Groups & Rings: Lecture #26

Repetition: Groups

- 2014-05 #1 • Groups: definition, examples, subgroups
  S_n (symmetric group) D_n (dihedral group)
  $C_n = \mathbb{Z}/n\mathbb{Z}$ (cyclic group) M_n, GL_n (matrix groups)
- • Permutation groups (cycles, conjugation, ...)
- 2014-03 #1 • Lagrange's theorem: order of groups & elements, FLT
- • Quotient groups: cosets, normal subgroups
- 2015-03 #3 • Isomorphism theorems, homomorphisms
- • Fundamental theorem of abelian groups
- 2014-03 #3 • Group actions: orbits, stabilizers
- 2014-03 #2 2014-05 #2 • Sylow theorems (and applications to classification of groups)

Problem 1 $\boxed{2014-03-19}$

Show for each integer a that $35 \mid a^{13} - a$.

$a \in \mathbb{Z}$ $\quad 35 \mid a^{13} - a \quad (a^{13} \equiv a \pmod{35})$

$35 = 5 \cdot 7$

Fermat's little theorem $\quad a^p \equiv a \pmod p \quad \forall$ primes p.

$\Rightarrow 13 \mid a^{13} - a$

$$35 \mid a^{13} - a \iff \underbrace{5 \mid a^{13} - a}\ \&\ \underbrace{7 \mid a^{13} - a}$$

$a^{13} = a^5 a^5 a^3 \equiv a a a^3 = a^5 \equiv a \pmod 5$ $\qquad$ (mod 7) $a^{13} = a^7 \cdot a^6 \equiv a \cdot a^6 = a^7 \equiv a$

Fermat l.t. $p=5$ $\qquad$ FLT $p=7$

Problem 2 $\boxed{2014-03-19}$

Let G be a group of order $340 = 2^2 \cdot 5 \cdot 17$.

1. Show that G has normal cyclic subgroups of orders 5 and 17. (2p)
2. Show that G has a cyclic subgroup N of order $85 = 5 \cdot 17$. (3p)
3. Show that N is normal. (1p)

1. $|G| = 340 = 2^2 \cdot 5 \cdot 17$

Recall: Sylow I says $\exists$ Sylow p-subgroups for $p = 2, 5, 17$

i.e., subgroups of orders $4, \underbrace{5}, \underbrace{17}$.

automatically cyclic: order of any non-trivial element has order $5/17$.

Recall: Sylow II says $n_p := (\#$ of Sylow p-subgroups$)$ satisfies:

$$n_p \equiv 1 \pmod p \quad \text{and} \quad n_p \mid |G|.$$

Recall: Sylow III says that Sylow p-subgroups are conjugated

that is, H & H' p-Sylows $\Rightarrow \exists g \in G \quad gHg^{-1} = H'$.

Consequence: H p-Sylow, then $\boxed{H \text{ is normal} \iff n_p = 1}$

Thus, need to prove: $n_5 = 1$ and $n_{17} = 1$.

Sylow II $\Rightarrow \quad n_5 \equiv 1 \pmod 5 \qquad n_5 \mid 4 \cdot \cancel{5} \cdot 17 \qquad n_5 = 1, 2, 4, 17, 34, 68$

$\not\equiv 1 \pmod 5$

$\Rightarrow \quad n_5 = 1 \iff$ 5-Sylow is normal

Similar argument for $p = 17 \Rightarrow n_{17} = 1$.

2. $\overset{?}{\exists} N \leq G$ with $|N| = 5 \cdot 17$. If N exists, then:

Sylow 5 $\quad C_5 \leq N \leq G$

Sylow 17 $\quad C_{17} \leq N$

b/c C_5 and C_{17} unique in G and N contains groups of orders 5 & 17.

Smallest group containing C_5 and C_{17} is denoted $\langle C_5, C_{17} \rangle$ (the join of C_5 & C_{17})

If elements in C_5 and C_{17} commute, then $\langle C_5, C_{17} \rangle$ coincides with

$$C_5 C_{17} = \{ g_1 g_2 : g_1 \in C_5, g_2 \in C_{17} \} \quad \text{(in general just a set)}$$

and if moreover $C_5 \cap C_{17} = \{e\}$ then $C_5 C_{17} \cong C_5 \times C_{17}$, that is, every element in $C_5 C_{17}$ has unique expression $g_1 g_2$

Thus, need to prove:

