4/21

look at notes for problems that will be for sure.

$G = \{e, y_2, \ldots, y_m\}$ $\quad \underline{n \mid m}$ Lagrange's Theor

~~H≤G~~ $H = \{e, x_2, \ldots, x_n\}$

$\underline{H \leq G}$

choose $z_1 \in G \setminus H$

$z_1 H = \{z_1, z_1 x_2, z_1 x_3, \ldots, z_1 x_n\}$ $\quad z_2 \in G \setminus (H \cup z_1 H)$

$z_2 H = \{ \quad \}$

$\underline{\mathbb{Z}, \mathbb{Z}_n \quad +}$ $\qquad \underline{U(n), \cdot, 1}$

$U(21) = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$

$\phi(21) = (7^1 - 7^0)(3^1 - 3^0)$ $\quad 3 \cdot 7$

$= 6 \cdot 2$

12

$\langle 4 \rangle = \{4, 16, 1\}$

$2\langle 4 \rangle = \{8, 11, 2\}$

$5\langle 4 \rangle = \{20, 17, 5\}$

$10\langle 4 \rangle = \{19, 13, 10\}$

6380

H

gH

$a+$

② $SL_2(\mathbb{Z}_3)$ $\quad |GL_2(\mathbb{Z}_p)|\ (p^2-1)(p^2-p)$

$$|GL_2(\mathbb{Z}_3)| = (3^2-1)(3^2-3) = 8 \cdot 6. = 48.$$

$\det : GL_2(\mathbb{Z}_3) \longrightarrow \cancel{\{1,2\}}\ \{1,2\}$ $\quad |SL_2(\mathbb{Z}_3)| = \frac{48}{2} = 24.$

$$\left\langle \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right.$$

$$o\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = 3$$

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$\left[SL_2(\mathbb{Z}_3) : \left\langle \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \right\rangle \right] = \frac{24}{3} = 8$$

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Question is $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \in SL_2(\mathbb{Z}_3)$ $\quad \det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad-bc$

yes

One coset $\quad \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \left\langle \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \right\rangle = \Big\{$ $\quad \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = 2 \cdot I_2$

$$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 0 & 2 \end{pmatrix}$$

Scalar matrices are $\cancel{Z(GL_n(\mathbb{F}))}$ $Z(M_n(\mathbb{F}))$

③

$\mathbb{Z}_{12}$

Extra Cr.

$\langle 3 \rangle = \{3, 6, 9, 0\}$

operation:

$2 + \langle 3 \rangle = \{5, 8, 11, 2\}$

$1 + \langle 3 \rangle = \{4, 7, 10, 1\}$

$S_3 = \{e, (12), (13), (23), (123), (132)\}$ $|S_n| = n!$

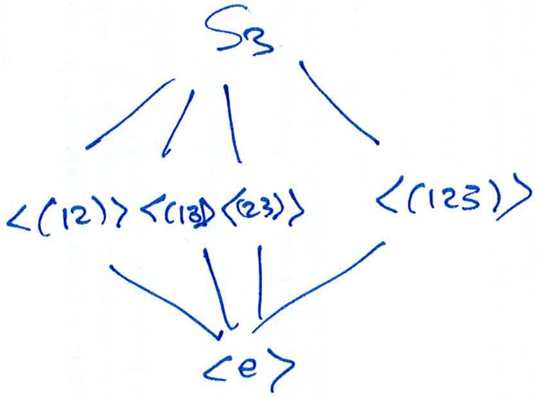
$|A_n| =$

S_5 (2, 2,2

3, 2,3 → 6

120

deco	$o(\sigma)$
2	2
2,2	2
2,3	6
3	3
4	4
5	5



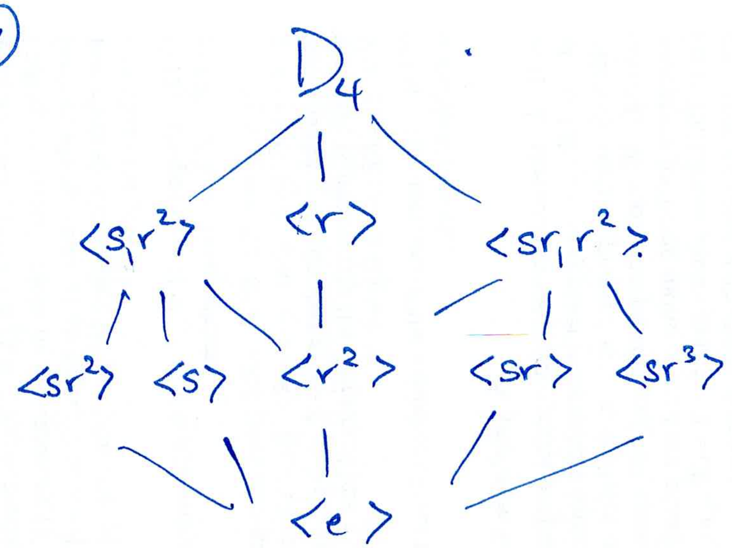
(123)

