II.

§5. p-groups. Sylow subgroups. ~~Nilpotent~~

(A) Let p be a prime. A group whose order is a power of p is called a *p-group*.

p-groups have many special properties which do not belong to finite groups generally. A good many of these follow from

Lemma 5.1 Let the p-group G be represented by permutations of a set X and let Y be the set of all elements of X which are left invariant by G. Then $|X| \equiv |Y| \bmod p$.

For by 4.5, if X_i is one of the transitivity classes in this representation of G, then $|X_i|$ divides the order of G. Since $|G|$ is a power of p, either $|X_i| = 1$ or else $|X_i|$ is divisible by p. Hence $|X| = \Sigma |X_i| \equiv |Y| \bmod p$, since $|Y|$ is the number of classes X_i with a single element.

Theorem 5.2 Let G be a p-group.

(i) Let $K \lhd G$ and $K \neq 1$. Then $K \cap \mathfrak{z}G \neq 1$.

(ii) If $G \neq 1$, then $\mathfrak{z}G \neq 1$.

(iii) Every minimal normal subgroup of G has order p and lies in $\mathfrak{z}G$.

(iv) Let H be a proper subgroup of G. Then $H < N_G(H)$.

(v) Every subgroup of index p is normal in G.

(vi) Every maximal subgroup of G is of index p, hence normal.

(vii) Every chief factor of G has order p.

Proof: (i) Apply 5.1 to the representation t_K of G by automorphisms of K. ~~The set of elements of K so left invariant is a~~ $Y = K \cap \mathfrak{z}G$ is not empty since it contains 1. But $|X| = |K| = p^r$ with some $r > 0$ by 2.4, since $K \neq 1$. Hence $|Y|$ is at least p, by 5.1.

(ii) is the special case $K = G$ of (i).

(iii) if K is a minimal normal subgroup of G, then $K \neq 1$. Hence $K \cap \mathfrak{z}G \neq 1$. But every subgroup of $\mathfrak{z}G$ is normal in G. Hence $K \cap \mathfrak{z}G = K$ has order p by the minimality of K.

(iv) By 2·4, H is a p-group and $|G:H| = p^r$, with $r > 0$ since $H < G$. The representation τ_H of G is of degree p^r. Apply 5·1 to the restriction f of τ_H to H. Then X is the set of all cosets of H in G and among these is H itself, which is invariant under H since $HH = H$. Since $|X| = p^r$, it follows that $|Y|$ is at least p, for it is not zero. Hence $H\xi H = H\xi$ for some element ξ of G which is not in H. This implies that $\xi H \xi^{-1} \leq H$ and so $\xi^{-1} \in N_G(H)$. Since $\xi \notin H$, we thus find $H < N_G(H)$.

(v) and (vi) are immediate corollaries of (iv).

(vii) follows from (iii) since a chief factor H/K of G is a minimal normal subgroup of the p-group G/K.

A section L/M of any group G is called a <u>central factor</u> of G if $M \lhd G$ and $L/M \leq \mathfrak{z}(G/M)$. This implies that $L \lhd G$ and 5·2 (iii) shows that <u>in a p-group G</u>, <u>every chief factor is a central factor</u>.

A group G is called <u>nilpotent</u> if it has a series whose factors are all central factors of G. Hence <u>all p-groups are nilpotent</u>.

(B) Apropos the proof of 5·2 (iv), we note here

<u>Lemma 5·3</u> If H is any subgroup of a group G and $N = N_G(H)$, then the centralizer of $\tau_H(G)$ in $\Sigma(G)$ consists of all the ~~maps~~ mappings

$$l_H(\alpha) : \quad H\xi \rightarrow \alpha H \xi = H\alpha\xi \qquad (\xi \in G)$$

with $\alpha \in N$. It is isomorphic with N/H and its order $|N:H|$ is the number of invariants of H in the representation τ_H.