(a) $C_5 \cap C_{17} = \{e\}$

(b) C_5 and C_{17} commute

$$\Rightarrow N = C_5C_{17} \cong \underbrace{C_5}_{\substack{\mathbb{Z}/5\mathbb{Z} \\ \| \\ \langle g_1\rangle}} \times \underbrace{C_{17}}_{\substack{\mathbb{Z}/17\mathbb{Z} \\ \| \\ \langle g_2\rangle}} \cong C_{5\cdot 17} \; (\mathbb{Z}/5\cdot17\mathbb{Z}) \cong \langle g_1g_2\rangle$$

5 & 17 rel prime. generator is $(1, 1)$

COMMENT: If (a)+(b) does not hold, can still consider $\langle g_1g_2\rangle$.
If (a) does not hold $|g_1g_2| < |g_1|\cdot|g_2|$ can happen.
If (b) does not hold $|g_1g_2| > |g_1|\cdot|g_2|$ can happen.

Proof of (a) + (b):

(a) $g \in C_5 \cap C_{17},\ g \neq e \Rightarrow |g| = 5\ \&\ |g| = 17$ ↯

(b) $g_1 \in C_5,\ g_2 \in C_7$: $\underline{g_1g_2 = g_2g_1}$?

$$\Leftrightarrow \underbrace{g_1g_2g_1^{-1}g_2^{-1}}_{\substack{\text{commutator of } g_1 \,\&\, g_2 \\ \| \\ [g_1, g_2]}} = e \Leftrightarrow g_1g_2g_1^{-1}g_2^{-1} \in \underbrace{C_5 \cap C_7}_{\substack{\| \, (a) \\ \{e\}}}$$

- $\underbrace{g_1g_2g_1^{-1}}_{\substack{\text{⋒} \\ g_1C_{17}g_1^{-1} = C_{17}}}\underbrace{g_2^{-1}}_{\in C_{17}} \in C_{17}$ ↑ C_{17} normal

- $\underbrace{g_1}_{C_5 \ni}\underbrace{g_2g_1^{-1}g_2^{-1}}_{\substack{\text{⋒} \\ g_2C_5g_2^{-1} = C_5}} \in C_5$ ↑ C_5 normal

More generally: If H_1, H_2 normal subgroups of G and $|H_1|, |H_2|$ relatively prime $\Rightarrow H_1H_2 \cong H_1 \times H_2$

3. Is N normal? That is, $gNg^{-1} = N \ \forall g \in G$?
Equivalently: is $gng^{-1} \in N \ \forall g \in G, n \in N$?
By **2.** $N = C_5C_{17} \Rightarrow n = g_1g_2,\ g_1 \in C_5,\ g_2 \in C_{17}$.

$$gng^{-1} = g(g_1g_2)g^{-1} = \underbrace{gg_1g^{-1}}_{\substack{\text{⋒} \\ C_5}}\underbrace{gg_2g^{-1}}_{\substack{\text{⋒} \\ C_{17}}} \in C_5C_{17} = N$$

b/c C_5 normal → ; ← b/c C_{17} normal.

So N normal.

Problem 3 $\boxed{2014-03-19}$

Let G be a group such that all non-identity elements are conjugate. Show that the order of G is 1, 2, or infinite.

Recall: g_1, g_2 conjugate means $\exists g \in G: \ g g_1 g^{-1} = g_2$.

Rmk: • e is always only conjugate to itself $geg^{-1} = e$.

• conjugacy is an equivalence relation

Conj. classes of G are $\{e\}$, $G \setminus \{e\}$ in the current problem.

Mentioned in book: (size of conjugacy class) $\big|$ $|G|$.

Thus $(|G|-1) \,\big|\, |G| \implies |G| = 1, 2$ or ∞.

Why? Lagrange's theorem? (conjugacy classes are not subgroups)

Group action? If G acts on set X (pictorially: $\underset{\text{group}}{G} \circlearrowright \underset{\text{set}}{X}$)

we write $g.x$ for image of $x \in X$ by action of $g \in G$:

- orbit of $x \in X$: $Gx = O(x) = \{ g.x : g \in G \} \subseteq X$
- stabilizer of $x \in X$: $G_x = \{ g \in G : g.x = x \} \leq G$ subgroup

Orbit-stabilizer thm: Let $x \in X$. Then $|Gx| \cdot |G_x| = |G|$.

Conjugation action: $\underset{\substack{\psi \\ g}}{G} \circlearrowright \underset{\substack{\psi \\ x}}{G}$ $\quad g.x = gxg^{-1}$

(orbit of $x \in G$) = conj. class of x

$|\text{conj class of } x| = |Gx| = |G| / |G_x|$

$\implies |\text{conj class of } x| \,\big|\, |G|$.

