Lecture 19

Last time: $|G| = p^k \cdot n \quad (\gcd(n,p)=1)$

- First Sylow thm. $\rightsquigarrow \exists H \subset G,\ |H| = p^k$

- Second Sylow thm. $\rightsquigarrow$ if $H' \subset G$ Sylow
  then $H' = gHg^{-1}$ for some $g \in G$

- Third Sylow thm. $\rightsquigarrow$ if $s \leftarrow$ # Sylow p-subgroups

$\Downarrow$

$$s \mid n$$

$$s \equiv 1 \mod p$$

Classification of groups of order pq

Why Sylow thms are important?

Many reasons, one is that using them one can classify all groups of order pq ($p < q$ $\leftarrow$ prime numbers)

Thm. G $\leftarrow$ group, $|G| = pq$ then:

$$G \simeq \mathbb{Z}/p\mathbb{Z} \ltimes (\mathbb{Z}/q\mathbb{Z}) \text{ for}$$

some homomorphism $\varphi : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$

How to describe homomorphisms φ?

Claim: $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}, +) \cong \left((\mathbb{Z}/q\mathbb{Z})^\times, \cdot \right)$

$$\begin{array}{ccc} \psi & & \psi \\ (x \mapsto mx) & \longleftarrow\!\!| & m \end{array}$$

true in general, for q not nec. prime

For q prime, $(\mathbb{Z}/q\mathbb{Z})^\times = \{1, 2, \ldots, q-1\}$

So $\varphi \leftrightarrow$ element $m \in \mathbb{Z}/q\mathbb{Z}$

s.t. $m^p = 1$

<u>Example</u> $q = 5$, $p = 2$

$(\mathbb{Z}/5\mathbb{Z})^\times = \{1, 2, 3, 4\}$

$m = 1$ ✓

$m = 2$ ✗ $(2^2 = 4 \neq 1)$

$m = 3$ ✗ $(3^2 = 4 \neq 1)$

$m = 4$ ✓

$q=5,\ p=4 \Rightarrow m=1,2,3,4$ ✓

$$\mathbb{Z}/p\mathbb{Z} \ltimes_m (\mathbb{Z}/q\mathbb{Z}) \leftarrow \langle x, y \rangle \big/ \langle x^q = y^p = 1,\ yxy^{-1} = x^m \rangle$$

Note: $(\mathbb{Z}/5\mathbb{Z})^\times \leftarrow \{1, 2, \underset{4}{\underset{\|}{2^2}}, \underset{3}{\underset{\|}{2^3}}\}$

$\Downarrow$

$$(\mathbb{Z}/5\mathbb{Z})^\times \simeq \mathbb{Z}/4\mathbb{Z}$$

is a cyclic group

It's true in <u>general</u> that

$$(\mathbb{Z}/q\mathbb{Z})^\times \simeq \mathbb{Z}/(q-1)\mathbb{Z}$$

<u>So</u>: (1) if $p \nmid (q-1) \Rightarrow \varphi$ must be trivial $\Rightarrow G \simeq \underbrace{(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})}_{\text{is } \mathbb{Z}/pq\mathbb{Z}}$

(2) if $p \mid q \Rightarrow$ the subgroup of

$(\mathbb{Z}/q\mathbb{Z})^{\times} \simeq \mathbb{Z}/(q-1)\mathbb{Z}$ consisting of

m s.t. $m^p = 1$ is <u>isomorphic</u> to $\mathbb{Z}/p\mathbb{Z}$

(in $\mathbb{Z}/(q-1)\mathbb{Z}$ it is $\underbrace{0, \frac{q-1}{p}, \frac{2(q-1)}{p}, \ldots}_{\mathbb{Z}/p\mathbb{Z}}$)

So it's of the form: $\{1, a, a^2, \ldots, a^{p-1}\}$

for some a

We see that $m = a^k$ for some k.

