Chapter 9.3

9.3 The Sylow Theorems $\quad$ <u>G - a finite group</u> $\quad$ <u>p is a prime</u>

Th 9.13 - <u>First Sylow Theorem</u>

Let p be a prime, and assume that $p^k \mid |G|$ for some $k > 0$.

Then G has a subgroup of order p^k.

Cor 9.14 (Cauchy theorem)

If $p \mid |G|$, then G contains an element of order p.

p - a prime

Pf Any group of prime order is cyclic (Th 8.7), its generator has order p.

<u>Def</u> Let $|G| = p^n m$, $p \nmid m$.

A subgroup of order p^n is called a <u>Sylow p-subgroup</u>

For an element $x \in G$ consider the map

$$\begin{aligned} f: G &\longrightarrow G \\ g &\longmapsto x^{-1} g x \end{aligned} \quad \Big\} \text{ conjugation by } x$$

Prop f is an automorphism

inner automorphisms

Automorphism is an isomorphism from a group to itself

Pf f is a bijection because it has an inverse $g \mapsto xgx^{-1}$

f is a homomorphism:

$$f(g_1 g_2) = x^{-1} g_1 g_2 x = x^{-1} g_1 x x^{-1} g_2 x = \underline{f(g_1) f(g_2)}$$

If K is a subgroup of G

then its image under f is a subgroup (as the image of a subgroup under a homomorphism)

This image is $x^{-1}Kx = \{x^{-1}kx \mid k \in K\}$

The groups $K \simeq x^{-1}Kx$ are isomorphic because f is a homomorphism and f is a bijection between K and $x^{-1}Kx$

In particular if K is a Sylow p-subgroup, then so is $x^{-1}Kx$.

for different choices of x, we may get different subgroup $x^{-1}Kx$

Th 9.15 <u>Second Sylow Theorem</u>

If P and K are Sylow p-subgroups, then there exists $x \in G$ s.t.

$$P = x^{-1} K x$$

All Sylow p-subgroups are conjugated

In particular, all Sylow p-subgroups in G are isomorphic

Cor 9.16 Let K be a Sylow p-subgroup in G.

K is normal in G <u>iff</u> K is the only Sylow p-subgroup.

Th 8.11

A subgroup N s.t. $x^{-1} N x = N$ for every $x \in G$ is normal

Th 9.17 <u>Third Sylow Theorem</u>

The number of Sylow p-subgroups, n_p

- divides the order of the group: $\underline{n_p \mid |G|}$
- is of the form $1+pk$ with positive integer k: $\underline{n_p \equiv 1 \pmod{p}}$

Application

Cor 9.18 Let $|G| = pq$, both p and q are primes, $p > q$

Assume $q \nmid (p-1)$ $\quad p \not\equiv 1 \pmod q$

Then $G \simeq \mathbb{Z}_{pq}$ - cyclic of order pq

If $|G| = p^2$, then G may not be cyclic: $\mathbb{Z}_p \times \mathbb{Z}_p$ - is not cyclic while $\mathbb{Z}_{p^2}$ is

Pf Consider n_p Options: $1, \cancel{p}, \cancel{q}, \cancel{pq}$

$n_p \equiv 1 \pmod p$ $\quad q \neq 1 + pk$, $k \geq 0$ because $p > q$

Thus we have $n_p = 1$

Therefore the Sylow p-subgroup is normal, it's cyclic; call it H

$|H| = p$

$H \simeq \mathbb{Z}_p$

Consider n_q Options: $1, \cancel{p}, \cancel{q}, \cancel{pq}$

$n_q \equiv 1 \pmod q$ $\quad p \not\equiv 1 \pmod q$ by assumption

Thus we have $n_q = 1$ Therefore the Sylow q-subgroup is normal, it's cyclic, call it K

$|K| = q$

$K \simeq \mathbb{Z}_q$

H and K are normal subgroups

$H \cap K$ is a subgroup in both H and K;

Thus $|H \cap K| \mid |H| = p$ $\quad |H \cap K| \mid |K| = q$ $\quad$ implies $|H \cap K| = 1$

$H \cap K = \{e\}$

Claim $G = HK = \{hk \mid h \in H, k \in K\}$

$$H \times K \longrightarrow G$$
$$(h, k) \longmapsto hk$$

The amount of elements in $H \times K$ is $|H| \times |K| = pq = |G|$

Thus the injective map exhausts G and is therefore surjective.

This map is injective:

$$h_1 k_1 = h_2 k_2$$
$$h_2^{-1} h_1 k_1 = k_2$$
$$\underbrace{h_2^{-1} h_1}_{\in H} = \underbrace{k_2 k_1^{-1}}_{\in K}$$

This belongs to $H \cap K = \{e\}$

$$h_2^{-1} h_1 = e \qquad k_2 k_1^{-1} = e$$
$$h_1 = h_2 \qquad k_1 = k_2$$

$\left.\begin{array}{l} H \,\&\, K \text{ are normal} \\ H \cap K = \{e\} \\ G = HK \end{array}\right\}$ Th 9.3 implies that $G \simeq H \times K$

$$G \simeq H \times K \simeq \mathbb{Z}_p \times \mathbb{Z}_q \underbrace{\simeq}_{\text{Lemma 9.8}} \mathbb{Z}_{pq}$$

Remark on abelian groups

Let $|G| = p^n m$ $\quad p \nmid m$ $\qquad$ Ex 15 p 297 If $p^k \mid |G|$ then G has a subgroup of order p^k

$G \simeq G(p) \oplus \dots$ (Th 9.5)

$G(p)$ is a subgroup of G $\qquad \underline{|G(p)| = p^n}$ that is $G(p)$ is the Sylow p-subgroup

Exer 13 p297 - every abelian p-group has a p-power order.

$$G(p) \simeq \mathbb{Z}_{p^{k_1}} \oplus \mathbb{Z}_{p^{k_2}} \oplus \dots \oplus \mathbb{Z}_{p^{k_t}}$$

$$k_1 + k_2 + \dots k_t = n$$

Note that $p\mathbb{Z}_{p^k} = \{ px \mid x \in \mathbb{Z}_{p^k} \}$ is a cyclic subgroup in the cyclic group $\mathbb{Z}_{p^k}$ of order $\mathbb{Z}_{p^{k-1}}$

- solving ~~Exer~~ 15 p297