$\gcd(a,b)=d \Leftrightarrow \exists r,s\in\mathbb{Z}$ w/ $ar+bs=d$ $\quad a|b \Leftrightarrow \exists c\in\mathbb{Z}\ b=ca$

$a\equiv b \pmod n \Leftrightarrow n|a-b \Leftrightarrow \exists c: (a-b)=cn \Leftrightarrow a=nq+b,\ q\in\mathbb{Z}$

$\mathrm{lcm}(l_1,\dots l_n)$ odd $\Rightarrow$ each l_i odd.

$\mathrm{lcm}(m,n)=mn \Leftrightarrow \gcd(m,n)=1$

Group - Satisfy axioms 1) $\forall g,h,k\in G: g(hk)=(gh)k$ $\quad$ 2) $\exists e\in G\ \forall g\in G: eg=ge=g$
3) $\forall g\in G\ \exists g^{-1}\in G: gg^{-1}=g^{-1}g=e$

*e, g^{-1} unique (but left-inverse or right inverse need not be unique). * $\forall a,b,c\in G: ab=ac\Rightarrow b=c,\ ba=ca\Rightarrow b=c$.

* $\forall a,b\in G\ (aba^{-1})^n=ab^na^{-1},\ (g_1g_2\cdots g_n)^{-1}=g_n^{-1}g_{n-1}^{-1}\cdots g_1^{-1},\ g^mg^n=g^{m+n},\ (g^m)^n=g^{mn},\ (gh)^n=(h^{-1}g^{-1})^{-n}$

Abelian Group - Satisfy axioms 1)-3) and 4) $\forall x,y\in G,\ xy=yx$.

* $\forall a\in G\ a^2=e\Rightarrow G$ abelian, $x^{-1}y^{-1}=xy\Rightarrow G$ abelian. Abelian $\Rightarrow gH=Hg\ \forall g$ $\quad H,K\subset G\Rightarrow H\cap K\subset H,\ H\cap K\subset K$.

Subgroup - $H\subseteq G \Leftrightarrow$ 1) $H\neq\emptyset$, 2) $\forall g,h\in H,\ gh^{-1}\in H \Leftrightarrow$ 1) $e\in H$ 2) $\forall h_1,h_2\in H,\ h_1h_2\in H$ 3) $\forall h\in H,\ h^{-1}\in H$.

* $H_1,H_2\subseteq G\Rightarrow H_1\cap H_2\subseteq G$. $\langle a\rangle\subset G$, and is the smallest subgroup containing a. Normal if $\forall g\in G,\ gH=Hg$. $gH=Hg\Leftrightarrow gHg^{-1}\subseteq H \Leftrightarrow gHg^{-1}=H$
subset
$\hookrightarrow G$ commutative $\Rightarrow$ any subgroup is Normal $\hookrightarrow \{ghg^{-1}|h\in H\}$

Cyclic group = $\exists a\in G: \langle a\rangle=G$, [$a^0=e$ by convention], Homomorphisms can be defined only on generator

*Every cyclic group is abelian. *Let G cyclic group, $|G|=n$ and $\langle a\rangle=G$, $b=a^k\Rightarrow |b|=\frac{n}{\gcd(k,n)}$

* G cyclic, $|n|$, $\langle a\rangle=G$, then $a^k=e\Leftrightarrow n|k$. * Every $H\subseteq G$ is cyclic if G cyclic.

* $a,b\in G,\ |a|=m,\ |b|=n,\ \gcd(m,n)=1\Rightarrow\langle a\rangle\cap\langle b\rangle=\{e\}$, $\langle a^m\rangle\cap\langle a^n\rangle$ generated by $a^{\mathrm{lcm}(m,n)}$. $G=\bigcup_{a\in G}\langle a\rangle$

Cycle of length k - $(a_1\dots a_k)$ *disjoint cycles commute. $(a_1\dots a_k)^{-1}=(a_ka_{k-1}\cdots a_1)=(a_1a_{k-1}\dots a_k)$

Permutation group - S_X= set of permutations (self bijections of X) * S_n is a group, $|S_n|=n!$ operation is function composition.

