Ch 1: INTRODUCTION TO GROUPS

Thurs. Sep 26 '13

Section 1.1: Basic Axioms & Examples

Def: A **GROUP** is a set G w/ a binary operation $*$ such that the following are satisfied:

1.) **CLOSURE:** If $a, b \in G$, then $a * b \in G$

2.) **ASSOCIATIVITY:** $(a*b)*c = a*(b*c)$ $\forall\, a, b, c \in G$

3.) **IDENTITY:** $\exists\, e \in G$ s.t. $a*e = e*a = a$ $\forall\, a \in G$.

4.) **INVERSES:** $\forall\, a \in G$, $\exists\, a^{-1} \in G$ s.t. $a * a^{-1} = a^{-1} * a = e$.

Def: A group G is **ABELIAN** (COMMUTATIVE) if $a*b = b*a$ $\forall\, a, b \in G$.

Notation: We write $a*b$ as ab when dealing w/ an abstract group.

Ex.) $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ under $+$.

1.) If $a, b \in \mathbb{Z}$, then $a+b \in \mathbb{Z}$ (CLOSED UNDER $+$)

2.) $(a+b)+c = a+(b+c)$ $\forall\, a, b, c \in \mathbb{Z}$ (ASSOCIATIVE)

3.) $e = 0 \in \mathbb{Z}$, since $a+0 = 0+a = a$ $\forall\, a \in \mathbb{Z}$ (IDENTITY)

4.) $a^{-1} = -a \in \mathbb{Z}$, since $a+(-a) = (-a)+a = 0$ $\forall\, a \in \mathbb{Z}$

5.) $a+b = b+a$ $\forall\, a, b \in \mathbb{Z}$ (COMMUTATIVE) (ADDITIVE INVERSES)

$\therefore \langle \mathbb{Z}, + \rangle$ is an Abelian Group.

Ex.)

GROUPS	NON-GROUPS
$\langle \mathbb{R}, + \rangle$	$\langle \mathbb{R}, \cdot \rangle$ $\because$ 0 is NOT invertible!
$\langle \mathbb{R} \setminus \{0\}, \cdot \rangle$	$\langle \mathbb{Z}, \cdot \rangle$
$\langle \mathbb{C}, + \rangle$	$\langle \mathbb{C}, \cdot \rangle$
$\langle \mathbb{Q}, + \rangle$	$\langle \mathbb{Q}, \cdot \rangle$

Prop: Let G be a group. Then...

1.) $\exists!\, e \in G$ s.t. $e*a = a*e = a$ $\forall\, a \in G$ (UNIQUE IDENTITY)

Pf: Let $e, e' \in G$ be identity elements.
$\Rightarrow e = ee' = e'$ ▨

2.) $\forall\, a \in G$, $\exists!\, a^{-1} \in G$ s.t. $a * a^{-1} = a^{-1} * a = e$ (UNIQUE INVERSES)

Pf: Let $a \in G$, and let $b, c \in G$ be inverses of a.
$\Rightarrow b = be = b(ac) = (ba)c = ec = c$ ▨

M® MIQUELRIUS

3.) $(a^{-1})^{-1} = a \quad \forall\, a \in G$

Pf: Let $a \in G$

$\Rightarrow aa^{-1} = a^{-1}a = e$

$\Rightarrow (a^{-1})^{-1} = a$ ▨

4.) $(ab)^{-1} = b^{-1}a^{-1} \quad \forall\, a,b \in G$

Pf: Let $a,b \in G$. Let $c = (ab)^{-1}$

$\Rightarrow (ab)c = e$

$\Rightarrow a(bc) = e$

$\Rightarrow a^{-1}(a(bc)) = a^{-1}e = a^{-1}$

$\Rightarrow (a^{-1}a)(bc) = a^{-1}$

$\Rightarrow ebc = a^{-1}$

$\Rightarrow bc = a^{-1}$

$\Rightarrow b^{-1}(bc) = b^{-1}a^{-1}$

$\Rightarrow (b^{-1}b)c = b^{-1}a^{-1}$

$\Rightarrow ec = b^{-1}a^{-1}$

$\Rightarrow c = b^{-1}a^{-1}$ ▨

Def: Let n be an integer w/ $n \geq 2$. Given $a,b \in \mathbb{Z}$, we write $a \equiv b \pmod n$ if $n \mid a-b$.

