# Groups

- Binary Operation: $*$ on a set $S$; $*: S\times S \to S$, a function from $S\times S$ to $S$.
  - E.g. $S = M_n(\mathbb{R})$, $*$ could be matrix multiplication, addition etc.
  - Association: $*$ is associative if $\forall a,b,c \in S$, $a*(b*c) = (a*b)*c$
- Group: $(G, *)$, an unordered pair of set $G$ and binary operation $*$ where the group axioms are satisfied:
  - (G1) $*$ is associative. (Associativity)
  - (G2) $\exists e \in G : e*g = g*e = g \ \forall g \in G$. (Identity)
  - (G3) $\forall g \in G\ \exists g' \in G : g*h = h*g = e$. (Invertibility / Inverse)
  - (G0) $g, h \in G \Rightarrow g*h \in G$. (Closure)
  - Uniqueness of identity: If $e, e'$ satisfy G2, then $e = e*e' = e'$.
    - Proof: By axiom G2, $e = e*e' = e'$.
  - Uniqueness of inverse: If $g*h = e = g*g'$ then $g' = h$.
    - Proof: $(g*g')*h = e*g' = g'$; $g'*(g*h) = g'*e = g'$.
  - Equations in a group: $gx = h$ or $x*g = h$.
    - Proof: given $gx = h$, $g^{-1}*(gx) = g^{-1}*h$, $(g^{-1}*g)*x = g^{-1}*h$, $e*x = g^{-1}*h$, $x = g^{-1}*h$.
  - Inverse of a product: $(g*h)^{-1} = h^{-1}*g^{-1}$
    - Proof: $(g*h)*(h^{-1}*g^{-1}) = g*(h*h^{-1})*g^{-1} = g*e*g^{-1} = g*g^{-1} = e$; $(h^{-1}*g^{-1})*(g*h) = h^{-1}*(g^{-1}*g)*h = h^{-1}*e*h = h^{-1}*h = e$.
  - Examples:
    - $(\mathbb{R}, +)$ is a group since $0 \in \mathbb{R}$ and $\forall x \in \mathbb{R}$, $-x \in \mathbb{R}$ is its inverse. (Additive group over $\mathbb{R}$)
    - $(\mathbb{R}\setminus\{0\}, \times)$ is a group since $1 \in \mathbb{R}$ and $\forall x \in \mathbb{R}$, $x^{-1} \in \mathbb{R}$ is its inverse. (Multiplicative group over $\mathbb{R}$)
    - For any field $F$ and $n \in \mathbb{N}$, $(F^n, +)$ is a group.
    - For $V$ a vector space over $F$, $(V, +)$ is a group.
    - General Linear Group: $GL(n, F)$ is the set $G$ of $n\times n$ invertible matrices over $F$ and operation matrix multiplication. (Important group)
      - $A, B \in G$, since $\det(AB) = \det A \cdot \det B \neq 0$ (Closure)
      - $A, B, C \in G \Rightarrow A(BC) = (AB)C$ (Associativity)
      - $I_n \in G$ (Identity)
      - $A^{-1} \in G$ (Inverse)
  - Power notation: For $g \in G$, $G$ from $(G, \cdot)$, we have $g^{m+n} = g^m \cdot g^n$ and $g^{mn} = (g^m)^n$, $m, n \in \mathbb{N}$.
    - If $m, n \in \mathbb{Z}$, we have
      1) $g^{m+n} = g^m \cdot g^n$
      2) $(g^m)^n = g^{mn}$
      3) $g^m \cdot g^n = g^{m+n} = g^n \cdot g^m$
      4) $g^{-m} = (g^m)^{-1}$
      - Proof:
        1) Let $m = 0$, then $g^{0+n} = g^n \cdot g^0$ by definition. Let $m = k$, $k \in \mathbb{N}$, so then $g^{k+n} = g^k \cdot g^n$. Now $g^{k+1+n} = g^{k+n} \cdot g^1 = g^k \cdot g^n \cdot g^1 = g^{k+1} \cdot g^n$.
        2) $(g^m)^1 = g^m = g^{m\cdot 1}$ } true for $m = 0, 1$. $(g^m)^n = g^{mn}$. Assume true for $m < n$. Then $g^m \cdot g^{m(n-1)} \Rightarrow g^{m+m(n-1)} = g^{mn}$, $g^{m+mn-m} = g^{mn}$, $(g^m)^n = g^{mn}$.
        3) $n = 0$, $g^{m+0} = g^m = g^0 \cdot g^m = g^m \cdot g^0$. Suppose $g^{m+n} = g^n \cdot g^m$, $g^{m+(n+1)} = g^{(m+n)+1} = g^{m+n} \cdot g^1 = g^n \cdot g^m \cdot g^1 = g^n \cdot g^{m+1}$.
