherwise

Example: Computing with the Euler phi function.

1. $\phi(40) = \phi(2^3 5^1) = \phi(2^3)\phi(5^1) = (2^3 - 2^2)(5^1 - 5^0) = (4)(4) = 16$
2. $\phi(300) = \phi(2^2 3^1 5^2) = \phi(2^3)\phi(3^1)\phi(5^2) = (2^2 - 2^1)(3^1 - 3^0)(5^2 - 5^1) =$ $(3)(2)(20) = 120$
3. $\phi(6^3) = \phi(2^3 3^3) = \phi(2^3)\phi(3^3) = (2^3 - 2^2)(3^3 - 3^2) = (4)(18) = 72$

Normal subgroups

A subgroup N of the group G is a normal subgroup if g −1Ng = N for all g ∈ G. We indicate that N is a normal subgroup of G with the notation N E G.

Example: 1. Every subgroup of an abelian group is a normal subgroup. 2. The subset of matrices of $GL_2(R)$ that have determinant 1 is a normal subgroup of $GL_2(R)$.

Theorem: The subgroup N of G is a normal subgroup of G if and only if g −1Ng ⊆ N for all g ∈ G.

Theorem: If N is a normal subgroup of G, then the cosets of N form a group. If G is finite, this group has order |G : N|.

LAWS

because N is normal in G. Thus the product of two cosets is a coset. It is easy to see N is the identity and Nx^{-1} is $(Nx)^{-1}$ for this multiplication. Thus the cosets form a group as claimed.

The group of cosets of a normal subgroup N of the group G is called the quotient group or the factor group of G by N. This group is denoted by G/N which is read "G modulo N" or "G mod N".

The most important elementary theorem of group theory is:

Theorem: Let $\theta : G \to H$ be a homomorphism. Then $N = \text{kernel}(\theta)$ is a normal subgroup of G and $G/N \sim= \text{image}(\theta)$.

Theorem: If $H \leq G$ and N E G, then $HN = NH$ is a subgroup of G.

Theorem: Let H and N be subgroups of G with N normal. Then $H \cap N$ is normal in H and $H/(H \cap N) \sim= NH/N$

Theorem: Let $M \subset N$ be normal subgroups of G. Then N/M is a normal subgroup of G/M and

$(G/M)/(N/M) \sim= G/N$

The fourth law of isomorphism is the law of correspondence given in Theorem 2.6.5. If X and Y are any sets and $f : X \to Y$ is any onto function. then f defines a one-to-one correspondence between the all of the subsets of Y and some of the subsets of X. Namely if $S \subseteq X$

$f(S) = \{f(x) : x \in S\} \subseteq Y$

and if $T \subseteq Y$, then

$f^{-1}(T) = \{x \in X : f(x) \in T\}$.

The Law of Correspondence is a group theoretic translation of these observation.

A subgroup N is a maximal normal subgroup of the group G if N E G and there exists no normal subgroup strictly between N and G.

Conjugation

Let x and y be elements of the group G. If there is a $g \in G$ such that $g^{-1}xg = y$, then we say that x is conjugate to y. The relation "x is conjugate to y" is an equivalence relation and the equivalence classes are called conjugacy classes. We denote the conjugacy class of x by K(x). Thus,

$K(x) = \{g^{-1}xg : g \in G\}$

If x is an element of the group G, then it is easy to see that $K(x) = \{x\}$ if and only if x commutes with every element of G. So, in particular, conjugacy classes of abelian groups are not interesting.

The center of G, is

$Z(G) = \{x \in G : xg = gx, \text{ for all } g \in G\}$.

It is the set of all elements of G that commute with every element of G. Observe that for $x \in G$, $|K(x)| = 1$ if and only if $x \in Z(G)$. Consequently if the group G is finite we can write

$G = Z(G) \dot\cup K(x_1) \dot\cup K(x_2) \dot\cup \cdots \dot\cup K(x_r)$

Theorem: Let x be an element of the finite group G. The number of conjugates of x is the index of $C_G(x)$ in G. That is

$|K(x)| = |G : C_G(x)|$.

Theorem: If G is a group of order p n for some prime p, then $|Z(G)| > 1$.