We have already noted that $H\xi H = H\xi$ if and only if $\xi \in N$ so that $|N:H|$ is the number of invariants of H in the representation τ_H. If $\alpha \in N$, then $\alpha H = H\alpha$ and $l_H(\alpha)$ is therefore a permutation of the set X of all cosets of H in G. If $\alpha \in H$, $l_H(\alpha)$ is the identity on X, but if $\alpha \notin H$ then $l_H(\alpha)$ maps H into $H\alpha \neq H$. Further, $l_H(\alpha\beta) = l_H(\beta)\, l_H(\alpha)$ so that $\alpha \rightarrow l_H(\alpha^{-1})$

$(\alpha \in N)$ is a representation of N with kernel H. Thus $l_H(N) \cong N/H$. It is clear that $l_H(\alpha)$ commutes with $r_H(\eta)$ for all $\alpha \in N$, $\eta \in G$. If τ belongs to the centralizer of $r_H(G)$ in $\Sigma(G)$ and if τ maps H into the coset H^*, then τ must map $H\xi$ into $H^*\xi$ for all $\xi \in G$. Hence $H^*\xi = H^*\eta\xi$ for all $\eta \in H$, so $H^* = H^*H$ and $H^* = H\alpha$ with $\alpha \in N$. Thus $\tau = l_H(\alpha)$ and 5·3 is proved.

(C) Let p be a prime and let G be a group of order $p^n m$ where $(m, p) = 1$. Any subgroup of G of order p^n is called a <u>Sylow p-subgroup</u> of G. Thus S is a Sylow p-subgroup of G if and only if S is a p-group and $|G:S|$ is prime to p. If p does not divide $|G|$, then $n = 0$ and the only Sylow p-subgroup of G is the unit subgroup.

The following theorem, due to L. Sylow 1832–1918, is fundamental

<u>Theorem 5.4</u> (i) Every group G has at least one Sylow p-subgroup.
(ii) The Sylow p-subgroups of G are all conjugate in G.
(iii) Every p-subgroup of G is contained in at least one Sylow p-subgroup
(iv) The number of Sylow p-subgroups of G is $\equiv 1 \bmod p$.

Proof: (i) due to Wielandt. Let X be a subset of G with $|X| = p^n$ and let $\xi \in G$. Then $|X\xi| = p^n$ by 1·6. Hence the regular representation of G induces a representation f of G:

$$f(\xi) : X \to X\xi \qquad (|X| = p^n)$$

on the $\binom{p^n m}{p^n}$ sets X. Since $(m, p) = 1$, the numbers $p^n m - r$ and $p^n - r$ are divisible by the same highest power of p for each value of $r = 0, 1, 2, \dots, p^n - 1$. So the degree of f is prime to p and f has at least one transitive component f_1 with degree m_1 prime to p. Let X_1 be any member of the corresponding transitivity class and let S be the stabilizer of X_1 in G. Then $|X_1| = p^n$ and $|G:S| = m_1$,
omitted and $X_1 S = X_1$. So X_1 is the union of certain inverse cosets of S and hence $|S| \leqslant |X_1| = p^n$. But $(m_1, p) = 1$ and $|G:S| = m_1$. Hence p^n divides $|S|$. Thus $|S| = p^n$ and S is a Sylow p-subgroup of G

(ii) and (iii). Let H be any subgroup of G. In the proof of 5·2 (iv) we used the restriction to H of the representation τ_H of G. We now need the restriction f of τ_H to a second subgroup K of G. The transitivity class of f which contains a given coset $H\xi$ consists of all cosets of H which are contained in $H\xi K$. The set $H\xi K$ is called a <u>double coset</u> of H, K; so two distinct double cosets of H, K in G have no common element. Let T be a transversal to the double cosets of H, K in G, i.e. let T contain exactly one element from each of these double cosets. Then $G = \bigcup_{\tau \in T} H\tau K$ and the terms $H\tau K$ are disjoint in pairs. Hence

$$|G : H| = \sum_{\tau \in T} |H\tau K : H|.$$

The numbers $|H\tau K : H|$ are the degrees of the transitive components of the representation f of K. Now $\tau\xi$ and $\tau\eta$ lie in the same coset of H if and only if $\tau\xi\eta^{-1}\tau^{-1} \in H$ i.e. $\xi\eta^{-1} \in H^{\tau}$. Taking ξ, η in K we obtain