$(13)(12)$

(1234)

$(14)(13)(12)$

(4)



D_n

r rotation by $\frac{360°}{n}$

Q_8

$D_n = \langle r, s \mid \underline{r^n = s^2 = 1, \ rs = sr^{-1}}$

D_5

$\cancel{(sr^2)(sr^2)}$

$\cancel{\langle s, r^2 \rangle = \{e, s, r^2}$

$\langle x, y \rangle = \{e, x, x^2, x^3, \ldots x$
$y, y^2, y \ldots$

xy　xyx
yx

$G = \langle x, y \mid x^6 = y^2 = 1, \ xy = yx^5 \rangle$

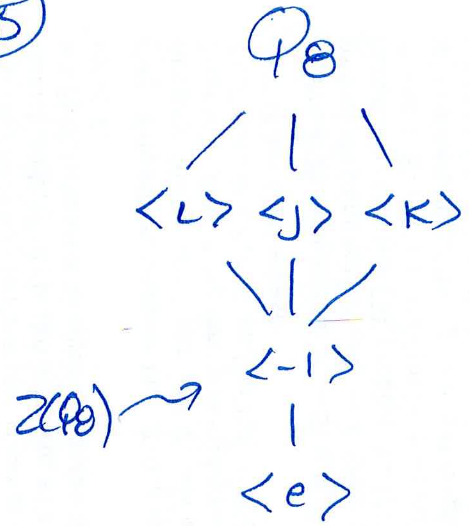
$x^3 \in Z(G)$

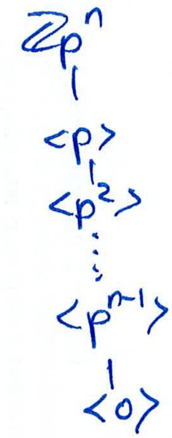
$o(x^3) = 2$

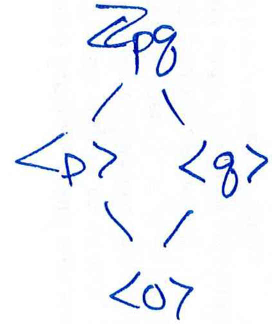
$x^3 y = y x^3$

$\langle x^3, y \rangle = \{e, x^3, y, x^3 y\}$

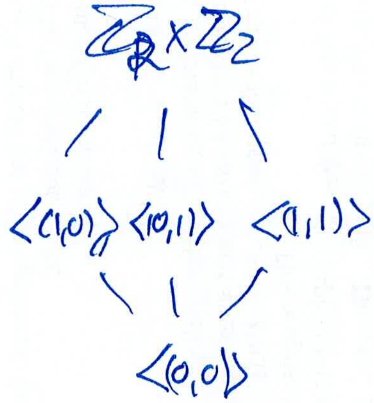
(5)

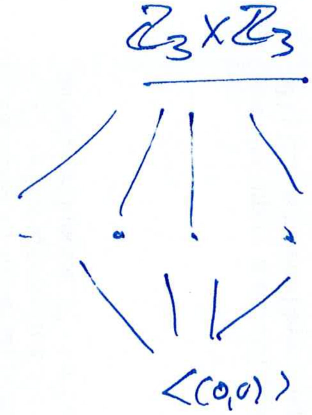






$$|A \times B| = |A| \cdot |B|$$





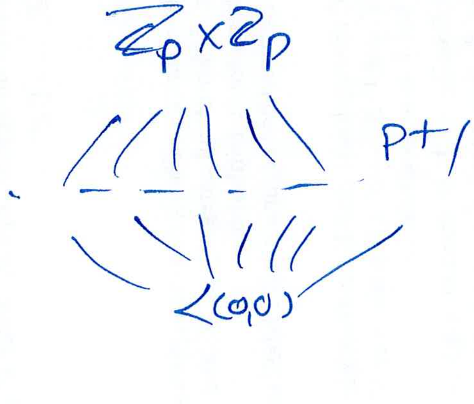
$\langle (1,0) \rangle$

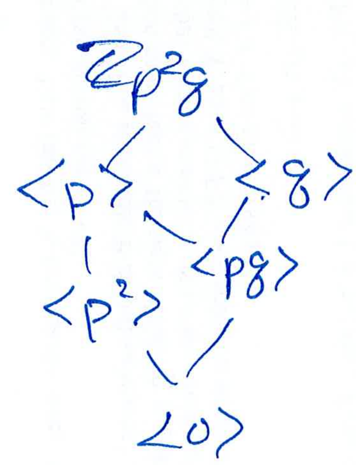
$\langle (0,1) \rangle$

$\langle (1,1) \rangle$

$\langle (1,2) \rangle$

$\langle (0,0) \rangle$





$G/Z(G)$ cyclic $\Rightarrow$ G is abelian

6 $H, K \leq G$

K normalizes H. : $\forall k \in K \quad kHk^{-1} = H$.

