- G-set X.
  - $e\cdot x = x$
  - $(g_1 g_2)\cdot x = g_1\cdot(g_2\cdot x)$

  $G_x = \{g\in G : g\cdot x = x\}$.

- $C_G(x) = \{g\in G : gx = xg\}$. $N_G(H) = \{g\in G : gH = Hg\}$.

  $orb(x) = \{g\cdot x : g\in G\} \subseteq X$.

- $$|orb(x)| = \frac{|G|}{|G_x|} \Leftrightarrow |orb(x)|\,|G_x| = |G|.$$

<u>Thm 13.3</u>. Let G be a finite group of order p^n, where p is prime. Then $Z(G)$ contains more than one element. ($Z(G)$ contains at least p elements.)

<u>Pf</u>. Let $X = G$ with $g\cdot x = gxg^{-1}$.

$$G = orb(g_1) \cup \cdots \cup orb(g_k)$$

$$\Rightarrow \quad |G| = |orb(g_1)| + \cdots + |orb(g_k)|.$$

$g_k = e \Rightarrow |orb(e)| = 1$.

$$\Rightarrow \quad \underbrace{|G|}_{p^n} = \underbrace{|orb(g_1)|}_{p^m} + \cdots + |orb(g_{k-1})| + 1$$

orbit-stabiliser
$$\Rightarrow \quad p^n = p^{m_1} + p^{m_2} + \cdots + p^{m_{k-1}} + 1.$$

$$\Rightarrow \quad \exists\, h \in G, h \neq e \text{ s.t. } orb(h) = \{h\}. \Rightarrow \quad ghg^{-1} = h \Rightarrow h \in Z(G).$$

Thm 13.4 Let G be a group such that $G/Z(G)$ is a cyclic group. Then G is ablieian.

Pf. $G/Z(G)$ is a cyclic group, then there is $g \in G$, s.t.

$$G/Z(G) = \langle gZ(G) \rangle.$$

$$\boxed{(gZ(G))^n = g^n Z(G)}$$

$\forall\, g_1, g_2 \in G$, $\exists\, n_1, n_2 \in \mathbb{Z}$, s.t. $g_1 = g^{n_1} z_1$, $g_2 = g^{n_2} z_2$, $z_1, z_2 \in Z(G)$.

$z_1 \in Z(G)$

$$g_1 g_2 = g^{n_1} z_1 g^{n_2} z_2 = g^{n_1} g^{n_2} z_1 z_2 = g^{n_2} g^{n_1} z_2 z_1 = g^{n_2} z_2\, g^{n_1} z_1 = g_2 g_1.$$

$\Rightarrow$ G is abelian.

Thm 13.5 Any finite group G with $|G| = p^2$ elements, p is prime, $\boxed{\text{is abelian}}$.

Pf. $Z(G) \trianglelefteq G \quad \Rightarrow \quad |Z(G)| = 1, p, p^2$

Thm 13.3 $\Rightarrow$ $|Z(G)| > 1$.

$|Z(G)| = p^2 \Rightarrow Z(G) = G \Rightarrow G$ is abelian.

$|Z(G)| = p \Rightarrow |G/Z(G)| = p \Rightarrow G/Z(G)$ is cyclic.

Thm 13.6. $\Rightarrow$ G is abelian.

Lem 13.1. Let G and H be two subgroups of a finite group J. Then

$$|GH| = \frac{|G||H|}{|G \cap H|}$$

Pf. Note that $G \cap H \leq G$, consider left cosets

$g_1(G\cap H), g_2(G \cap H), \cdots, g_n(G\cap H)$, $g_i^{-1}g_j \notin G\cap H$ $\forall i \neq j$ $\wedge$ $g_1, \cdots, g_n \in G$.

$\forall gh \in GH$, $g \in G$, $h \in H$, $\exists g_i$, s.t. $g \in g_i(G\cap H)$.

$$gh = g_i g' h = g_i(g'h) \in g_i H$$

$\uparrow$ $G \cap H$

$\Rightarrow$ $GH = g_1 H \cup g_2 H \cup \cdots \cup g_n H$.

$g_i H = g_j H \Leftrightarrow g_i^{-1} g_j \in H \Rightarrow g_i^{-1} g_j \in G \cap H$. contradiction.

$\Rightarrow \quad g_i H \neq g_j H, \quad \forall\, i \neq j.$

$$\frac{|GH|}{|H|} = n := \frac{|G|}{|G \cap H|}. \qquad \boxed{V}.$$

Thm 13.6 A group of order p^2 is isomorphis to either $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$.

Pf. $|G| = p^2$. If $\exists\, g \in G$, $\text{order}(g) = p^2 \Rightarrow G \cong \mathbb{Z}_{p^2}$.

If $\text{order}(g) = p$, $\forall\, g \in G$, $g \neq e$.

let $g, h \in G$ be such elements such that $\langle g\rangle \cap \langle h\rangle = \{e\}$

$\langle g\rangle\langle h\rangle = \langle h\rangle\langle g\rangle$

$\langle g\rangle\langle h\rangle$ is a group.

$$|\langle g\rangle\langle h\rangle| = \frac{|\langle g\rangle|\,|\langle h\rangle|}{|\langle g\rangle \cap \langle h\rangle|} = |\langle g\rangle|\,|\langle h\rangle| = p^2.$$

$\Rightarrow \quad \langle g\rangle\langle h\rangle = G. \cong \mathbb{Z}_p \times \mathbb{Z}_p.$

$\Rightarrow \quad G \cong \mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$.

$|G| = 4, 9, 25, 49, \dots$

$\mathbb{Z}_4$ or $V_4 = \mathbb{Z}_2 \times \mathbb{Z}_2$

$\mathbb{Z}_9$ or $\mathbb{Z}_3 \times \mathbb{Z}_3$.

- $|G| \le 7$.

$\underline{1}$ $\{e\}$

$\underline{2}$ $\mathbb{Z}_2$.

$\underline{3}$ $\mathbb{Z}_3$

$\underline{4}$ $\mathbb{Z}_4$, V_4.

$\underline{5}$ $\mathbb{Z}_5$

$\underline{6}$ $\mathbb{Z}_6$, $S_3 \cong D_3$.

$\underline{7}$ $\mathbb{Z}_7$.

- $\boxed{8}$ $\mathbb{Z}_8$, D_4 ... 5

$\underline{9}$ $\mathbb{Z}_9$, $\mathbb{Z}_3 \times \mathbb{Z}_3$.

- $|G| = p$, p is prime, $G \cong \mathbb{Z}_p$.
- $|G| = \underline{p^2}$, p is prime, $G \cong \mathbb{Z}_{p^2}$, $\mathbb{Z}_p \times \mathbb{Z}_p$.

§14. The Sylow Theorems.

$|S_4| = 24$. $\quad |A_4| = 12$. $\quad 2\times 6$

$\sigma = (i_1 i_2)(j_1 j_2)\cdots(l_1 l_2) \leftarrow$ even

even

$a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (23)(14)$ ~~odd~~ even.

$a = (1234) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$

$= (14)(13)(12)$. $\Rightarrow$ odd.

Exercise

- A_4 does not have a subgroup of order 6.

$H \leq A_4$, $\quad |H| = 6$. $\quad H \cong \mathbb{Z}_6$ or S_3

A_4 $\quad$ 1 $\;\sigma(e)=1$. $\quad$ 3 $\;$ order 2 $\quad$ 8 $\;$ order 3

Def 14.1 Let p be a positive, prime integer. A p-group is a group in which every element has order a power of p. $\boxed{|G| = p^k}$

Exam 16.1 Any cyclic group of prime order is a p-group.

Exam 16.2 $|S_3| = 2\times 3$. $\langle a\rangle = \{e, a, a^2\}$ 3-subgroup.

$\{e, b\}$, $\{e, ab\}$, $\{e, a^2b\}$. 2-subgroup.

Def 16.2 Let G be a finite group with $|G| = mp^k$, $p\nmid m$. A subgroup of p^k is called Sylow p-subgroup.

Exam 16.3 $|G| = 60 = 2^2 \cdot 3 \cdot 5$

Sylow 2-subgroup (order 4).

Sylow 3-subgroup (order 3)

Sylow 5-subgroup (order 5)

Thm 16.1 (The Sylow theorem). Let G be a group of order mp^k $p\nmid m$, p is prime. Then

1. a Sylow p-subgroup (order p^k) exists.

II. for each prime p, the Sylow p-subgroups are conjugate to each other.

III. let n_p be the number of Sylow p-subgroups then

(i) $n_p \equiv 1 \pmod p$.

(ii) $n_p = \dfrac{|G|}{|N_G(P)|}$. $P \leq G$ Sylow p-subgroup.