↖ CONGRUENCE MODULO n

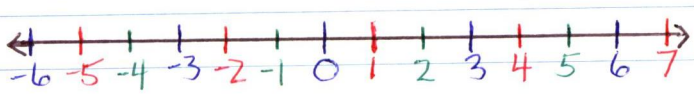
Ex.) $n = 3$

$7 \equiv 4 \pmod 3$ ∵ $7 - 4 = 3 = 3(1)$

NOTE: Congruence is an EQUIVALENCE RELATION on $\mathbb{Z}$.

Def: Let $n \in \mathbb{Z}$ w/ $n \geq 2$. Given $a \in \mathbb{Z}$, the EQUIVALENCE CLASS of a is $\bar{a} = \{x \in \mathbb{Z} : x \equiv a \pmod n\}$.

Ex.) $n = 3$



$\bar{0} = \{\ldots, -6, -3, 0, 3, 6, \ldots\} = \{x \in \mathbb{Z} : x \equiv 0 \pmod 3\}$

$\bar{1} = \{\ldots, -5, -2, 1, 4, 7, \ldots\} = \{x \in \mathbb{Z} : x \equiv 1 \pmod 3\}$

$\bar{2} = \{\ldots, -4, -1, 2, 5, 8, \ldots\} = \{x \in \mathbb{Z} : x \equiv 2 \pmod 3\}$

FACT: Let $a,b \in \mathbb{Z}$. Then $\bar{a} = \bar{b}$ iff $a \equiv b \pmod n$ iff $b \in \bar{a}$ iff $a \in \bar{b}$. ∴ $\bar{6} = \bar{0}$, since $6 \in \bar{0}$

MIQUELRIUS

Also written as $\mathbb{Z}/n\mathbb{Z}$

Def: Let $n \geq 2$ be an integer. Then $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$ is the set of **INTEGERS MODULO n**.

Ex.) $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$ $\quad \mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$

ADDITION & MULTIPLICATION IN $\mathbb{Z}_n$:

a.) $\bar{a} + \bar{b} = \overline{a+b}$

b.) $\bar{a} \cdot \bar{b} = \overline{ab}$

Ex.) cln $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$, $\bar{2} + \bar{3} = \bar{5} = \bar{1}$ & $\bar{3} \cdot \bar{3} = \bar{9} = \bar{1}$.

FACT: $\langle \mathbb{Z}_n, + \rangle$ is a **GROUP**.

$\bar{e} = \bar{0}$

$\bar{a}^{-1} = \overline{-a}$

NOTE: $\langle \mathbb{Z}_n, \cdot \rangle$ is **NOT** a group! ← UNLESS $n = 1$

- To form a group, delete all non-invertible elements in $\mathbb{Z}_n$ under $\cdot$.

Def: $\mathbb{Z}_n^\times = \{\bar{a} \in \mathbb{Z}_n : \gcd(a,n) = 1\} = \{\bar{a} \in \mathbb{Z}_n : \exists \bar{b} \in \mathbb{Z}_n \text{ s.t. } \bar{a} \cdot \bar{b} = \bar{1}\}$.

"$\mathbb{Z}_n$ Cross" ← Coprime w/ n

FACT: $\langle \mathbb{Z}_n^\times, \cdot \rangle$ is a **GROUP**.

$\bar{e} = \bar{1}$

Ex.) $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

$\mathbb{Z}_6^\times = \{\bar{1}, \bar{5}\}$ $\quad \bar{1}^{-1} = \bar{1}$ & $\bar{5}^{-1} = \bar{5}$

Pf:

$\exists \bar{x} \in \mathbb{Z}_n$ s.t. $\bar{a} \cdot \bar{x} = \bar{1}$

$\iff ax = 1 + n(-y)$ f.s. $x, y \in \mathbb{Z}$

$\iff ax + ny = 1$

$\iff \gcd(a,n) = 1$ ☒

NOTATION: Let G be a group. Let $n \in \mathbb{Z}$ & $x \in G$.

a.) clf $n > 0$, then $x^n = \underbrace{x \cdot x \cdot \ldots \cdot x}_{n \text{ times}}$ and $x^{-n} = \underbrace{(x^{-1}) \cdot (x^{-1}) \cdot \ldots \cdot (x^{-1})}_{n \text{ times}}$

b.) $x^0 = e$

Def: Let G be a group, and let $x \in G$. The **ORDER OF x** is the smallest positive integer s.t. $x^k = e$.