* $(x,\pi(x),\dots\pi^{k-1}(x))$ cycle of length k, where $\pi^k(x)=x$. * $\sigma\tau(x)=\sigma(\tau(x))$ apply τ then σ! * X finite $\Rightarrow\sigma\in S_X$ can be written as product of disjoint cycles. order of a k cycle is k, $|a|=k\Rightarrow a^{-1}=a^{k-1}$, length of $a=k$

$(a_1\cdots a_k)^k=(1)$. Every k cycle can be written as a product of transpositions. $(a_1\cdots a_k)=(a_1a_k)(a_1a_{k-1})\cdots(a_1a_2)$

If $\sigma\in S_n$ can be written as a product of an even/odd # of transpositions, then any way of writing σ as such a product has even/odd # of transpositions. So σ even/odd. (1) even, (12) odd, ...

order of $\sigma_1\cdots\sigma_m=\mathrm{lcm}($length of $\sigma_1\dots\sigma_n)$. $\Leftarrow$ must be disjoint

Left Cosets: Let $g\in G,\ H\subset G,\ gH=\{gh:h\in H\}$ - $gH\not\subset G$ if $g\in G\setminus H$ - $gH=H$ if $g\in H$, G is partitioned (disjoint union) of distinct cosets of H. # left cosets = # right cosets.

$K\subset G,\ \varphi:G\to H$ homomorphism, then $\varphi(K)\subset\varphi(G)\subset H$

Lagranges Thm: If G finite, $H\subset G$, $|G|=|H|\cdot[G:H]$, $|H|\,|\,|G|$, $|H|=|gH|$. G finite, $a\in G\Rightarrow |a|\,|\,|G|$, $a^{|G|}=e$, $|G|=p$, prime $\Rightarrow$ G cyclic. $K\subset H\subset G\Rightarrow[G:K]=[G:H][H:K]$, $[G:H]=2\Rightarrow gH=Hg$ (H normal). $H,K\subset G$, $gH\cap gK$ coset of $H\cap K$.

$H\subset G,\ g_1,g_2\in G\quad g_1H=g_2H\Leftrightarrow Hg_1^{-1}=Hg_2^{-1}\Leftrightarrow g_1H\subseteq g_2H\Leftrightarrow g_2\in g_1H\Leftrightarrow g_1^{-1}g_2\in H$

$\phi:\mathbb{N}\to\mathbb{N},\ \phi(0)=1,\ \phi(1)=1,\ \phi(n)=\#\ 1\leq m<n$ s.t. $\gcd(m,n)=1$, $n>1$. $\to\phi(mn)=\phi(m)\phi(n)$ m,n rel. prime. $\phi(p^k)=p^k-p^{k-1}$, p=prime, $k>0$

1st Isomorphism thm:
$\psi:G\to H$ group homomorphism
$\varphi:G\to G/Ker(\psi)$
$\exists\eta:G/Ker(\psi)\to\psi(G)$
s.t. $\psi=\eta\circ\varphi$
$G/Ker(\psi)\cong\psi(G)$

$$\begin{tikzcd} G \arrow[rr, "\psi"] \arrow[dr, "\varphi"'] & & H \\ & G/Ker(\psi) \arrow[ur, "\eta"'] & \end{tikzcd}$$

Eulers thm - $a,n\in\mathbb{N}$, $\gcd(a,n)=1$. $a^{\phi(n)}\equiv1\pmod n$ $\quad$ Fermats little thm - $a\in\mathbb{N}$, p prime. $a^p\equiv a\pmod p$. If $p|a$, $a\equiv0\pmod p$. If $p\nmid a$, $a^{p-1}\equiv1\pmod p$. $\quad\varphi(x)=e_H\Leftrightarrow x=e_G$. $\quad G\cong H,\ K\cong H\Rightarrow G\cong K$, $G\cong G',\ K\cong K'\Rightarrow G\times K\cong G'\times K'$, $G\cong G\times\{e\}$