Problem 1 $\boxed{2014\text{-}05\text{-}21}$

Let G be a group with an element x such that $xyx = y^3$ for all $y \in G$. Show that

1. $x^2 = e$ (1p);
2. $y^8 = e$ for all $y \in G$ (3p).

Know: $\exists x \in G,\ \forall y : \boxed{xyx = y^3}$. $(*)$

(1.) FAILED ATTEMPT: Take $y = x$ in $(*) \Rightarrow x^3 = x^3$.

NEW ATTEMPT: Take $y = e$ in $(*) \Rightarrow x^2 = e^3 = e$ OK.

(2.) FAILED ATTEMPT: $y^8 = y^3 \cdot y^3 \cdot y^2 \overset{(*) \text{ for } y}{=} (xyx)(xyx)y^2$ $\underbrace{x)(x}_{= e \text{ by } (1)}$

$= xy^2xy^2 \overset{(*) \text{ for } y^2}{=} y^6 \cdot y^2 = y^8$

NEW ATTEMPT: $xyx = y^3 \Rightarrow y^2 = xyxy^{-1}$

$\overset{\text{by } (1)}{=} xyxy^{-1}x^2 = xy(xy^{-1}x)x \overset{y^{-1}}{=} xyy^{-3}x = xy^{-2}x \overset{y^{-2}}{=} y^{-6}$

$\Rightarrow y^8 = e$

SHORTER ARGUMENT: $y \overset{\text{by } (1)}{=} x^2yx^2 = x(xyx)x \overset{y}{=} xy^3x \overset{y^3}{=} y^9$

$\Rightarrow y^8 = e$

Problem 2 $\boxed{2014-05-21}$

Let G be a simple group of order $168 = 2^3 \cdot 3 \cdot 7$ (i. e. a group with no nontrivial normal subgroups). How many elements of order 7 does G have?

$|G| = 168 = 8 \cdot 3 \cdot 7$, no normal subgroups.

If $g \in G$, $|g| = 7 \Rightarrow \langle g \rangle \cong C_7$ has to be a 7-Sylow.

$n_7 = ?$ Sylow II $\Rightarrow n_7 \equiv 1 \pmod 7$ $\quad n_7 \mid 8 \cdot 3$

$n_7 = 1, \cancel{3}, 8, \cancel{24}$ $\quad \neq 1$

$n_7 = 1$ impossible b/c no normal subgroup

$\Rightarrow n_7 = 8.$

Set of elements of order $7 = \{ g \in G : |g| = 7 \} = \bigcup_{\substack{H < G \\ \text{7-Sylow}}} (H \setminus \{e\})$

CLAIM: Union is disjoint:

H_1, H_2 7-Sylows $\Rightarrow H_1 \cap H_2 \leq H_1$

$\Rightarrow |H_1 \cap H_2| \mid |H_1| = 7$

$\Rightarrow |H_1 \cap H_2| = 1$ or 7

$\Rightarrow H_1 \cap H_2 = \{e\}$ or $H_1 = H_2$

$\Rightarrow$ The number of elements of order 7 is:

$(7-1) \cdot 8 = \underline{\underline{48}}$

Problem 3. (6 points). $\boxed{\text{2015-03-16}}$

Let $f: G \to H$ be a group homomorphism with kernel K and image I. Show:

(a) For every subgroup $N \leq G$, $f^{-1}(f(N)) = KN = \{kn \mid k \in K, n \in N\}$.

(b) For every subgroup $L \leq H$, $f(f^{-1}(L)) = I \cap L$.

$f: G \longrightarrow H$. Kernel $K = \ker(f)$ subgroup of G.
Image $I = \operatorname{im}(f)$ subgroup of H.

a $\quad N \leq G, \quad \underbrace{f^{-1}(\underbrace{f(N)}_{\text{subgroup of } H})}_{\text{subgroup of } G} \overset{?}{=} KN := \underbrace{\{kn : k \in K, n \in N\}}_{\text{a priori only a set: } k_1 n_1 k_2 n_2 = k_3 n_3\ ?}$

LHS ⊂ RHS

$g \in f^{-1}(f(N)) \Rightarrow f(g) = f(n)$ for some $n \in N$

$\Leftrightarrow f(gn^{-1}) = e \Leftrightarrow gn^{-1} \in K$ i.e. $gn^{-1} = k$ for some $k \in K$

$\Rightarrow g = kn$.

RHS ⊂ LHS

Let $g = kn$. Then $f(g) = \underbrace{f(k)}_{=e} f(n) = f(n) \in f(N)$

so $g \in f^{-1}(f(N))$.

b $\quad f(f^{-1}(L)) = \{f(x) : x \in G, f(x) \in L\} = \operatorname{im}(f) \cap L$

$= I \cap L$