If $k = 0 \Rightarrow G \simeq (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/q\mathbb{Z})$

If $k \neq 0$ then:

$$\mathbb{Z}/p\mathbb{Z} \ltimes_a (\mathbb{Z}/q\mathbb{Z}) \simeq \mathbb{Z}/p\mathbb{Z} \ltimes_{a^k} (\mathbb{Z}/q\mathbb{Z})$$

$$\langle x, y\rangle / \langle x^q = y^p = 1,\ yxy^{-1} = x^a\rangle \simeq \langle x, y\rangle / \langle x^q = y^p = 1,\ yxy^{-1} = x^{a^k}\rangle$$

$$x \mapsfrom x$$
$$y^k \mapsfrom y$$

if choose generators $\{x, y^k\}$ here then get

<u>So</u>:

<u>Thm</u> if $p \nmid (q-1) \Rightarrow G \simeq \mathbb{Z}/pq\mathbb{Z}$

if $p \mid (q-1) \Rightarrow \begin{cases} G \simeq \mathbb{Z}/pq\mathbb{Z} \\ G \simeq (\mathbb{Z}/p\mathbb{Z}) \ltimes (\mathbb{Z}/q\mathbb{Z}) \end{cases}$

all of them are <u>iso</u>

How to prove (idea)

$p < q$

(1) S ⟜ number of q-subgroups of G

$$\left.\begin{aligned} &S \equiv 1 \mod q \\ &S \mid p \quad (p<q) \end{aligned}\right\} \Rightarrow S = 1$$

Pick $H \subset G$ ⟜ Sylow q-subgroup

(2) $H \subset G$ ⟜ normal (use that $S = 1$)

$\Rightarrow gHg^{-1} = H$

(3) H ⟜ cyclic $(|H| = q)$

④ Pick any $K \subset G$ ← p-subgroup

cyclic

⑤ $K \xrightarrow{\varphi} \mathrm{Aut}(H)$ ← homomorphism

$$k \longmapsto (h \mapsto khk^{-1})$$

⑥ $K \simeq \mathbb{Z}/p\mathbb{Z}$, $H \simeq \mathbb{Z}/q\mathbb{Z}$

$$(k, h) \longmapsto kh$$

⑦ $K \ltimes H \xrightarrow{\simeq} G$ ← homomorphism ✓ injective ✓

is

$$\mathbb{Z}/p\mathbb{Z} \ltimes (\mathbb{Z}/q\mathbb{Z})$$

Questions!

New topic: rings!

$\mathbb{Z}/n\mathbb{Z}$ ⊸ has $+, \cdot$, both of these structures are important, so far we never considered them "together"

(considered $(\mathbb{Z}/n\mathbb{Z}, +)$ or $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$)

What if we consider $\underline{\underline{(\mathbb{Z}/n\mathbb{Z}, +, \cdot)}}$?

<u>Definition</u>. A ring R is a set with $+ : R \times R \to R$ and $\cdot : R \times R \to R$

addition   multiplication

Such that:

(a) $(R, +)$ ← commutative group, its identity is $0 \in R$

(b) $(R, \cdot)$ ← monoid, identity is $1 \in R$

$((a \cdot b) \cdot c = a \cdot (b \cdot c))$

$(a \cdot 1 = a = 1 \cdot a)$

(c) distributive law: $\forall a, b, c \in R$,

$$(a+b) \cdot c = a \cdot c + b \cdot c$$

Remark: in general, people also consider rings without identity ($(R, \cdot)$ ← semigroup), we will not consider this generalization

Examples: $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

<u>commutative</u> rings ($\cdot$ is commutative)

$$\mathrm{Mat}_{2\times 2} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \,\middle|\, a, b, c, d \in \mathbb{R} \right\}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix}$$

Exercise: check that $(\mathrm{Mat}_{2\times 2}, +, \cdot)$ is a <u>noncommutative</u> ring

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}; \quad \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Note: R ← ring $\rightsquigarrow$ $R^\times$ ← group

$$R^\times = \{x \in R \mid \exists y \in R,\ xy = 1\}$$

Important subclass of rings:

R ← skew field if $R^\times = R \setminus \{0\}$

field if $R^\times = R \setminus \{0\}$

R ← commutative

Examples:

$\mathbb{Z}$ ← not a field

$\mathbb{Q}$ ← field

$\mathbb{R}$ ← field

$\mathbb{C}$ ← field

$\mathbb{Z}/n\mathbb{Z}$ ← field iff n ← prime

$(\mathbb{Z}/n\mathbb{Z})^{\times} = \{ k = 1, \dots, n-1 \mid \gcd(k,n) = 1 \}$

φ

coincides with $\{1, \dots, n-1\}$ iff n - prime