Theorem 11.4 (Burnside) The number of equivalence classes into which a set S is divided by the equivalence relation induced by a permutation group $(G, \circ)$ of S is given by

$$\frac{1}{|G|} \sum_{\pi \in G} \psi(\pi)$$

where $\psi(\pi)$ is the number of elements that are invariant under the permutation π.

So that we can appreciate more the meaning of Burnside's theorem, let us illustrate its application before proceeding to the proof. Let $S = \{a, b, c, d\}$, and let G be the permutation group consisting of

$$\pi_1 = \begin{pmatrix} abcd \\ abcd \end{pmatrix} \quad \pi_2 = \begin{pmatrix} abcd \\ bacd \end{pmatrix} \quad \pi_3 = \begin{pmatrix} abcd \\ abdc \end{pmatrix} \quad \pi_4 = \begin{pmatrix} abcd \\ badc \end{pmatrix}$$

The equivalence relation on S induced by G is shown in Fig. 11.8. Clearly, S is divided into two equivalence classes, $\{a, b\}$ and $\{c, d\}$. To compute the number of equivalence classes according to Burnside's theorem, we note that since $\psi(\pi_1) = 4$, $\psi(\pi_2) = 2$, $\psi(\pi_3) = 2$, and $\psi(\pi_4) = 0$, the number of equivalence classes is

$$\tfrac{1}{4}(4 + 2 + 2 + 0) = 2$$

PROOF For any element s in S, let $\eta(s)$ denote the number of permutations under which s is invariant. Then

$$\sum_{\pi \in G} \psi(\pi) = \sum_{s \in S} \eta(s)$$

because both $\sum_{\pi \in G} \psi(\pi)$ and $\sum_{s \in S} \eta(s)$ count the total number of invariants under all the permutations in G. [One way to count the invariances is to go through the permutations one by one and count the number of invariances under each permutation. This gives $\sum_{\pi \in G} \psi(\pi)$ as the total count. Another way to count the invariances is to go through the elements one by one and count the number of permutations under which an element is invariant. That gives $\sum_{s \in S} \eta(s)$ as the total count.]

Let a and b be two elements in S that are in the same equivalence class. We want to show that there are exactly $\eta(a)$ permutations mapping a into b. Since a and b are in the same equivalence class, there is at least one such permutation which we shall denote by π_x. Let $\{\pi_1, \pi_2, \pi_3, \ldots\}$ be the set of the $\eta(a)$ permutations under which a is invariant. Then, the $\eta(a)$ permutations in the set $\{\pi_x \circ \pi_1, \pi_x \circ \pi_2, \pi_x \circ \pi_3, \ldots\}$ are permutations that map a into b. First, we see that these permutations are all distinct because, if $\pi_x \circ \pi_1 = \pi_x \circ \pi_2$, we have

$$\pi_x^{-1} \circ (\pi_x \circ \pi_1) = \pi_x^{-1} \circ (\pi_x \circ \pi_2)$$

This gives $\pi_1 = \pi_2$, which is impossible. Secondly, we see that no other permutation in G maps a into b. Suppose that there is a permutation π_y that maps a into b. Then, $\pi_x^{-1} \circ \pi_y$ is a permutation that maps a into a, because π_x^{-1} maps b into a. Since $\pi_x^{-1} \circ \pi_y$ is a permutation in the set $\{\pi_1, \pi_2, \pi_3, \ldots\}$, $\pi_x \circ (\pi_x^{-1} \circ \pi_y) = \pi_y$ is a permutation in the set $\{\pi_x \circ \pi_1, \pi_x \circ \pi_2, \pi_x \circ \pi_3, \ldots\}$. Therefore, we conclude that there are exactly $\eta(a)$ permutations in G that map a into b.

Let $a, b, c, \ldots, h$ be the elements in S that are in one equivalence class. All the permutations in G can be categorized as those that map a into a, those that map a into b, those that map a into c, ..., and those that map a into h. Since we have shown that there are exactly $\eta(a)$ permutations in each of these categories we have

$$\eta(a) = \frac{|G|}{\text{number of elements in the equivalence class containing } a}$$

Using a similar argument, we obtain

$$\eta(b) = \eta(c) = \cdots = \eta(h)$$

$$= \frac{|G|}{\text{number of elements in the equivalence class containing } a}$$

and, therefore,

$$\eta(a) + \eta(b) + \eta(c) + \cdots + \eta(h) = |G|$$

It follows that, for any equivalence class of elements in S,

$$\sum_{\text{all } s \text{ in equivalence class}} \eta(s) = |G|$$

and

$$\sum_{s \in S} \eta(s) = \left(\begin{matrix}\text{number of equivalence classes}\\ \text{into which } S \text{ is divided}\end{matrix}\right) \times |G|$$

Therefore, we have

Number of equivalence classes into which S is divided

$$= \frac{1}{|G|} \sum_{s \in S} \eta(s) = \frac{1}{|G|} \sum_{\pi \in G} \psi(\pi) \qquad \square$$

then $e(b)$ is a group code.

Q. Show that.

$(B^n, \oplus)$ is a Group.