        4) $n = 0$, $g^{-m+0} = g^{-m} = g^0 \cdot g^{-m} = (g^m)^{-1} \cdot g^{-m}$. Suppose $(g^m)^{-n} = g^{-mn}$, $g^{-m+-n} = g^{-m-n} = g^{-m} \cdot g^{-n} = (g^m)^{-1} \cdot (g^n)^{-1} = (g^m \cdot g^n)^{-1}$.
  - Subgroups: Subset $H$ of $G$ is a subgroup if $(H, \cdot)$ satisfies the group axioms. $H \leq G$ denotes $H$ is a subgroup of $G$.
    - Trivial Subgroups: $G$, $\{e\}$
    - $H = \{g \in G : \det(g) = 1\} \leq GL(n, \mathbb{R})$
    - $K = \{\text{rank} = n\} \leq GL(n, \mathbb{R})$
    - $2\mathbb{Z} \times 2\mathbb{Z} \times 2\mathbb{Z} \leq (\mathbb{Z}, +)$
    - $U = \{z^n : \theta \in \mathbb{R}\} \leq (\mathbb{C}^*, \cdot)$
    - Let $C = z^{2\pi\theta}$, then $\langle C \rangle \leq U \leq \mathbb{C}^*$
    - $\mathbb{Q}^* \leq \mathbb{R}^*$ (Subgroup but not subgroup)
    - $V = \{-1, 1\} \leq \mathbb{Z}$, $-1 + 1 \notin V$, $V \leq S_3$ (Subset but not group)
    - $\Rightarrow V \leq G$, $\Rightarrow$ this is a subgroup.
  - Test for a subgroup: Suppose $(G, \cdot)$ is a group and $H \subseteq G$. Then $H$ is a subgroup iff
    - $H \neq \emptyset$ (Non-empty)
    - $\forall h_1, h_2 \in H$, $h_1 h_2 \in H$ (Closure under operation)
    - $\forall h \in H$, $h^{-1} \in H$. (Closure under inverse)
    - Let assume there are more than one group element to show $H \leq G$. (i.e. $\Leftarrow$ direction)
      - $\Rightarrow$ subgroup shows $H \leq G \Rightarrow$ $G, H$ and inverse is in use the same as in $G$
      - $\Leftarrow$ $\exists g$, $g \in G$. $H = \{g^n : n \in \mathbb{Z}\}$.
      - (a) Associativity follows directly (G1)
        By closure, $h, g \in H \Rightarrow h^{-1}g \in H \Rightarrow h^{-1}*g \in H$ (G2)
        Existence of inverse follows (G3)
        Closure under operation follows (G0)
  - Cyclic Subgroup: Suppose $(G, \cdot)$ is a group and $g \in G$. The cyclic subgroup generated by $g$ is $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$.
    - $\hookrightarrow$ A group $(G, \cdot)$ is cyclic if $\exists g \in G$, $\langle g \rangle = G$. $g$ is the generator of $G$.
      - $\hookrightarrow$ E.g. $2\mathbb{Z} = \langle 2 \rangle$, $\mathbb{Z} = \langle 1 \rangle$
    - $\langle \alpha, \beta \rangle$ denotes a group generated by $\alpha$ and $\beta$, ie $\alpha^i \beta^j$
    - Cyclic group are abelian (Commutative). Proof: $\forall a, b \in G$, $a*b = b*a = a^{i+j}$ by $a^i \cdot a^j = a^j \cdot a^i$ or $b^i \cdot b^j = b^j \cdot b^i$
    - If $G$ is of prime order, it is cyclic.
    - Euler Totient function: For $n \in \mathbb{N}$, $\phi(n) = |\{k \in \mathbb{N} : 1 \leq k \leq n \text{ and } \gcd(k, n) = 1\}|$
      - $\hookrightarrow \forall n \in \mathbb{N}$, $\sum_{d \mid n} \phi(d) = n$ (sum over all divisors of $n$ replacing $d$ in for $k$ here)
      - For $G$ is cyclic, then count the $\phi(n)$ elements of order $n$.
      - Number of generators for $G$ is $\phi(n)$ if $G$ is of order $n$.
      - Gives the order of the multiplicative group $\mathbb{Z}_n^*$ is cyclic iff $n \in \{1, 2, 4, p^k, 2p^k\}$
      - Proof: Let $G$ be a cyclic group of order $n$. If $d \mid n$, then $\langle g^{n/d} \rangle$ forms a subgroup of order $d$. Any order of $g \in G$ has order dividing $n$. Then $\sum_{d \mid n} \phi(d) = n$ $\square$
    - Suppose $(G, \cdot)$ is a cyclic group and $G = \langle g \rangle$.