- clf no such k exists, then the order of x is infinite.
- **NOTATION:** $|x| = \text{Order}(x) = O(x)$
- $|e| = 1$

MIQUELRIUS

Ex.) $\mathbb{Z}_{14}^{\times} = \{\overline{1}, \overline{3}, \overline{5}, \overline{9}, \overline{11}, \overline{13}\}$

$\overline{3}^1 = \overline{3}$
$\overline{3}^2 = \overline{9}$
$\overline{3}^3 = \overline{27} = \overline{13}$
$\overline{3}^4 = \overline{39} = \overline{11}$
$\overline{3}^5 = \overline{33} = \overline{5}$
$\overline{3}^6 = \overline{15} = \overline{1}$ $\quad \therefore |\overline{3}| = \text{order}(\overline{3}) = O(\overline{3}) = 6$

$\langle \mathbb{Z}_{12}, + \rangle$

HW #11: Find the orders of each element of $\langle \mathbb{Z}/12\mathbb{Z}, + \rangle$

Observation: $|\overline{a}| = \frac{n}{\gcd(a,n)} = \frac{\text{lcm}(a,n)}{a}$

$|\overline{0}| = \frac{12}{12} = 1$
$|\overline{1}| = \frac{12}{1} = 12$
$|\overline{2}| = \frac{12}{2} = 6$
$|\overline{3}| = \frac{12}{3} = 4$
$|\overline{4}| = \frac{12}{4} = 3$
$|\overline{5}| = \frac{12}{1} = 12$
$|\overline{6}| = \frac{12}{6} = 2$
$|\overline{7}| = \frac{12}{1} = 12$
$|\overline{8}| = \frac{12}{4} = 3$
$|\overline{9}| = \frac{12}{3} = 4$
$|\overline{10}| = \frac{12}{2} = 6$
$|\overline{11}| = \frac{12}{1} = 12$

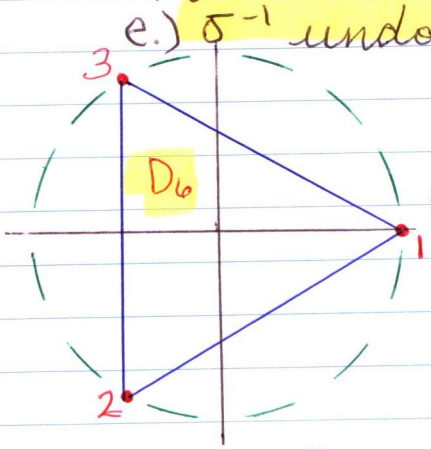
MIQUELRIUS

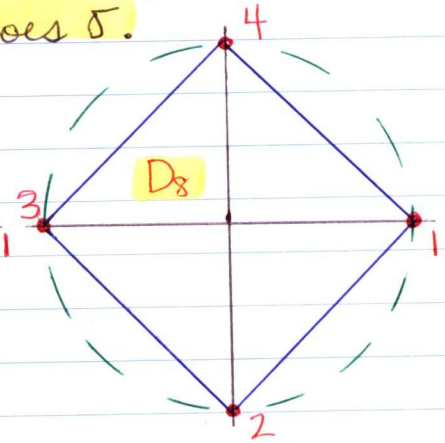
Tues. Oct 01 '13

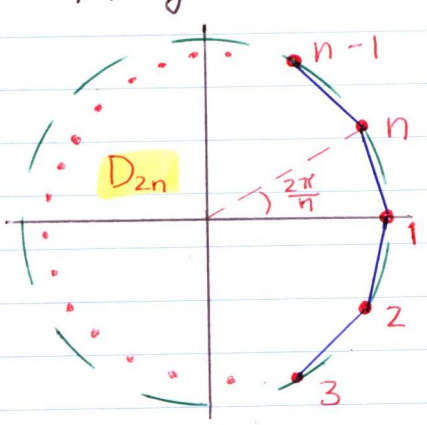
Section 1.2: Dihedral Groups

Def: The **DIHEDRAL GROUP D_{2n}** ($n \geq 3$) is the group of symmetries of a regular n-gon.