(iii) $n_p \mid m$.

Lem 4.1. The number of ways to pick p^k elements from a set of mp^k elements, which is equal to $\binom{mp^k}{p^k}$, is m mod p, $p \nmid m$.

$$\frac{(mp^k)!}{p^k!(mp^k-p^k)!} = \binom{mp^k}{p^k} \equiv m \pmod p.$$

Pf. $\binom{mp^k}{p^k}$ is the coefficient of x^{p^k} in the binomial expasion of

$$(1+x)^{mp^k} = ((1+x)^{p^k})^m.$$

$$(1+x)^{p^k} = \sum_{j=0}^{p^k} \binom{p^k}{j} x^j = 1 + x^{p^k} + \sum_{j=1}^{p^k-1} \binom{p^k}{j} x^j \equiv 1 + x^{p^k} \pmod p$$

$$((1+x)^{p^k})^m \equiv (1+x^{p^k})^m \pmod p$$

$$(1+x^{p^k})^m = \sum_{j=0}^{m} \binom{m}{j} (x^{p^k})^j = 1 + m x^{p^k} + \cdots$$

$$(1+x)^{mp^k} \equiv (1 + m x^{p^k} + \cdots) \pmod p$$

$$\Rightarrow \binom{mp^k}{p^k} \equiv m \pmod p.$$

Pf of Sylow thm I. $|G| = mp^k$, $p \nmid m$.

Let S be the set of all subsets of G containing p^k elements.

Hence $|S| = \binom{mp^k}{p^k}$. Then Lemma 1 implies that $|S| \equiv m \pmod p$.

Now let S be G-set with the action $g \cdot S_i = gS_i$, $\forall S_i \in S$.

Then

$$S = \mathrm{orb}(\hat{S}_1) \cup \mathrm{orb}(\hat{S}_2) \cup \cdots \cup \mathrm{orb}(\hat{S}_r).$$

$$|S| = |\mathrm{orb}(\hat{S}_1)| + \cdots + |\mathrm{orb}(\hat{S}_r)|$$

Suppose that $|\mathrm{orb}(\hat{S}_1)| = l$, and $p \nmid l$.

$$|G_{\hat{S}_1}| \overset{\text{orbit-stabilizer}}{=} \frac{|G|}{|\mathrm{orb}(\hat{S}_1)|} = \frac{mp^k}{l} = tp^k, \quad t = \frac{m}{l} \in \mathbb{Z}.$$

Now consider $g \in G_{\hat{S}_1}$, $g \cdot \hat{S}_1 = \hat{S}_1$. Then

$$gs \in \hat{S}_1, \quad \forall s \in \hat{S}_1.$$

which implies $G_{\hat{S}_1} s \subset \hat{S}_1$.

$$|G_{\hat{S}_1}| = |G_{\hat{S}_1} s| \leq |\hat{S}_1| = p^k.$$

Then

$$|G_{\hat{S}_1}| = p^k.$$

Exam 6.6 S_3, $6 = 2 \times 3$. $\exists\, 1$ Sylow 2-subgroup (order 2).

$\exists\, 1$ Sylow 3-subgroup (order 3).

Exam 16.5 S_4. $24 = 2^3 \cdot 3$. $\exists$ 1 Sylow 2-subgroup (order 8)

$\exists$ 1 Sylow 3-subgroup (order 3).

Lem. If $H \le G$ is a p-subgroup, $P \le G$ is a Sylow p-subgroup. Then there exists $a \in G$, s.t. $H \subseteq aPa^{-1}$.

Pf. $X = \{xP : x \in G\}$ left cosets. H-set.

$h \cdot (xP) = hxP$. $|orb(xP)| = \dfrac{|H|}{|H_{xP}|}$ $\leftarrow p^l$

$|X| = |orb(x_1P)| + |orb(x_2P)| + \cdots + |orb(x_rP)|$.

$\boxed{|G| = mp^k,\ p \nmid m.}$

$|X| = m$. $\Rightarrow$ $p \nmid |X|$ $\Rightarrow$ $\exists\, x_i$, s.t. $|orb(x_iP)| = 1$.

$\forall\, h \in H$, $hx_iP = x_iP$. $\Rightarrow$ $hx_ig_1 = x_ig_2$. $\Rightarrow$ $h = x_ig_2g_1^{-1}x_i^{-1}$

$\in x_iPx_i^{-1}$

$\Rightarrow$ $H \subseteq x_iPx_i^{-1}$, take $a = x_i$.

