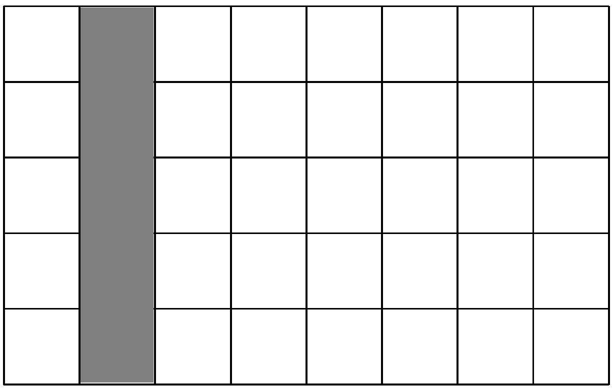
## Week 9

If $G/N$ is a group, then $N$ acts as an identity element in $G/N$. $N$ is regarded as being collapsed to a simple element $o$ (addition) or $e$ (multiplication).



N

$|G| = 40$, $|N| = 5$, $|G/N| = 8$.

**Example** $Z_4 \times Z_6 \;/ < (2,3) > \cong\; Z_4 \times Z_3 \;\simeq\; Z_{12}$

$$| < (2,3) > | = 2 \;\Rightarrow\; |Z_4 \times Z_6/_{<(2,3)>}| = 12$$

**Example** $Z_m \times Z_m/_{<(0,1)>} \;\simeq\; Z_m$

**Defn.** A group is simple if it is nontrivial and has no proper nontrivial normal subgroups.

**Theorem** A finite simple abelian group is isomorphic to $Z_p$ for some prime $p$.

**Theorem** (Thompson and Feit, 1963)

Every finite nonabelian simple group if of even order. Construct an example (as large order as possible)

"Monster"

808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000, 000,000.

**Theorem** $\varphi : G \overset{homo.}{\longrightarrow} G', \ N \lhd G, \ N' \lhd \varphi[G]$.

(1) $\varphi[N] \lhd \varphi[G]$.

(2) $\varphi^{-1}[N'] \lhd G$.

**Defn.** A maximal normal subgroup of $G$ : $M$

No $N$ satisfies $M \subsetneq N \subsetneq G$ and $N \lhd G$.

**Theorem** If $M$ is a maximal normal subgroup of $G$, then $G/M$ is simple.

**Proof** $\gamma : G \to G/M$ is a homomorphism.

$\gamma(g) = gM$ and $\gamma(g_1 g_2) = (g_1 g_2)M = (g_1 M)(g_2 M) = \gamma(g_1)\gamma(g_2)$.

Now, if $H \lneq G/M$, $H \lhd G/M$ and $H \neq M$, then $\gamma^{-1}[H]$ is a subgroup of $G$ and $M \subsetneq \gamma^{-1}[H] \subsetneq G$. Since $\gamma^{-1}[H] \lhd G$ and $M$ is maximal, no such $H$ exists. Therefore $G/M$ is simple.

On the other hand, if $N$ is a normal subgroup of $G$ such that $M \subsetneq N \subsetneq G$ then $\gamma[N] \lhd G/M$. Since $\gamma[N] \supsetneq M$ and $\gamma[N] \subsetneq G/M$, $G/M$ is not simple. Therefore, no such $N$ exists. The proof is concluded. ■

**Ex.(Bonus)** Show that $A_n$ is a simple for $n \geq 5$

**Group Action on a set**

**Defn.** Let $X$ be a set and $G$ a group. an action of $G$ on $X$ is a map $* : G \times X \longrightarrow X$ such that

1. $e * x = x$ for each $x \in X$.
2. $(g_1 g_2) * x = g_1 * (g_2 * x)$ $\forall$ $x \in X$ and $g_1$, $g_2 \in G$.

Under these conditions, $X$ is a $G$-set.

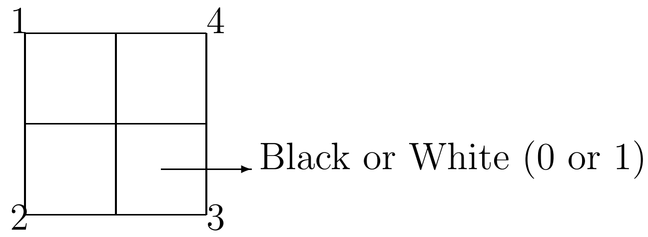
**Example** (Most important)

Let $X$ be a nonempty set and $H \leq S_X$ (the set of all permutations of $X$). Then $X$ is an $H$-set and the action $*$ of $\sigma \in H$ on $X$ is defined as $\sigma * x = \sigma(x)$ for each $x \in X$.

**Example** Let $H \leq G$. Then $G$ is an $H$-set under conjugation where $*(h, g) = hgh^{-1}$, or $h * g = hgh^{-1}$.

**Example** Scalars in vector spaces: $\mathcal{R}^*$ is a multiplicative group. Let $X$ be the set of all vectors. Then $X$ is an $\mathcal{R}^*$-set (or $\mathcal{C}^*$).

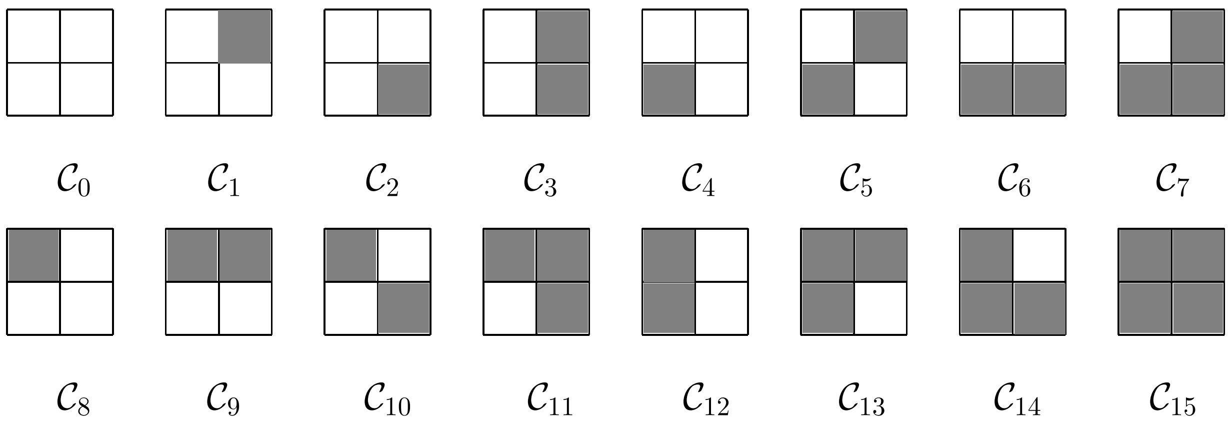
**Example**




$X = \{(x_1, x_2, x_3, x_4) | \; X_i \in \{0, 1\}, \; i = 1, 2, 3, 4\}$

Let $\mathcal{C}_j = (x_1, x_2, x_3, x_4)$ where $j = x_1 \cdot 2^3 + x_2 \cdot 2^2 + x_3 \cdot 2 + x_4$.

$X = \mathcal{C}_0, \mathcal{C}_1, \cdots, \mathcal{C}_{15}$.




$G = \{\rho_0, \rho_1, \rho_2, \rho_3\} \quad \rho_1 = (1234), \; \rho_2 = (13)(24), \; \rho_3 = (1432)$

$\rho_0 * \mathcal{C}_i = \mathcal{C}_i, \quad \rho_1 * \mathcal{C}_2 = \mathcal{C}_1, \quad \rho_1 * \mathcal{C}_1 = \mathcal{C}_8, \cdots$.

**Defn.** Let $X$ be a $G$-set. Let $x \in X$ and $g \in G$.

$X_g = \{x | \; g * x = x\}$ and $G_X = \{g \in G | \; g * x = x\}$

$X_{\rho_1}$ (From above example)$=\{\mathcal{C}_0, \mathcal{C}_5\}$

$X_{\rho_2} = \{\mathcal{C}_0, \mathcal{C}_5, \mathcal{C}_{10}, \mathcal{C}_{15}\}$

$X_{\rho_3} = \{\mathcal{C}_0, \mathcal{C}_{15}\}$

$X_{\rho_4} = X$

$G_{\mathcal{C}_0} = G$

$G_{\mathcal{C}_1} = \{\rho_0\}$

$G_{\mathcal{C}_2} = \{\rho_0\}$

$G_{\mathcal{C}_5} = \{\rho_0, \rho_2\}$

$\vdots$

**Observation** $\sum_{g\in\ G} |X_g| = \sum_{x\in X} |G_X|$.

**Proof** Consider $(g, x)$ such that $g * x = x$. (Two-way counting!)
e.g. $(\rho_2, \mathcal{C}_5)$.

**Theorem** Let $X$ be a $G$-set. For each $x_1, x_2 \in X$, let $x_1 \sim x_2$ if and only if $\exists\ g \in G$ such that $gx_1 = x_2$. Then $\sim$ is an equivalence relation.

$(*)$ $\sim$ induces a partition of $X$ into cells and each cell is called an orbit in $X$ under $G$. If $x \in X$, the cell containing $x$ is the orbit of $x$, denoted by **Gx**.

**Example** Orbits
$\{\mathcal{C}_0\}, \{\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_4, \mathcal{C}_8\}, \{\mathcal{C}_3, \mathcal{C}_6, \mathcal{C}_9, \mathcal{C}_{12}\}, \{\mathcal{C}_5, \mathcal{C}_{10}\}, \{\mathcal{C}_7, \mathcal{C}_{11}, \mathcal{C}_{13}, \mathcal{C}_{14}\}, \{\mathcal{C}_{15}\}$.

**Theorem** (Burnside's Formula)

Let $G$ be a finite group and $X$ a finite $G$-set. If $r$ is the number of orbits in $X$ under $G$, then $r|G| = \sum_{g\in G} |X_g| = \sum_{x\in X} |G_x|$.