<u>Lemma 5·5</u>. Let H and K be subgroups of G, let $\xi \in G$ and let T be a transversal to the double cosets of H, K in G. Then

$$|H\xi K : H| = |K : H^{\xi} \cap K|$$

and

$$|G : H| = \sum_{\tau \in T} |K : H^{\tau} \cap K|.$$

Now let $H = S$ be a Sylow p-subgroup of G and let K be any p-subgroup of G. Then $|G : S|$ is prime to p and so, by 5·5, $|K : S^{\tau} \cap K|$ is prime to p for some $\tau \in T$. Since K is a p-group, it follows that $|K : S^{\tau} \cap K| = 1$ and so $K \leq S^{\tau}$, which is a Sylow p-subgroup of G. This gives (iv). If K is actually a Sylow p-subgroup of G, then $|K| = |S^{\tau}|$ and so $K = S^{\tau}$ is conjugate to S in G. This gives (iii).

(iv) Here we take $H = N_G(S)$ and $K = S$ in ~~5.5~~ 5·5. By 4·5 Cor. 2, the number l of Sylow p-subgroups of G is equal to $|G : H|$, since they are all conjugate to S by (iii). If $S \not\leq H^{\tau}$, then $|S : H^{\tau} \cap S|$ is a positive power of p. If $S \leq H^{\tau}$, then

$S_1 = \tau S \tau^{-1} \leq H$ and S_1, S are Sylow p-subgroups of H. But $S \lhd H$ and so $S = S_1$ by (iii). Hence $\tau \in H$ and $H\tau S = HS$. Thus there is exactly one double coset of H, S viz. the product HS, for which $|S : H^\tau \cap S|$ is not divisible by p. For this exceptional one, $\tau \in H$ and $|S : H^\tau \cap S| = 1$. Thus $l \equiv 1 \mod p$ and Sylow's Theorem is completely proved.

(D) A few immediate consequences of Sylow's Theorem are worth recording as corollaries.

<u>Corollary 5·41</u> If p^r divides $|G|$, then G has subgroups of order p^r. For by 5·2 (vii), a Sylow p-subgroup S of G has subgroups of every order $1, p, p^2, \cdots, p^n = |S|$.

On the other hand, the tetrahedral group Σ_4^+ ~~[illegible]~~ of order 12 has no subgroups of order 6. (The symmetric and alternating groups $\Sigma(X)$ and $\Sigma^+(X)$ with $|X| = n$ will often be denoted by Σ_n, Σ_n^+ when it is not necessary to indicate the set X. This may be taken as the set of integers $1, 2, \cdots, n$).

Note that a subgroup H of index 2 in G is always normal:

$$|G : H| = 2 \quad \Rightarrow \quad H \lhd G.$$

For $\xi H = H\xi = H$ for all $\xi \in H$; while if $\xi \in G - H$ (in G but not in H), then again $\xi H = H\xi$ since each of these sets coincides with $G - H$.

<u>Corollary 5·42</u> Every normal p-subgroup M of G is contained in $K_G(S) = \bigcap_{\xi \in G} S^\xi$, where S is a Sylow p-subgroup of G. $K_G(S)$ is the unique maximal normal p-subgroup of G.

~~For by 5·4(iii), $K \leq S^\xi$ for some $\xi \in G$ and so $K \leq K^{\xi^{-1}\eta}$ $\leq S^\eta$ for all $\eta \in G$.~~

For by 5·4(iii), $M \leq S^\tau$ for some $\tau \in G$. Since $M \lhd G$, we then have $M = M^{\tau^{-1}\xi} \leq S^\xi$ for all $\xi \in G$. Hence $M \leq K_G(S)$.

<u>Corollary 5.43</u> If H and K are subgroups of G such that $N \leq H \leq K$, where N is the normalizer in G of the Sylow p-subgroup S of G, then $|K:H| \equiv 1 \bmod p$.

For S is a Sylow p-subgroup of both H and K; and $N = N_H(S) = N_K(S)$. Hence $|H:N|$ and $|K:N|$ are the numbers of Sylow p-subgroups of H and K, respectively, by 5.4 (ii). So $|H:N| \equiv |K:N| \equiv 1 \bmod p$ by 5.4 (iv). Consequently $|K:H| \equiv 1 \bmod p$ by 2.6.

More important is

<u>Lemma 5.6</u> Let $K \lhd G$ and let S be a Sylow p-subgroup of G. Then KS/K is a Sylow p-subgroup of G/K and $S \cap K$ is a Sylow p-subgroup of K.