$HK = \{hk \mid h \in H, k \in K\}$ don't switch order.

<u>Claim</u> $HK \leq G$.

$h_1 k_1 h_2 k_2 = h_3 k_3$

(10) Let $\sigma \in \mathrm{Aut}(\mathbb{Z}_7)$ be the automorphism induced by $\sigma(1) = 4$. Find $o(\sigma)$.
(11) When is the operation on cosets well-defined? So $g_1H * g_2H = (g_1g_2)H$?
(12) Find a set representatives of the distinct cosets of a given H. For example, consider $G = D_4$ and $H =< r^2 >$. Then $[G : H] = 4$. Find representatives of the 4 distinct left cosets of H.
(13) Suppose $G =< x, y | x^n = y^m = e$ and $xy = yx^k >$
  (a) Prove by induction that $x^j y = yx^{jk}$.
  (b) Write $xy^2 = y^2x^j$ for appropriate j.
  (c) Compute $< xy >$ and find the order of xy.
(14) Draw the lattice of subgroups of S_3.
(15) Draw the lattice of subgroups of D_4.
(16) Draw the lattice of subgroups of Q_8.
(17) Draw the lattice of subgroups of $\mathbb{Z}_p$.
(18) Draw the lattice of subgroups of $\mathbb{Z}_{pq}$.
(19) Draw the lattice of subgroups of $\mathbb{Z}_{p^2q}$.
(20) Draw the lattice of subgroups of $\mathbb{Z}_p \times \mathbb{Z}_p$.

Proofs

(1) Prove using induction.

— Prove something is a subgp.

(2) State and prove Lagrange's Theorem.
(3) Prove that every cyclic group is abelian.
(4) Prove that every subgroup of a cyclic group is cyclic.
(5) Let G be an abelian group. Prove that the elements of finite order form a subgroup of G.
(6) Let H be a subgroup of G and $g \in G$. Prove that gHg^{-1} is a subgroup of G.
(7) Prove that $Z(G)$ or $C_G(g)$ is a subgroup of G.
(8) Prove that addition and multiplication on Z_n is well-defined.
(9) Prove that the set of cosets of a subgroup form a partition of G.
(10) Prove the following. Let G be a cyclic group of order n and suppose that a is a generator for G. Then $a^k = e$ if and only if n divides k.
(11) Let $(G, *, e)$ be a group. Prove that the identity is unique.
(12) Let $(G, *, e)$ be a group. Prove that the inverse of an element is unique.
(13) Prove that $| < g > | = o(g)$.
(14) Prove that the intersection of subgroups is a subgroup.
(15) For a subgroup $H \leq G$ and $g \in G$, prove that $|gH| = |H|$.
(16) Prove that for every $n \in \mathbb{Z}$, $(aba^{-1})^n = ab^na^{-1}$.
(17) Prove that $(g_1 \cdot \ldots \cdot g_n)^{-1} = g_n^{-1} \cdot \ldots \cdot g_1^{-1}$.
(18) Prove that $|H| = |gHg^{-1}|$.
(19) Prove that a given subgroup is normal, e.g. $\mathrm{Ker}\,\varphi$, $Z(G)$.
(20) Prove that $gHg^{-1} \leq G$.
(21) Given that $\phi : G \to H$ is a homomorphism, prove that $\phi(e_G) = e_H$.
(22) Given that $\phi : G \to H$ is a homomorphism, prove that $\phi(g^{-1}) = \phi(g)^{-1}$.
(23) Given that $\phi : G \to H$ is a homomorphism, prove that $\phi(G) \leq H$.
(24) Given that $\phi : G \to H$ is a homomorphism, prove that if G is abelian, then $\phi(G)$ is abelian.
(25) Given that $\phi : G \to H$ is a homomorphism, prove that if G is cyclic, then $\phi(G)$ is cyclic.
(26) Prove that if $G/Z(G)$ is cyclic, then G is abelian.
(27) Prove that $\varphi_g : H \to gHg^{-1}$ defined by $\varphi_g(h) = ghg^{-1}$ is an isomorphism.
(28) Prove that a given map is a homomorphism (resp. isomorphism or automorphism).
(29) Prove that a composition of homomorphisms is a homomorphism.
(30) Is the map $f : G/H \to K$ well-defined? For example $\varphi : \mathbb{Z}_7 \to \mathbb{Z}_{10}$ defined by $\varphi(x) = 2x$.