Isomorphism - $(G,\cdot)\cong(H,\circ)$ if $\exists\varphi:G\to H$ s.t. $\varphi(g\cdot h)=\varphi(g)\circ\varphi(h)\ \forall g,h\in G$. $G\cong H\Rightarrow|G|=|H|$, G commutative/cyclic/subgroup of size $n\Rightarrow$ H does too. $|\varphi(g)|\,|\,|g|$ All infinite cyclic groups $\cong\mathbb{Z}$. G cyclic w/ $|G|=n\cong\mathbb{Z}_n$, $|G|=p$ prime $\Rightarrow G\cong\mathbb{Z}_p$. $\varphi:G\to G\Rightarrow\varphi$ automorphism.

Direct Products - $\prod_{i=1}^n G_i=\{(g_1,g_2,\dots,g_n)|g_i\in G_i\}$ and $(g_1,\dots,g_n)\circ(h_1,\dots,h_n)=(g_1h_1,\dots,g_nh_n)$. If $g_i\in G_i$, $|g_i|=r_i$, $|(g_1,\dots,g_n)|=\mathrm{lcm}(r_1,\dots,r_n)$. $A\times B$ abelian $\Leftrightarrow A,B$ abelian. $H_1\subseteq A,\ H_2\subseteq B\Rightarrow H_1\times H_2\subset A\times B$. $|\prod_{i=1}^nG_i|=\prod_{i=1}^n|G_i|$

Internal Direct Products - H,K IDP G if (1) $G=HK=\{hk|h\in H,k\in K\}$ (2) $H\cap K=\{e\}$ (3) $\forall h\in H,k\in K,\ hk=kh$.

G IDP of $H,K\Rightarrow G\cong H\times K$. $\quad\varphi(e_G)=e_H,\ \varphi(g^{-1})=(\varphi(g))^{-1}$, $K\subset G$, $\varphi(K)\subset\varphi(G)$, $\varphi(K)\subset H$ $\quad Ker\,\varphi=\{g\in G:\varphi(g)=e_H\}$ - is a normal subgroup of G.
*Homomorphisms only need to be defined on generators satisfying relations

Homomorphism - G,H groups $\varphi:G\to H$ $\forall g_1,g_2\in G$ $\varphi(g_1g_2)=\varphi(g_1)\varphi(g_2)$ φ bijective $\Rightarrow\varphi$ isomorphism. $\varphi(G)=\{h\in H|\exists y\in G:\varphi(y)=h\}$
$\hookrightarrow$ homomorphic image of φ.

<u>Groups</u>

$D_3 = \{id, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\}$ – Not abelian, not cyclic, all subgroups cyclic
$0°$ $120°$ $240°$ fixA fixB fixC

$D_4 = \{id, \rho_1, \rho_2, \rho_3, \mu_1, \mu_2, \mu_3, \mu_4\}$ – Not abelian, not cyclic, cyclic subgroups
$0°$ $90°$ $180°$ $270°$ fixA fixB fixC fixD

$(\mathbb{Z}, +)$ – cyclic, infinite order, $-1, 1$ generators, abelian, infinitely large subgroups. $\mathbb{Z} \cong n\mathbb{Z}$

$(\mathbb{Q}^*, \cdot), (\mathbb{R}^*, \cdot), (\mathbb{C}^*, \cdot)$ – Noncyclic, commutative groups

$(\mathbb{Z}_n, +)$, generators are $r \in \mathbb{Z}$ s.t. $1 \leq r < n$ and $\gcd(r,n) = 1$ $\quad \mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn} \Leftrightarrow \gcd(m,n) = 1 \Rightarrow U(mn) \cong U(m) \times U(n)$