Proof: By 5.5, $|KS:K| = |S:K \cap S|$ which is a power of p; while the index of KS/K in G/K is $|G:KS|$ by 3.5, and this divides $|G:S|$ by 2.6. Hence $|G:KS|$ is prime to p.

mitted [Again, $|S \cap K|$ is a power of p; while $|K : S \cap K| = |SK:S|$ by 5.5 and $|SK:S|$ is prime to p.

<u>Corollary</u>: If $|G:K|$ is prime to p, then $S \leq K$. If $|G:K|$ is a power of p, then $KS = G$.

Let ϖ be any set of primes. A <u>ϖ-number</u> is a number whose prime factors all lie in ϖ. Let ϖ' be the complementary set of primes. Every positive integer $n = n_\varpi n_{\varpi'}$, where n_ϖ is a ϖ-number and $n_{\varpi'}$ is a ϖ'-number uniquely determined by n. An <u>S_ϖ-subgroup</u> of a group G is any subgroup S of order $|G|_\varpi$ i.e. such that $|S|$ is a ϖ-number and $|G:S|$ is a ϖ'-number. When $\varpi = p$ is a single prime, we come back to the notion of a Sylow p-subgroup which is the same as an S_p-subgroup. G is called a <u>ϖ-group</u> whenever $|G|_\varpi = |G|$ or what is the same $|G|_{\varpi'} = 1$.

Remark: the symbol ϖ should not be confused with ω, the last letter of the Greek alphabet. In fact ϖ is a special form of π

often used by astronomers: it is not omega but pi in the sky.

Clearly the proof of 5.6 applies equally well with p replaced by an arbitrary set of primes. So we may state

<u>Lemma 5.7</u> Let $K \triangleleft G$ and let S be any S_ϖ-subgroup of G. Then KS/K is an S_ϖ-subgroup of G/K and $S \cap K$ is an S_ϖ-subgroup of K.

We also need

<u>Lemma 5.8</u> If G has a normal S_ϖ-subgroup K, then every ϖ-element and every ϖ-subgroup of G is contained in K.

For let H be a ϖ-subgroup of G. Since $K \triangleleft G$, KH is a subgroup of G. By 5.5, $|KH| = |K| \cdot |H : K \cap H|$. Here $|H : K \cap H|$ is a ϖ-number and $|K| = |G|_\varpi$. Hence $|H : K \cap H| = 1$ and $H \leq K$.

Consequences of Sylow's Theorem.

§6. Pronormal Subgroups. Nilpotent Groups

(A) Let H be a subgroup of G.

(i) We call H subnormal in G if and only if it belongs to some series of G i.e. if any only if there exist subgroups H_i such that

$$H = H_0 \lhd H_1 \lhd H_2 \lhd \cdots \lhd H_r = G. \qquad (1)$$

(ii) We call H pronormal in G if and only if H is conjugate to H^ξ in $\{H, H^\xi\}$ for all $\xi \in G$.

(iii) We call H disnormal in G if and only if $N_G(H) = H$.

(iv) We call H abnormal in G if and only if it is both pronormal and disnormal in G.

These relations will be denoted as follows:

$$H \text{ sbn } G, \quad H \text{ prn } G, \quad H \text{ dsn } G, \quad H \text{ abn } G$$

respectively.

Lemma 6.1 $H \lhd G$ if and only if H is both subnormal and pronormal in G.

Obviously $H \lhd G$ implies H sbn G and also H prn G, for $H = H^\xi = \{H, H^\xi\}$ for all $\xi \in G$. Suppose H sbn G but that H is not normal in G. We may assume that (1) holds and that H is not normal in H_2. Then $H \neq H^\xi$ for some $\xi \in H_2$. Then $H^\xi \leq H_1^\xi = H_1$ since $H_1 \lhd H_2$ and so $J = \{H, H^\xi\} \leq H_1$. But $H \lhd H_1$ so $H \lhd J$ and H cannot be conjugate to H^ξ in J. Hence H is not pronormal in G. Thus H sbn G and H prn G imply $H \lhd G$.

The only subgroup of G which is both subnormal and disnormal in G is G itself. So we may picture these five classes of subgroups diagrammatically as follows: