本节我们总假设 G 是有限群 ，

若 H 是 G 的子群 ，则根据拉格朗日定理可知 H 的阶是 G 的阶的因数 ，

现在的问题是拉格朗日定理的逆定理是否成立呢?

也就是说 ，若正整数 m 是群 G 的阶的因数 ，那么 G 是否有 m 阶子群?

本章定理 5.4 告诉我们 ，拉格朗日定理的逆定理对于有限循环群是成立的 ，

但是 ，对于交错群 A_5 来说 ，A_5 有 2 , 3 , 4 , 5 阶子群 ，没有 30 阶子群

(否则 ，30 阶子群的指数为 2，是正规子群 ，这与 A_5 是单群矛盾)，

本节的西罗定理将会指出: 当 m 为某个特殊值时 ，G 有 m 阶子群 ，

定义 8.1 令 p 是素数 ，r 是正整数 ，

若$|G|=p^r l$，且 p , l 互素 ，则称群 G 的 p^r 阶子群为 G 的西罗 p−子群 ，

例 8.1 求 S_3 的西罗 p−子群 ，

解: $|S_3|=6=2\times3$，则 S_3 的西罗 2−子群为{(1) , (12)} , {(1) , (13)} , {(1) , (23)}，

西罗 3−子群为{(1) , (123) , (132)}，

我们首先研究西罗 p−子群的存在性 ，

引理 8.1 设 G 是有限交换群 ，若素数 p 是|G|的因数 ，则 G 含有 p 阶子群 ，

证: 设$|G|=n$，对 n 用数学归纳法 ，当 n=2 时 ，结论成立 ，

假设结论对阶小于 n 的有限交换群成立 ，然后考察阶数为 n 的情形 ，

为此 ，我们任取属于 G 的 a , $a\neq e$，若 a 的阶为 k，则 $k>1$ 且 k|n，

(1)若 p|k，则由本章推论 5.2(1)可知 ，$b=a^{\frac{k}{p}}$的阶为 p，则 G 含有 p 阶子群$\langle b\rangle$，

结论成立 ，

(2)若 p∤k，由于 G 是交换群 ，故$\langle a\rangle$是 G 的正规子群 ，

若设商群 $G/\langle a\rangle$的阶为 m，则 n=mk，进而 ，$m<n$ 且 p|m，

从而由归纳假设 ，在群 $G/\langle a\rangle$中存在 p 阶元素$\overline{c}$ ，即 c^p 属于$\langle a\rangle$，

另外 ，$(c^k)^p=(c^p)^k=e$ 且 $c^k\neq e$(否则$\overline{c}^k=\overline{e}$ ，p|k，矛盾)，即 c^k 是 p 阶元素 ，

所以$\langle c^k\rangle$是 G 的 p 阶子群 ，

结论成立 ，

定理 8.1(西罗)设 G 是有限群 ，p 是素数 ，r 是正整数 ，

若$p^r \| |G|$且 P∤|G|，则 G 有西罗 p−子群(即 p^r 阶子群)，

证: 我们对群 G 的阶用数学归纳法 ，如果|G|=2，则定理结论平凡成立 ，

下面假设当群的阶数小于|G|时结论成立 ，然后考察阶数为|G|时的情形 ，

(1)如果 G 有真子群 N，满足 p∤|G: N|，

则由|G|=|N||G: N|可知 ，$p^r \| |N|$ ，$p^{r+1} \nmid |N|$，

再由 N 是 G 的真子群有|N|小于|G|，

于是 ，由归纳假设 ，N 有 p^r 阶子群 H，当然 H 也是 G 的 p^r 阶子群 ，

(2)如果对群 G 的每个真子群 N，都有 $p \| |G : N|$

则从群的类方程$|G| = |C(G)| + \sum_{a \in I - C(G)} |G : G_a|$ 可知 $p \| |C(G)|$

从而由引理 8.1 可知 ，C(G)中存在 p 阶子群 ，设其为 H，

若 G=H，|G|则|G|=p，定理结论平凡成立 ，

若 G≠H，则考虑商群 G/H，由$|G/H|=\frac{|G|}{|H|}$ ，可知$p^{r-1} \| |G/H|$，$p^r \nmid |G/H|$

若 r=1，则 H 为所求 ，

若 r>1，则由归纳假设可知 ，在 G/H 中存在 p^{r-1} 阶子群 K/H，

于是 ，子群 K 就是 G 的 p^r 阶子群(|K|=|H| • |K/H|=p^r)，

下面我们探讨西罗 p−子群的个数及两个西罗 p−子群之间的关系 ，

定理 8.2(西罗定理)设 G 是有限群 ，p 是素数 ，r 是正整数 ，

若$p^r \| |G|$且 $p^{r+1} \nmid |G|$，则

(1)若 G 的子群 H 是 p−群 ，则 H 含于 G 的某个西罗 p−子群(即 p^r 阶子群)中;

(2)群 G 的任意两个西罗 p−子群是共轭的;

(3)群 G 的西罗 p−子群的个数 $k \equiv 1 (\mathrm{mod}\ p)$ ，

证: 令 $S=\{N|N$ 是群 G 的 p^r 阶子群$\}$，

定义群 G 在集合 S 上的作用$\varphi: G \times S \to S$, $(g, N) \to gNg^{-1}$ ，

对属于 S 的任意 N，易知 N 的稳定子群为 $G_N=\{g \in G | gNg^{-1}=N\}$，

轨道为$\overline{N}=\{gNg^{-1}|g \in G\}$，显然 ，N 包含于 G_N ，

由本章的推论 3.2 和定理 7.1 可知$|G:N|=|G:G_N||G_N:N|=|\overline{N}||G_N:N|$ ，

因为 N 是 G 的西罗 p−子群 ，所以 $p \nmid |G:N|$，从而 $p \nmid |\overline{N}|$ ，

(1)令 H 是群 G 的阶为 p^m 的子群 ，

对属于 S 的任意 N，考虑群 H 在轨道$\overline{N}$上的作用:

$\psi: H \times \overline{N} \to \overline{N}$ ，　　$(h, gNg^{-1}) \to h(gNg^{-1})h^{-1}$ ，

根据定理 7.1 可知 ，

集合$\overline{N}$中元素 $x=gNg^{-1}$ 的轨道 Hx 所含元素的个数是$|H|=p^m$ 的因数 ，

而由轨道分解方程$|\overline{N}| = \sum_{x \in I} |Hx|$ 及 $p \nmid |\overline{N}|$可知

至少存在一个仅含一个元素的轨道 ，设其为 Hx，即 $Hx=\{x\}$，

由轨道的定义可知 ，

对属于 H 的任意 h，有 xh=hx，从而 Hx 是 G 的子群 ，$x=gNg^{-1}$ 是 Hx 的正规子群

再由群的第一同构定理 ，我们有 $Hx/x \cong H/(H \cap x)$ ，

由于 $H/(H \cap x)$的阶数是 p 的幂 ，于是 Hx/x 的阶数自然也是 p 的幂 ，

因为等于 gNg^{-1} 的 x 属于 S，所以 x 是 p^r 阶子群 ，从而 Hx 是 p^{-1} 阶子群 ，

即 x=Hx，

进而，$H=(H\cap x)$，H 包含于等于 gNg^{-1} 的 x 之中，

即 H 包含于 p^r 阶子群 x 之中，(1)的结论得证，

注意，因为 x 属于$\overline{N}$，所以根据(1)的证明过程可知:

对属于 S 的任意 N，存在有属于 G 的 a，使得 H 包含于 aNa^{-1}，

(2)令 H，N 是群 G 的任意两个 p^r 阶子群，则 H 当然也是一个 p−群，

所以由结论(1)，存在有属于 G 的 a，使得 H 包含于 aNa^{-1}，

而 H 本身就是 p^r 阶子群，所以 $H=aNa^{-1}$，即 H，N 是共轭的，

(3)设 N 是 G 的一个 p^r 阶子群，则由(2)可知，

$S=\{gNg^{-1}|g\in G\}$是 G 的所有 p^r 阶子群的集合，

映射ψ: $N\times S\to S$，$(n,gNg^{-1})\to n(gNg^{-1})n^{-1}$ 是群 N 在集合 S 上的作用，

轨道分解方程为$|S|=\sum_{x\in I}|\bar{s}|$

若将(1)中的 H 换为 N，则可知仅含一个元素的轨道只有{N}，

而由定理 7.1 得，$|\bar{s}|$是$|N|=p^r$的因数，所以$|S|\equiv 1(\mathrm{mod}\ p)$，

推论 8.1 设有限群 G 的阶为$|G|=p^rl$，其中 p 为素数，r 为正整数且 p，l 互素，则

(1)G 的西罗 p−子群的个数是 l 的因数;

(2)若 G 是交换群，则 G 有唯一一个西罗 p−子群，

证: (1)由定理 8.2(1)的证明过程可知，

G 的西罗 p−子群的个数是$|\overline{N}|$，而$|\overline{N}|$是|G|的因数，

再由定理 8.2 的(3)知$(|\overline{N}|,p)=1$，因此，$|\overline{N}|$是 l 的因数，

(2)若 G 是交换群，则 G 的所有的西罗 p−子群为 $S=\{gNg^{-1}=N|g\in G\}=\{N\}$，

结合推论 8.1、定理 8.1 及本章例 6.5 的结果，我们有如下推论:

推论 8.2 有限交换群可以唯一地表示为它的西罗 p−子群的直和，

利用西罗定理，我们可以判断某些群是否是循环群及是否是单群，

例 8.2 令 p，q 是互异的素数，G 是 pq 阶交换群，证明 $G\cong Z_{pq}$

证: 由定理 8.1 可知，群 G 中含有 p 阶和 q 阶子群

因为素数阶群是循环群，所以 G 中存在 p 阶元素和 q 阶元素，分别记为 a 和 b，

由 a 和 b 的阶互素及 ab=ba 可知，ab 的阶为 pq，所以 $G=\langle ab\rangle$是循环群，

从而由本章的推论 5.1 可知 $G\cong Z_{pq}$

例 8.3 证明 35 阶群 G 是循环群，

证: 因为 $35=5\times7$，所以 G 有 5 阶子群和 7 阶子群，

5 阶子群的个数整除 7，且模 5 同余 1，

因此 5 阶子群只有一个，从而是正规子群，

同理 7 阶子群也只有一个，且为正规子群，

因为素数阶群是循环群，所以可以设 5 阶子群为$\langle a\rangle$，7 阶子群为$\langle b\rangle$，

易知，$H\cap K=\{e\}$，从而 $aba^{-1}b^{-1}$ 属于$(H\cap K)$，即 ab=ba，

由本章的推论 5，2 可知，ab 的阶为 35，所以 $G=\langle ab\rangle$是循环群，

例 8.4 证明 56 阶群 G 不是单群，

证: 因为 $56=2^3\bullet7$，所以 G 有 8 阶子群和 7 阶子群，

7 阶子群的个数整除 8，且模 7 同余 1，因此 7 阶子群有 1 个或 8 个，

若 7 阶子群只有 1 个，则为正规子群，因此 G 不是单群，

若 7 阶子群有 8 个，则 8 阶子群只能有一个，

因而这个 8 阶子群是 G 的正规子群，从而 G 不是单群，