      1) If $H \leq G$, $H$ is cyclic. } Subgroups of cyclic groups are cyclic. $\square$
      2) Suppose $|G| = n$ and $m \in \mathbb{Z}$. Let $d = \gcd(m, n)$. Then $\langle g^m \rangle = \langle g^d \rangle$ and $|\langle g^d \rangle| = \frac{n}{d}$ (i.e. $\langle g^m \rangle = G \Leftrightarrow \gcd(m, n) = 1$). } Cyclic subgroups of the form $\langle g^m \rangle$ ($m \in \mathbb{Z}$) are such that $\gcd(m, n) = 1$
      3) If $|G| = n$ and $k \in \mathbb{N}$, then $G$ has a subgroup of order $k$ iff $k \mid n$, $\langle g^{n/k} \rangle$ is the subgroup. } $|\langle g^{n/k} \rangle| = |G|/k = n/k = d$. If $d \mid n$, then $G$ has a unique subgroup $G_d$ of order $d$.
      - Proof:
        1) Assume $H \neq \{e\}$. Let $S = \{n \in \mathbb{N} : g^n \in H\}$. Let $k = \min(S)$, so. Let $h \in H$, $h = g^m$. By $\langle g \rangle \leq G$, $m = qk + r$, $0 \leq r < k$. Then $h = g^m = g^{qk+r} = (g^k)^q \cdot g^r$. Since $h, g^k \in H$, we have $g^{-qk} \cdot h = g^r \in H$ by definition. So $g^r$ minimality of $k$ in $S$, we have $r = 0$. Then $h = g^{qk} \in \langle g^k \rangle$. Thus $H \leq \langle g^k \rangle$
        2) $d = \gcd(m, n)$. By Bezout, $\exists x, y$; $mx + ny = d$. Since $d \mid m$, $g^d = (g^m)^x$, $h \in H \Rightarrow h = g^{-n} \in \langle g^n \rangle$. $g^d = (g^m)^x \cdot (g^n)^y$. $\langle g^d \rangle \leq \langle g^m \rangle$ $\Rightarrow g^d \in \langle g^m \rangle$. Thus $\langle g^d \rangle \leq \langle g^m \rangle$. Consider $|\langle g^m \rangle| = \text{ord}(g^m)$. Since $d \mid n$, $n = kd$. Define $G_d = \{g^{jk} : \{g^k, \dots, g^{dk} = e\}$, $j = 1, \dots, d\}$. $\Rightarrow |\langle g^m \rangle| = \frac{n}{d} = k$
        3) Suppose $|G| = n$ and $k \mid n$. ($\Rightarrow$). Suppose $H \leq G$ and $|H| = k$. Then by Lagrange, $H = \{g^n, \dots, g^{n-k}\}$. $\Rightarrow |H| = |\langle g^{n/k} \rangle| \Rightarrow k \mid n$. ($\Leftarrow$) Suppose $k \mid n$. Then by 2), $\langle g^{n/k} \rangle$ is a subgroup of order $k$.
    - Finite Groups: $(G, \cdot)$ is a finite group if $G$ is a finite set. The order of $G$ is then $|G|$, the number of elements in $G$.
      - $\hookrightarrow$ If we have $a \in G$, then $|\langle a \rangle| \leq |G|$ (the order of an element is less or equal to the order of the group)
      - Proof: $|\langle a \rangle|$ is the number of permutation on $n$ elements, ie $|\{a, a*a, \dots, a*\dots*a\}|$
    - Lagrange's Theorem: Suppose $G$ is a finite group and $H$ is a subgroup of $G$. Then $|H|$ divides $|G|$. ($\frac{|G|}{|H|}$ = number of left cosets of $H$)
      - Proof: Suppose $G$ finite and $H \leq G$. Any $\{gH\} \subseteq H$. Therefore, any $g_1 g_2$, $\Rightarrow g_1 H \cap g_2 H = \emptyset$. Any $g \in G \Rightarrow g \in g_1 H$. $\therefore |G| = |H| \cdot$ number of distinct left cosets. $\Rightarrow |H|$ divides $|G|$ $\square$
    - Permutation: A bijection or from $X$ to $X$, i.e. $\sigma: X \to X$, where $X$ is non-empty. $Sym(X)$ denotes the set of all permutations of $X$. ($Sym(X)$ = the set of all permutations of $X$)
      - Given $n$, $S_n$ = $Sym$ is a permutation on $n$ elements
      - Notation: Let $X = \{a\} = \{1, 1, \dots, n\}$. Then we denote $\sigma(a) \to \sigma(a)$ by $\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$
      - Cycle decomp notation: $\sigma = (1\ 2\ 3\ 4\ 5)$
      - Triple notation: $\sigma = (1\ 2\ 3)(4\ 5)$ (you can do it from left to right, or from right to left)
    - Symmetric Group: Let $X$ be any non-empty set then $Sym(X)$ with $\circ$ (composition) forms a group called the symmetric group.
      - $\forall \alpha, \beta, \gamma \in Sym(X)$ permutations $\alpha \circ (\beta \circ \gamma) = (\alpha \circ \beta) \circ \gamma$ (Associativity)
      - $i: X \to X$ where $i(x) = x$ $\forall x \in X$. (Identity) $\alpha \circ i = Sym(X)$
      - $\alpha \in Sym(X)$ : $\exists \alpha^{-1}$ since $\alpha$ is a bijection (Inverse)
    - Abelian/Commutative Group: A group where $\forall g, h \in G$, $g*h = h*g$. The operation is usually written with $+$ instead of $*$ and the inverse of $-g$ is written as $-g$.
