Chapter 11 - Subgroups

Definition: Let G be a group. A subset $H \subset G$ which is a group under the same operation is called a subgroup of G. We denote this as

$$H < G$$

read "subgroup"

Example: ① $H = \{\varepsilon, (1\,2\,3), (1\,3\,2)\}$ is a subgroup of S_4.

② $K = \{\varepsilon, (1\,2), (1\,2\,3)\}$ is not a subgroup of S_4,

Theorem 11.1.1 — Two-Step Subgroup Test. Let G be a group and H a nonempty subset of G. If

(a) for every $a, b \in H$, $ab \in H$ (closed under multiplication), and
(b) for every $a \in H$, $a^{-1} \in H$ (closed under inverses),

then H is a subgroup of G.

Creating Subgroups:

Let G be a group, and $g_1, g_2, \dots, g_k \in G$. We can create a subgroup by forming the set of all possible products, and inverses of products, of g_i's. This is called the subgroup generated by $\{g_1, \dots, g_k\}$:

$$\langle g_1, g_2, \dots, g_k \rangle = \{ x \in G : x = g_{j_1}^{m_1} g_{j_2}^{m_2} \cdots g_{j_\ell}^{m_\ell} \text{ for some } j_i\text{'s and } m_i\text{'s} \}$$

Examples: $S_3 = \{\varepsilon, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$

$\langle (1\,2) \rangle =$

$\langle (1\,3) \rangle =$

$\langle (2\,3) \rangle =$

$\langle (1\,2\,3) \rangle =$

$\langle (1\,2), (1\,3) \rangle =$, $\langle (1\,2), (1\,2\,3) \rangle =$

Examples: ① $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$, operation $+_6$ (order 6 group)

$\langle 0 \rangle =$

$\langle 2 \rangle =$

$\langle 3 \rangle =$

$\langle 1 \rangle =$

② S_{10}, $\alpha = (1\,2)$, $\beta = (1\,5\,3)(2\,4)$

$\langle \alpha, \beta \rangle < S_{10}$ of size ______

In [2]:
```
S10=SymmetricGroup(10)
a=S10("(1,2)")
b=S10("(1,5,3)(2,4)")
H=PermutationGroup([a,b])  # could use H=S10.subgroup([a,b])
H.order()
```

Out[2]:
```
120
```

In [3]:
```
a*b*a*b^2
```

Out[3]:
```
(1,4,3,2)
```

In [4]:
```
S10("(1,4,3,2)") in H
```

Out[4]:
```
true
```

In [5]:
```
S10("(8,9,10)") in H
```

Out[5]:
```
false
```

③ $D_4 = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$

$\langle R_{90} \rangle =$

$\langle R_{180} \rangle =$

$\langle H, V \rangle =$

In [6]:
```
D4=DihedralGroup(4)
D4sublist=["()","(1,3)(2,4)", "(1,4)(2,3)", "(1,2)(3,4)"]
D4subnames=["R0","R180","H","V"]
D4.cayley_table(names=D4subnames,elements=D4sublist)
```

Out[6]:
```
*      R0  R180     H     V
  +------------------------
  R0|  R0  R180     H     V
R180| R180   R0     V     H
   H|   H     V    R0  R180
   V|   V     H  R180    R0
```

④ In S_6 what is the subgroup generated by $\alpha = (1\,2)$, $\beta = (3\,4)$, $\gamma = (5\,6)$?

Theorem 11.4.1 — Lagrange's Theorem. If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$.

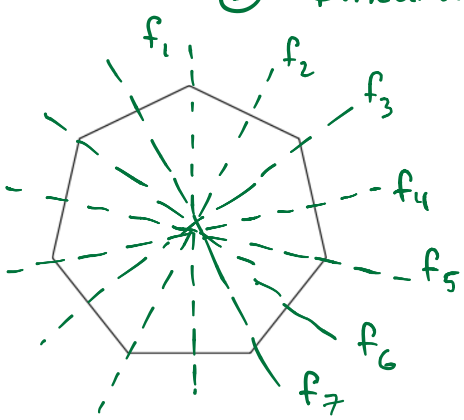
Corollary 11.4.2 — $ord(a)$ divides $|G|$. In a finite group, the order of each element divides the order of the group.

Theorem 11.4.3 — Cauchy's Theorem. Let p be a prime dividing $|G|$. Then there is a $g \in G$ of order p.

Example: ① Rubik's Cube group

$$RC_3 = \langle R, L, U, D, F, B \rangle < S_{48}$$

② Dihedral group D_7



r = cw rotation through $360/n$ degrees

f_i = flip over axis f_i

Elements	order

Cyclic Groups Revisited :

Theorem 11.5.1 — Fundamental Theorem of Cyclic Groups. Every subgroup of a cyclic group is cyclic. Moreover, if $|\langle g\rangle| = n$ then for each divisor k of n there is exactly one subgroup of $\langle g\rangle$ of order k.

Example: $\langle (1\,2\,3)(4\,5) \rangle$

Finding other generators of a cyclic group :

Theorem 11.5.2 — Generators of Cyclic Groups. Let $G = \langle g\rangle$ be a cyclic group of order n. Then $G = \langle g^k\rangle$ if and only if $\gcd(k,n) = 1$.

So there are $\varphi(n)$ different possible generators.

Euler φ function : $\varphi(n) =$ [# of integers between 1 and n that are relatively prime to n]

Theorem 11.5.4 — Generators, Subgroups, and Orders in $\mathbb{Z}_n$. Consider the group of integers modulo n, $\mathbb{Z}_n$.

(a) An integer k is a generator of $\mathbb{Z}_n$ if and only if $\gcd(k,n) = 1$.

(b) For each divisor k of n, the set $\langle n/k\rangle$ is the unique subgroup of $\mathbb{Z}_n$ of order k, moreover, these are the only subgroups of $\mathbb{Z}_n$.

(c) For each $k \mid n$ the elements of order k are of the form $\ell \cdot (n/k)$ where $\gcd(\ell,k) = 1$. The number of such element is $\phi(k)$, and each of these is a generator of the unique subgroup of order k.

Example: Determine all subgroups of $\mathbb{Z}_{24}$

subgroup	order	generators