Lem $\Rightarrow$ Sylow thm II.

Cor. If $P \le G$ is a Sylow p-subgroup, then

(i) $\forall g \in G$, gPg^{-1} is also a sylow p-subgroup.

(ii) $\boxed{P \text{ is the unique} \Leftrightarrow P \trianglelefteq G}$.

Pf. (ii) " $\Rightarrow$ " $\forall g \in G$, $gPg^{-1} = P$. $\Rightarrow$ $P \trianglelefteq G$.

" $\Leftarrow$ " $P \trianglelefteq G \Rightarrow gPg^{-1} = P$.

Pf of sylow thm III. Let X be the set of all sylow p-subgroup.

Let P $\leftarrow$ fixed. set with action $g \cdot Q = gQg^{-1}$, $\forall g \in P$, $Q \in X$.

$$|X| = \underbrace{|orb(Q_1)|}_{1} + |orb(Q_2)| + \cdots + |orb(Q_t)| .$$

$Q_1 = P$

$\forall g \in P$, $gPg^{-1} = P$. $\quad |orb(P)| = 1$.

$\forall g \in P$, $gQg^{-1} = Q$ $\Rightarrow$ $g \in N_G(Q) = \{g \in G : gQg^{-1} = Q\}$

$\Rightarrow$ $P \leq N_G(Q)$ $\qquad Q \trianglelefteq N_G(Q) \leq G$.

$p^k \qquad lp^k. > \qquad mp^k$.

$\Rightarrow$ $P = Q$

$\Rightarrow$ $n_p \equiv 1 \pmod p$.

(ii) G-set $\quad g \cdot P = gPg^{-1}$.

$$n_p = |orb(P)| = \frac{|G|}{\underbrace{|N_G(P)|}_{lp^k}} = \frac{mp^k}{lp^k} = \underline{\frac{m}{l}} \in \mathbb{Z}.$$

(iii) $\Rightarrow$ $n_p \mid m$.

<u>Exam 10.8</u>. $|G| = 15 = 3\times 5$. There are Sylow 3-subgroup and Sylow 5-subgroup. $n_3 \equiv 1 \pmod 3$. $n_3 = \underline{3k+1}$. $n_3 \mid 5$.

$\Rightarrow$ $n_3 = 1$. P is the unique Sylow 3-subgroup, $P \trianglelefteq G$.

$n_5 \equiv 1 \pmod 5$ $\quad n_5 = 5k+1 \mid 3$.

$\Rightarrow$ $n_5 = 1$, Q is the unique Sylow 5-subgroup, $Q \trianglelefteq G$.

$P \cap Q = \{e\}$. $\quad \underline{PQ = QP}$.

$$|PQ| = \frac{|P||Q|}{|P\cap Q|} = \frac{3\times 5}{1} = 15$$

$\Rightarrow$ $PQ = G \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}$.

Exam 10.9 $\quad |G| = 10 = 2\times 5$.

$n_2 = 2k+1 \mid 5$, $k=0,2$ $\quad n_2 = 1$ or $n_2 = 5$.

$n_5 = 5k+1 \mid 2$, $k=0$, $\quad n_5 = 1$.

Q is the unique Sylow 5-subgroup, $Q \trianglelefteq G$.

① $n_2 = 1$, P is the unique Sylow 2-subgroup, $P \trianglelefteq G$.

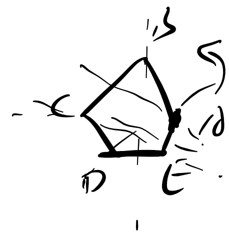
$G \cong \mathbb{Z}_{10}$.

② $n_2 = 5$ $\quad Q = \{e, a, a^2, a^3, a^4\}$.

$\forall\ b \in G$, $bQb^{-1} = Q$.

$P = \langle b \rangle$, $b^2 = e$.

$bab \in \{e, a, a^2, a^3, a^4\}$.



$bab = e, a, a^2, a^3, a^4$.

Exercise

$\Rightarrow$ $bab = a^4$. $\qquad S_3 = D_3$.

$G = \langle a, b \rangle$, $a^5 = e$, $b^2 = e$, $bab = a^4$ $\qquad G = D_5$

$G \cong \mathbb{Z}_{10}$ or D_5 $\qquad \boxed{D_n = \langle a, b \rangle,\ a^n = e,\ b^2 = e,\ bab = a^{n-1}}$