    - Examples:
      - $(\mathbb{R}, +)$ is a group where $0 \in \mathbb{R}$ and $\forall x \in \mathbb{R}$, $-x \in \mathbb{R}$ is its inverse. (Additive group over $\mathbb{R}$)
      - $(\mathbb{R}\setminus\{0\}, \times)$ is a group where $1 \in \mathbb{R}$ and $\forall x \in \mathbb{R}$, $x^{-1} \in \mathbb{R}$ is its inverse. (Multiplicative group over $\mathbb{R}$)
      - For any field $F$ and $n \in \mathbb{N}$, $(F^n, +)$ is a group.
      - For $V$ a vector space (over $F$), $(V, +)$ is a group.
      - General Linear Group: $GL(n, F)$ is the set $G$ of $n\times n$ invertible matrices over $F$ and operation matrix multiplication. ($GL(n, F)$ is the multiplicative group $F^n$)
        - $A, B \in G$, since $\det(AB) = \det A \cdot \det B \neq 0$ (Closure)
        - $A, B, C \in G \Rightarrow A(BC) = (AB)C$ (Associativity)
        - $I_n \in G$ (Identity)
        - $A^{-1} \in G$ (Inverse)
    - Homomorphisms: Suppose $(G, \cdot)$ and $(H, \cdot)$ are groups. $\phi: G \to H$, is a homomorphism if $\forall g_1, g_2 \in G$, $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$.
      - $\hookrightarrow$ if $\phi = \{\phi(g), g \in G\}$,
      - $\ker \phi = \{g \in G : \phi(g) = e_H\}$
      - If $\phi$ is a bijection the $\phi$ is an isomorphism. $G$ and $H$ are isomorphic if $\exists$ an isomorphism $\phi$ $G \to H$. ($G \cong H$)
      - Fund Isomorphism Theorem: If $\phi: G \to H$ is a group homomorphism, then $\Im \phi(G) \cong G/\ker(\phi)$
      - E.g.
        - Let $G = GL(n, F)$. Then $\det: G \to (F^*, \cdot)$ is a homomorphism, $\det g_1 g_2 = \det g_1 \det g_2$.
        - Suppose $(G, \cdot)$ is any group and $b \in H$. Define $\phi: (\mathbb{Z}, +) \to H$, $\phi(n) = b^n \in H$. Then $\phi$ is a homomorphism, $\phi(m+n) = b^{m+n} = b^m b^n = \phi(m)\phi(n)$.
        - $\exp: (\mathbb{R}, +) \to (\mathbb{R}^*, \cdot)$. Then $\exp$ is a homomorphism since $\exp(x+y) = e^{x+y} = \exp(x)\exp(y)$.
        - $|\cdot|: (\mathbb{C}^*, \cdot) \to (\mathbb{R}^*, \cdot)$ is a homomorphism as $|z_1 z_2| = |z_1||z_2|$.
      - Suppose $G, H$ are groups and $\phi: G \to H$ is a homomorphism. Then:
        1) $\phi(e_G) = e_H$
        2) $\phi(g^{-1}) = \phi(g)^{-1}$ $\forall g \in G$
        3) $\ker \phi = \{g \in G : \phi(g) = e_H\}$ is a subgroup of $G$.
        - Proof:
          1) $\phi(e_G) = \phi(e_G) \cdot \phi(e_G)$ $\Rightarrow \phi(e_G) = e_H$
          2) $e_H = \phi(e_G) = \phi(g)\phi(g^{-1})$ $\Rightarrow \phi(g^{-1}) = (\phi(g))^{-1}$
          3)
      - Suppose $G, H, K$ are groups.
        1) A homomorphism $\phi: G \to H$ is injective iff $\ker \phi = \{e_G\}$
        ii) If $\phi: G \to H$ and $\psi: H \to K$ are homomorphisms, then $\psi \circ \phi: G \to K$ is a homomorphism.
        iii) If $\phi: G \to H$ is an isomorphism, then $\phi^{-1}: H \to G$ is an isomorphism. ($G \cong H \Leftrightarrow H \cong G$)
        - Proof:
          1) (a) Supp $\phi: G \to H$ is injective. For homomorphism properties, $\phi(e_G) = e_H$. By injectivity, it follows $\ker \phi = \{e_G\}$. ($\Leftarrow$) Supp $\ker \phi = \{e_G\}$ and $\phi(g) = \phi(h)$. $\phi(g) \cdot \phi(h^{-1}) = e_H \Rightarrow \phi(g \cdot h^{-1}) = e_H$ $\Rightarrow g \cdot h^{-1} = e_G$ (ground component) $\square$
          2) Supp $\psi$ and $\phi$ are homomorphisms. Let $g, h \in G$. $\psi \circ \phi(g, h) = \psi(\phi(g, h))$ $= \psi(\phi(g)\phi(h))$ $= \psi(\phi(g))\psi(\phi(h))$ $\square$
          3) Supp $\phi$ is an isomorphism. Let $\phi^{-1}$ be its inverse. By surjectivity of $\phi$, $\phi^{-1}$ is surjective. Consider $\phi^{-1}(h_1) = \phi^{-1}(h_2)$. Then $g = h_1$ by injectivity of $\phi$. Thus $\phi^{-1}$ is an isomorphism.
      - Suppose $G$ and $H$ are cyclic groups of the same order. Then there is an isomorphism of $G \to H$.
        - Proof: Suppose $G, H$ finite, cyclic order $n$. Let $G = \langle a \rangle$ and $H = \langle b \rangle$. Define $\phi: G \to H$ by $\phi(a^k) = b^k$ for $k \in \mathbb{Z}$.
          - (Well defined) If $a^k = a^l$, $a^{k-l} = e_G$, so $n \mid (k-l)$ $\Rightarrow b^{k-l} = e_H$ $\Rightarrow b^k = b^l$.
          - (Injective) Suppose $b^k = b^l$. Then $b^{k-l} = e_H$ $\Rightarrow \phi(a^{k-l}) = \phi(e_G)$ $\Rightarrow a^{k-l} = e_G$ $\Rightarrow a^k = a^l$.
          - (Surjective) By definition.
          - (Homomorphism) $\phi(a^k a^l)$ $= \phi(a^{k+l})$ $= b^{k+l}$ $= b^k b^l$ $= \phi(a^k)\phi(a^l)$
          - Suppose $G, H$ infinite order. Then we get well-definedness from $a^k = a^l \Rightarrow a^{k-l} = e_G$ $\Rightarrow k = l$.
      - Suppose $V, V_2$ are non-cyclic groups of order 4. Then $V_1 \cong V_2$ (isomorphic)
        - Proof: Let $V_1 = \{e, a, b, c\}$. No element of order 4 in $V_1$ $\Rightarrow$ have order 2. Since order of $a, b, c$ must divide 4 by Lagrange.
          - Suppose $ab = e \Rightarrow b = c$ (cancel)
          - $ab = b \Rightarrow a = e$ (cancel)
          - $ab = a \Rightarrow b = e$ (cancel)
          - $ab = b \Rightarrow c$.
          - Similarly, $bc = a$ & $ca = b$.
          - So for $V_1$:

            | | e | a | b | c |
            |---|---|---|---|---|
            | e | e | a | b | c |
            | a | a | e | c | b |
            | b | b | c | e | a |
            | c | c | b | a | e |

          - Similarly we can show the same for $V_2$. Thus $e \to e$, $b \to b^2$, $a \to a^2$, $c \to a^3$. Is thus an isomorphism.
    - $\forall \sigma, \rho \in S_n$ and $\forall \rho$ disjoint with $\sigma$: $\sigma\rho = \rho\sigma$
      - $\hookrightarrow f(\rho(i)) = \sigma(f(i))$
      - $\rho(\sigma(i)) = (\rho \circ f)(i)$
      - Proof:
    - Let $\Delta = \prod_{1 \leq i < j \leq n} (x_i - x_j)$ then $\sigma(\Delta) = \Delta$ or $-\Delta$
      - Proof:
    - Signum/Sign: Suppose $f$ is a permutation. $\text{sgn}: S_n \to \{-1, 1\}$ gives the sign or signum of $f$. $\text{sgn}(f) = 1$ if $f(\Delta) = \Delta$ and $\text{sgn}(f) = -1$ if $f(\Delta) = -\Delta$. (permutation is even) } it is even } if is odd
      - Suppose $n \geq 2$ and $f, g \in S_n$
        1) $\text{sgn}(fg) = \text{sgn}(f)\text{sgn}(g)$
        2) If $f$ is a 2-cycle, $\text{sgn}(f) = -1$
        iii) If $g$ is an $r$-cycle, $\text{sgn}(g) = (-1)^{r-1}$
        - Proof:
          1) $(gf)(\Delta) = g(f(\Delta)) = g(\text{sgn}(f)\Delta)$ $= \text{sgn}(f)\text{sgn}(g)\Delta$; $(gf)(\Delta) = \text{sgn}(gf)\Delta$; $\therefore \text{sgn}(gf) = \text{sgn}(f)\text{sgn}(g)$
          ii) If $f = (i\ j)$, $f(\Delta) = -1$ since $(x_i - x_j)$ changes sign. Let $h \in S_n$, $h(i) = 1$, $h(j) = 2$. Then $h^{-1}(1)h = (j)$ so $\text{sgn}(h)\text{sgn}(h^{-1})\text{sgn}(h)\text{sgn}(h) = \text{sgn}(h) = -1$ $\square$
          iii) $r$-cycle $g$ we know that $g$ is product of $r-1$ 2-cycles. Thus $\text{sgn}(g) = (-1)^{r-1}$
    - Alternating group: The set of even permutation in $S_n$, a subgroup. It is the kernel of sign.
      - $\hookrightarrow$ If $n \geq 2$, then the index of $A_n$ in $S_n$ is 2. The then counts on the set of $A_n$ and odd permutations.
      - Proof:
    - $\forall A = (a_{ij}) \in M_n(\mathbb{F})$, $\det(A) = \sum_{f \in S_n} \text{sgn}(f) a_{1f(1)} \cdots a_{nf(n)}$
      - Proof: Let $\det'(A) = \sum_{f \in S_n} \text{sgn}(f) a_{1f(1)} \cdots a_{nf(n)}$
        - $\Rightarrow \det'(A) = \sum_{f \in S_n} \text{sgn}(f) a_{1f(1)} \cdots a_{nf(n)} + \sum_{f \in A_n} \text{sgn}(f a_{1f(1)} \cdots a_{nf(n)}$, where $S = S_n \setminus A_n \cup A_n$
        - $\Rightarrow \det'(A) = \sum_{f \in A_n} a_{1f(1)} \cdots a_{nf(n)} - \sum_{f \in A_n} a_{1f(1)} a_{2f(2)} \cdots a_{nf(n)}$
          - If $B$ is $A$ but with one row multiplied, $\det(B) = c\det(A)$ (Obviously follows from formula)
          - If $A, B, C$ are the same except the $i$th row where $c_i = a_i + b_i$, then $\det(C) = \det(A) + \det(B)$ (Exercise)
          - If $A$ has consecutive identical rows then $\det(A) = 0$ ($a_{1f(1)} = a_{2f(1)}$ and $a_{1f(2)} = a_{2f(2)}$ ... $\det(A) = 0$)
        - $\det(T_{ij}) = -1$ ($\det(T_{23}) = -1 = -0 = 1$)
        - Thus it satisfies the determinant properties.
    - Let $f, g \in S_n$ and $\alpha \in \{x\} = \{1, \dots, n\}$.
      - $f$ fixes $\alpha$ if $f(\alpha) = \alpha$
      - $f$ moves $\alpha$ if $f(\alpha) \neq \alpha$
      - The support of $f$ is $\{g \in \{x\} : f(g) \neq g\}$. (supp(f))
      - $f, g$ have disjoint supports if $\text{supp}(f) \cap \text{supp}(g) = \emptyset$
      - If $f, g$ have disjoint supports, then:
        1) $fg = gf$
        ii) $\forall \alpha \in \mathbb{Z}$, $(fg)^\alpha = f^\alpha g^\alpha$
        - Proof:
      - If $f = (i_1, \dots, i_r) \in S_n$, then $f^i$ is the $r$-cycle $f^{-i} = (i_r, \dots, i_1)$.
        - Proof:
      - Let $\alpha \in \mathbb{Z}$ and $r \in \mathbb{N}$. Suppose $i_1, \dots, i_r \in \{x\}$ are distinct. If $f \in S_n$ fixes the other elements of $\{x\}$ and $f(i_1) = i_2, \dots, f(i_{r-1}) = i_r$, then $f$ is an $r$-cycle and $f$ is written as $(i_1, \dots, i_r)$
        - E.g.
          - $(1, 2, 3, 4) \in S_4$ : $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$
          - The identity permutation (A 1-cycle)
    - Disjoint Cycle form: The cycle decomp of a permutation $f \in S_n$ is the sequence of cycle lengths in descending order, including repetitions and fixed points, (an partition is disjoint cycle form.
      - E.g. $(1\ 2\ 3\ 4\ 5)(6)(7)(8) \in S_8$ has cycle shape 5, 2, 1.
      - Suppose $g \in S_n$ is written in disjoint cycle form as $g = g_1 g_2 \cdots g_k$, $g_i$ an $r_i$-cycle. $\Sigma r_i = n$ (Ex. from)
        1) $g^{-1} = g_k^{-1} \cdots g_1^{-1}$
        2) $g^{r_i} = e$ and $g^{-r_i} = e$, $\forall i \in \{i, \dots, k\}$
        3) The order of $g$ is $\text{lcm}(r_1, \dots, r_k)$ of the lengths of the disjoint cycles in $g$.