Solⁿ :-

(1) $\forall\ b_1, b_2 \in B^n$, $b_1 \oplus b_2 \in B^n$

closed.

(2) $\forall\ b_1, b_2, b_3$, $(b_1 \oplus b_2) \oplus b_3$

$= b_1 \oplus (b_2 \oplus b_3)$

Associative.

(3) $e = 000$ (n times is identity in B^n.

(4) Every element is inverse of itself

Hence $(B^n, \oplus)$ is a group.

(ii) $\delta(x \cdot y) = |x \oplus y|$

≥ 0

Hence proved.

(iii) Let $\delta(x, y) = 0$

$\Leftrightarrow |x \oplus y| = 0$

$\Leftrightarrow x = y$

(iv) $\delta(x, y)$

$= |x \oplus y|$

$= |x \oplus z \oplus z \oplus y|$

$\leq |x \oplus z| + |z \oplus y|$

$= \delta(x, z) + \delta(z, y)$

Group Codes

let $e : B^m \to B^n$

where $(B^n, \oplus)$ is a group.

then if $e(b) = \{ b \mid b \in B^n \}$ is the subgroup of B^n.

$|x|$ = no. of one's in x

$|x| = 2$

$|y| = 4$

$|x \oplus y| = 2$.

Humming Distance

$$\delta(x,y) = |x \oplus y|$$
$$= 2$$

Theorem – 1 :-

(Long ques Imp. from [illegible])

Let x & y Bqe the word of B^n.

(i) $\delta(x,y) = \delta(y,x)$

(ii) $\delta(x,y) \geq 0$

(iii) $\delta(x,y) = 0$ iff $x = y$

(iv) $\delta(x,y) \leq \delta(x,z) + \delta(z,y)$.

Proof :-

(i) $\delta(x,y)$

$= |x \oplus y|$

$= |y \oplus x| = \delta(y,x)$

Homomorphism & Isomorphism:-

Let G_1 and G_2 be the two group. Then a map 'f' from G_1 to G_2

$$f : G_1 \rightarrow G_2$$

is homomorphic if $f(g+h) = f(g) \cdot f(h)$

It is isomorphic if it is one to one.

Group code:-

Bit = the value of 1 known as bit, word = combination of Bits of fixed length.

$B = \{0, 1\}$

code word

$$e : B^m \rightarrow B^n, \; n > m$$

is a encoding function and $e(b) \in B^n$ is a code word.

Bitwise Operations :-

$$x = 0101$$
$$y = 1111$$
$$x \oplus y = 1010$$

$x \oplus y = x\bar{y} + y\bar{x}$

additive identity.

3. The operation . is distributive over the operation +.

field:-

Let (A, +, ·) be an algebraic system with two binary operations. (A, +, ·) is called a field if:

1. (A, +) is an abelian group.
2. (A − {0}, ·) is an abelian group.
3. The operation . is distributive over the operation +.

Hence $O(H)$ divides $O(G)$.

Ring

An algebraic system $(A, +, \cdot)$ is called a ring if the following conditions are satisfied.

1. $(A, +)$ is an abelian group.
2. $(A, \cdot)$ is a semigroup.
3. The operation $\cdot$ is distributive over the operation $+$.

Integral domain:-

Let $(A, +, \cdot)$ be an algebraic system with two binary operations $(A, +, \cdot)$ is called an integral domain if:

1. $(A, +)$ is an abelian group.
2. The operation $\cdot$ is commutative.

Furthermore, if $c \neq 0$ and $c \cdot a = c \cdot b$, then $a = b$, where 0 denotes the

Langrange's theerem

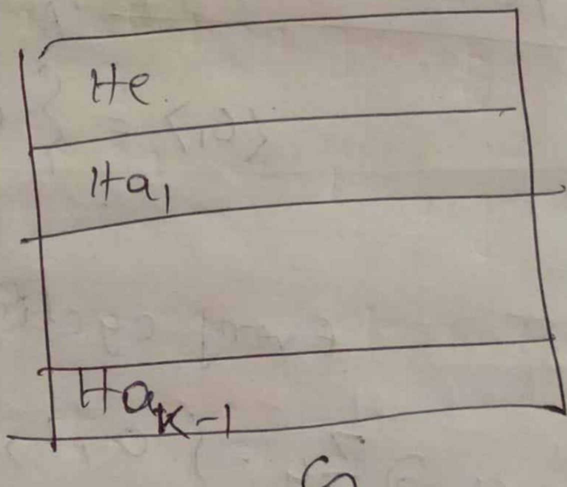
If G is a finite group and H is a subgroup of G. Then $o(H)$ (order of H) divides $o(G)$ (order of G)

$o(G) = n$, $o(H) = m$

Proof
Let $Ha = \{ha \mid h \in H, a \in G\}$
is a right Coset of G.

Since G can be partition into distincts right Coset.

$\therefore G = He \cup Ha_1 \cup \cdots Ha_{k-1}$



$o(G) = o(H) + o(Ha_1) \cdots + o(Ha_{k-1})$

Again $o(H) = o(Ha_1) \cdots = o(Ha_{k-1})$
$= m$

$= m + m + \cdots + m$ (k-times)

$= km$