Theorem: If G is a finite abelian group whose order is divisible by a prime p, then G contains an element of order p.

Cayley's theorem

In 1854 Author Cayley gave a one-to-one correspondence between an arbitrary finite group G and a subgroup of the symmetric group degree |G|. Burnside attributes the first proof that correspondence was a homomorphism to Jordan, but the first published proof is by Walther Dyck in 1882. Nevertheless it has become known as Cayley's theorem. If G is a finite group, then G acts on the the elements of G by right multiplication: g 7→ xg. The kernel of the action is K = {x ∈ G : xg = x}. But if xg = x, then g = 1 and hence K = 1. Furthermore xg = yg if and only if x = y and so the right multiplication map g 7→ xg is a one-to-one homomorphism and we have Cayley's theorem.

Theorem: Every finite group G is isomorphic to a subgroup of Sym (G). This representation of G as a group of permutations of degree |G| is called the right regular representation of G.

it is shown that there is a isomorphism between Sym (X) and P(X) the set of permutation matrices index by X. Because the entries of a permutation matrix are only 0 and 1, we may regard them as living in an arbitrary field F. Thus we have the following corollary to Cayley's theorem.

Theorem: f G is a finite group of order n and F is a field, then G is isomorphic to a subgroup of $GL_n(F)$ the multiplicative group of invertible n by n matrices with entires in F. In general the group $GL_d(F)$ of invertible d by d matrices is called the general linear group of degree d over the filed F and the determinant map

det : $GL_d(F) \rightarrow F$

has kernel $SL_d(F)$ the special linear group of matrices with determinant 1. Note that $GL_d(F)/SL_d(F)$ ~= F ? the multiplicative group of non-zero elements of the filed F. If ∆ : G 7→ GLd(R), for some degree d then ∆

is said to be a representation of G of degree d. The degree d need not be the order |G|.

Now we consider the action on the right cosets of a subgroup. Let S_n denote the symmetric group of degree n.

The Sylow theorems

A finite group G is a p-group if $|G| = p^x$, for some prime p and positive integer x. A maximal p-subgroup of a finite group G is called a Sylowp-subgroup subgroup-of G.

If P is a Sylow p-subgroup of G and H is a p-subgroup of G such that $P \subseteq H$, then H = P

Let H be a subgroup of a group G. A subgroup S of G is conjugate to H if and only if $S = g^{-1}Hg$ for some $g \in G$.

Notice that conjugate subgroups are isomorphic.

Let H be a subgroup of G. The normalizer of H in G is

$N_G(H) = \{g \in G : g^{-1}Hg = H\}$

Theorem: Let P be a Sylow p-subgroup of G. Then $N_G(P)/P$ has no element whose order is a power of p except for the identity.

Theorem: Let P be Sylow p-subgroup of G and let $g \in G$ have order a power of p. If $g^{-1}Pg = P$, then $g \in P$.

Theorem: Let G be a finite group with Sylow p-subgroup P.

Theorem: Let G be a finite group of order $|G| = p\,|^x m$, where p - m, then every Sylow p-subgroup of G has order p^x.

Some applications of the Sylow theorems

Let H and K be groups the direct product of H and K is the group H × K

$H \times K = \{(h, k) : h \in H \text{ and } k \in K\}$

with multiplication $(h_1, k_1)(h_2, k_2) = (h_1h_2, k_1k_2)$.

Theorem: Let H and K be subgroups of the group G. If

(1) G = HK,

(2) H and K are both normal subgroups of G, and

(3) $H \cap K = \{1\}$,

then $G \sim= H \times K$

Theorem: Every group of order 2p is either cyclic or dihedral, when p is an odd prime.

Theorem: Let G be a group of order |G| = pq, where p > q are primes. If q does not divide p − 1, then G is cyclic.

Theorem: Let G is a group of order |G| = pq, where p > q are primes. If q divides p − 1, then either G is cyclic or G is generated by two elements a and b satisfying

$a^p = 1$, $b^q = 1$, and $b^{-1}ab = a^r$

Theorem: Every group G of order 12 that is not isomorphic to A_4 contains an element of order 6 and a normal Sylow 3-subgroup.