        4) $g^{-1} = g_1^{-1} \cdots g_k^{-1}$
        - Proof:
          1) A generalization of $(i_1 \cdots i_r)^{-1} = i_r \cdots i_1$
          ii) ($\Rightarrow$) Suppose $g^{r_i} = e$. Then $g_i^{r_i} = e$. Since these are disjoint cycles, we have $g_i^{r_i} = e$ $\forall i$. ($\Leftarrow$) Suppose $g_i^{r_i} = e$ $\forall i$. Then $g^{r_1} = g_1^{r_1} \cdots g_k^{r_k} = e$
          iii) Suppose $g^{r_i} = e$ $\forall i$. Each $g_i$ has order $r_i$. Then $g_i^{r_i} = e$ $\Leftrightarrow r_i \mid n$. Thus $\exists$ smallest $n \in \mathbb{N}$ with $g^n = e$. $n = \text{lcm}(r_1, \dots, r_k)$
          iv) $g^{-1} = g_1^{-1} \cdots g_k^{-1}$. Since $\text{supp}(g_i) \cap \text{supp}(g_j) = \emptyset$ $g_i^{-1} \cdots g_k^{-1}$ has disjoint supports, hence the composition commutes $g_1^{-1} g_2^{-1} \cdots g_k^{-1}$
    - Suppose $(G, \cdot)$ is a group and $H \leq G$.
      1) If $g_1, g_2 \in G$ and $g_1 \in gH$, then $g_2 H = gH$
      2) If $g \in G$ and $gH \cap kH \neq \emptyset$, then $gH = kH$ (Cosets doesn't intersect unless equal)
      - Proof:
        1) Supp $g_1 \in g_2 H$. $\exists h \in H$, $g_1 = g_2 h$. $\forall g \in gH$, $g = g_2 h_1 \in g_2 H$, $gH \subseteq g_2 H$. $\forall g \in g_2 H$, $g = g_1 h_2 \in gH$, $g_2 H \subseteq gH$. $\therefore g_2 H = gH$ and $g_1 H = gH$ $\square$
        2) Let $x \in g_1 H \cap kH$ $\Rightarrow gH$ and $kH$ intersect by 1) $\Rightarrow gH = kH$
    - Suppose $(G, \cdot)$ is a group and $H \leq G$. Define $\sim$ by $g \sim h \Leftrightarrow g^{-1}h \in H$.
      1) $\sim$ is an equivalence relation
      2) $g \sim h \Leftrightarrow gH = hH$
      - Proof:
        1)
        2) $g \sim h \Leftrightarrow g^{-1}h \in H \Leftrightarrow g^{-1}hH = H \Leftrightarrow gH = hH$ $\square$
    - Let $G$ be a finite group of order $n$. Let $g \in G$. Then
      1) The order of $g$ divides $n$
      2) $g^n = e$
      - Proof:
        1) $k$ = order of $g = |\langle g \rangle|$. Since $\langle g \rangle \leq G$, $k \mid n$ by Lagrange.
        2) $\text{ord}(g) \mid n$. Since $k \mid n$, we have $g^{-(g)^k} = e^{-n} = e$.
    - Left Cosets: Suppose $(G, \cdot)$ is a group and $H \leq G$. Let $g \in G$. The subset $gH = \{gh : h \in H\} \subseteq G$ is the left coset of $H$ in $G$. (The order of $H$ is equal to the number of left cosets of $H$ in $G$.)
      - Right Coset: $Hg = \{hg : h \in H\} \subseteq G$.
      - E.g.
        - $G = (\mathbb{C}^*, \cdot)$, $H = \{z \in \mathbb{C}^* : |z| = 1\}$. Then $\forall w = |w| e^{i\theta} \in \mathbb{C}^*$, $wH = \{|w| e^{i\theta} : \theta \in \mathbb{R}\}$.
        - $G = (\mathbb{R}, +)$, $H = \{n : n \in \mathbb{Z}\}$. $\forall x \in \mathbb{R}$, $x + H = \{x + n : n \in \mathbb{Z}\}$.
        - $G = GL_n(\mathbb{R})$, $H = SL_n(\mathbb{R})$. Then $\det: G \to \mathbb{R}^*$ is surjective. Consider $\det^{-1}(\{a\}) = \{A \in GL_n(\mathbb{R}) : \det A = a\}$. Let $B \in \det^{-1}(\{a\})$. Then $\det^{-1}(\{a\}) = BH$.
        - $G = S_3$, $H = \langle (1\ 2) \rangle$. $(1\ 2\ 3)H = \{(1\ 2\ 3), (1\ 3)\}$.
      - Let $H \leq G$ and $r \in G$. Suppose $i_1, \dots, i_r \in \{x\}$ are distinct. If $f \in S_n$ fixes the other elements of $\{x\}$ and $f(i_1) = i_2, \dots, f(i_{r-1}) = i_r$, then $f$ is an $r$-cycle and $f$ is written as $(i_1, \dots, i_r)$
      - E.g.
        - $(1, 2, 3, 4) \in S_4$ : $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$
        - The identity permutation (A 1-cycle)
    - Suppose $G$ is a finite group with order $n$. Let $g \in G$. Then
      1) The order of $g$ divides $n$
      2) $g^n = e$
      - Proof:
        1) $k$ = order of $g = |\langle g \rangle|$. Since $\langle g \rangle \leq G$, $k \mid n$ by Lagrange.
        2) $\text{ord}(g) \mid n$. Since $k \mid n$, we have $g^{-(g)^k} = e^{-n} = e$.