$U(n) = \{b \in \mathbb{Z}_n : b \text{ has inverse mod } n\}$, ie $\gcd(b,n) = 1 \Leftrightarrow b \in U(n) \Leftrightarrow \exists r \in \mathbb{Z}^*$ s.t. $b \cdot r \equiv 1 \bmod n \Leftrightarrow \exists r, s \in \mathbb{Z}^*$ st. $br + ns = 1$

$\mathbb{M}_n(\mathbb{R})$ = $n \times n$ matrices w/ real entries and addition operation. Abelian.

$GL_n(\mathbb{R}) = \{A \in \mathbb{M}_n(\mathbb{R}) \mid A^{-1} \text{ exists}\}$ – $\det(A) \neq 0$, group under matrix multiplication. Non abelian.

$SL_n(\mathbb{R}) = \{A \in \mathbb{M}_n(\mathbb{R}) \mid \det(A) = 1\}$

$H_n = \{z \in \mathbb{C}^* \mid z^n = 1\}$ $(n \geq 1)$ – nth roots of unity. $\mathbb{T} = \{z \mid |z| = 1\}$ – $H_n \subset \mathbb{T} \subset \mathbb{C}^*$

$H_1 = \{1\}$, $H_2 = \{1, -1\}$, $H_4 = \{1, -1, i, -i\}$ ...

$Z(G) = \{g \in G \mid gh = hg \ \forall h \in G\}$ – <u>Centre</u> of G, $Z(G) = G$ when G abelian, $Z(G)$ normal subgroup of G.
$G/Z(G)$ cyclic $\Rightarrow G$ abelian, and $\Rightarrow G/Z(G) = \{e\}$ and cannot be nontrivial cyclic group!!!

$n\mathbb{Z} = \{nk : k \in \mathbb{Z}\} \subset \mathbb{Z}$ – cyclic, infinite,

$S_n = \{\pi : X \to X \mid \pi \text{ 1:1 and onto}, |X| = n\}$, $A_n = \{\sigma \in S_n \mid \sigma \text{ even}\} \subset S_n$, $D_n = \{\sigma \mid \sigma = r^i s^j$, $r, s \in S_n$ and $r^n = id$, $s^2 = id$, $srs = r^{-1}\}$

$\to A_n \subset S_n$, $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$, $D_n \subset S_n$, $|D_n| = 2n$, $Z(D_n) = \begin{cases} \{id\}, & n \text{ odd.} \\ \{id, r^{n/2}\}, & n \text{ even.} \end{cases}$ Non abelian group $|G| = 2p$ (p prime) $\Rightarrow G \cong D_p$

$sr^k s = r^{-k}$. $\quad D_{2n} \cong \mathbb{Z}_2 \times D_n$ (for n odd). $|G| = 2p$, (p odd prime) either $G \cong \mathbb{Z}_{2p}$ or $G \cong D_p$, $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$

G/H = set of cosets of G w.r.t. H, a normal subgroup of G. $|G/H| = [G:H]$; G abelian $\Rightarrow G/H$ abelian, G cyclic $\Rightarrow G/H$ cyclic,

G exactly one subgroup H s.t. $|H| = k \Rightarrow H$ normal in G. $\quad |gH| \mid |g|$.

$C(g) = \{x \in G : xg = gx\} \subset G$. $\langle g \rangle$ normal $\Rightarrow C(g)$ normal – <u>Centralizer</u> of g.

<u>Fundamental Thm of Finite Commutative Groups</u>: Every finite commutative group $\cong \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}$ $\alpha_j \geq 1$, p_i – primes, not necessarily distinct.

$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, # diff'l non-isomorphic abelian groups of order n is product of #s of diff'l unordered representations of α_j as a sum.

$H \cong H'$, $K \cong K' \Rightarrow H \times K \cong H' \times K'$