    - Fermat's Little Theorem: Suppose $p$ is any prime. If $a \in \mathbb{Z}$ and $p \nmid a$, then $a^{p-1} \equiv 1 \bmod p$. $\Rightarrow a^p \equiv a \bmod p$.
      - Proof: Let $F_p = \mathbb{Z}_p$. Consider $(\mathbb{Z}_p^*, \cdot)$. Then $|\mathbb{Z}_p^*| = p-1 = |\{a, \dots, (p-1)a\}|$. So $\forall g \in \mathbb{Z}_p$, $g^{p-1} = (1)_p$ (by group properties). Then $\bar{a} = \{\bar{a}, \bar{2a}, \dots, \overline{(p-1)a}\}$. Let $g = \overline{(a)_p}$, $a = \overline{(1)_p} = \overline{(a^2)_p} = \overline{(a^3)_p} = \dots = \overline{(a^{p-1})_p} = 1 \bmod p$.
      - Suppose $(G, \cdot)$ is a group and $H \leq G$.
        1) If $g_1, g_2 \in G$ and $g_1 \in gH$, then $g_2 H = gH$
        2) If $g \in G$ and $gH \cap kH \neq \emptyset$, then $gH = kH$ (Cosets doesn't intersect unless equal)
        - Proof:
          1) Supp $g_1 \in g_2 H$. $\exists h \in H$, $g_1 = g_2 h$. $\forall g \in gH$, $g = g_1 h_1 \in g_2 H$, $gH \subseteq g_2 H$. $\forall g \in g_2 H$, $g = g_1 h_2 \in gH$, $g_2 H \subseteq gH$. $\therefore g_2 H = gH$ and $g_1 H = gH$ $\square$
          2) Let $x \in g_1 H \cap kH$ $\Rightarrow gH$ and $kH$ intersect by 1) $\Rightarrow gH = kH$
    - Suppose $(G, \cdot)$ is a group and $H \leq G$. Define $\sim$ by $g \sim h \Leftrightarrow g^{-1}h \in H$.
      1) $\sim$ is an equivalence relation
      2) $g \sim h \Leftrightarrow gH = hH$
      - Proof:
        1)
        2) $g \sim h \Leftrightarrow g^{-1}h \in H \Leftrightarrow g^{-1}hH = H \Leftrightarrow gH = hH$ $\square$
    - Suppose $(G, \cdot)$ is a group and $H \leq G$. Define $\sim$ by $g \sim h \Leftrightarrow g^{-1}h \in H$.
      1) $\sim$ is an equivalence relation
      2) $g \sim h \Leftrightarrow gH = hH$
      - Proof:
        1)
        2) $g \sim h \Leftrightarrow g^{-1}h \in H \Leftrightarrow g^{-1}hH = H \Leftrightarrow gH = hH$ $\square$
    - Let $f, g \in S_n$ and $\alpha \in \{x\} = \{1, \dots, n\}$.
      - $f$ fixes $\alpha$ if $f(\alpha) = \alpha$
      - $f$ moves $\alpha$ if $f(\alpha) \neq \alpha$
      - The support of $f$ is $\{g \in \{x\} : f(g) \neq g\}$. (supp(f))
      - $f, g$ have disjoint supports if $\text{supp}(f) \cap \text{supp}(g) = \emptyset$
      - If $f, g$ have disjoint supports, then:
        1) $fg = gf$
        ii) $\forall \alpha \in \mathbb{Z}$, $(fg)^\alpha = f^\alpha g^\alpha$
        - Proof:
      - If $f = (i_1, \dots, i_r) \in S_n$, then $f^i$ is the $r$-cycle $f^{-i} = (i_r, \dots, i_1)$.
        - Proof:
      - Let $\alpha \in \mathbb{Z}$ and $r \in \mathbb{N}$. Suppose $i_1, \dots, i_r \in \{x\}$ are distinct. If $f \in S_n$ fixes the other elements of $\{x\}$ and $f(i_1) = i_2, \dots, f(i_{r-1}) = i_r$, then $f$ is an $r$-cycle and $f$ is written as $(i_1, \dots, i_r)$
      - E.g.
        - $(1, 2, 3, 4) \in S_4$ : $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$
        - The identity permutation (A 1-cycle)
    - Suppose $\sigma \in S_n$ is written in disjoint cycle form as $\sigma = g_1 g_2 \cdots g_k$, $g_i$ an $r_i$-cycle. $\Sigma r_i = n$ (Ex. from)
      1) $\sigma^{-1} = g_1^{-1} \cdots g_k^{-1}$
      2) $\sigma^{r_i} = e$ and $\sigma^{-r_i} = e$, $\forall i \in \{i, \dots, k\}$
      3) The order of $\sigma$ is $\text{lcm}(r_1, \dots, r_k)$ of the lengths of the disjoint cycles in $\sigma$.
      4) $\sigma^{-1} = g_1^{-1} \cdots g_k^{-1}$
      - Pro