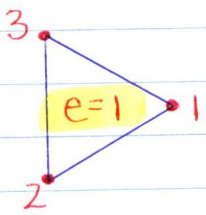
- **VISUAL:** Fix the n-gon w/ vertices evenly spaced on the unit circle. Label the vertices $1, \ldots, n$ clockwise.
  a.) The angle between vertices is $\frac{2\pi}{n}$ radians.
  b.) r = Clockwise rotation $\frac{2\pi}{n}$ radians.
  c.) s = Reflection across x-axis.
  d.) For $\sigma, \tau \in D_{2n}$, $\sigma\tau$ means apply τ then σ.
  e.) σ^{-1} undoes σ.

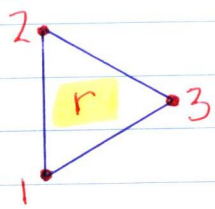


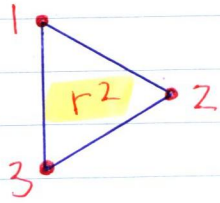


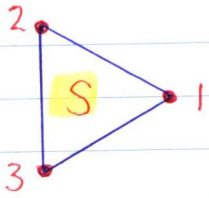


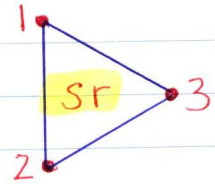
Ex.) D_6:

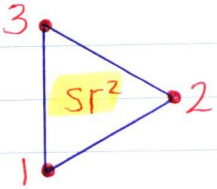




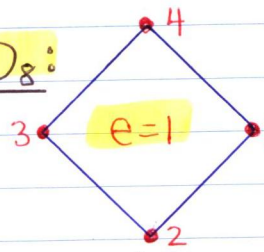


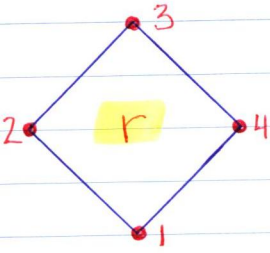


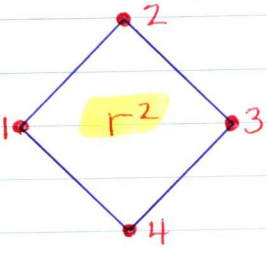


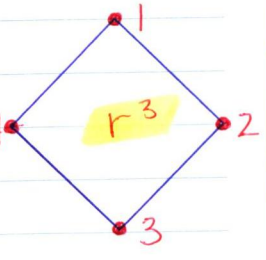


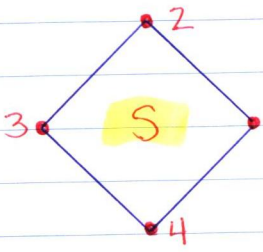
Ex.) D_8:

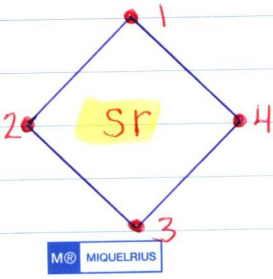


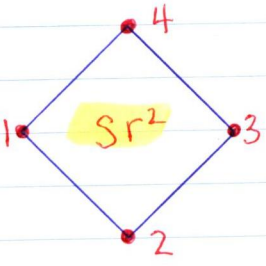


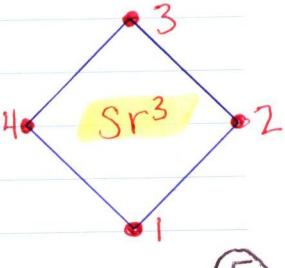












MIQUELRIUS

- **ALGEBRAIC:** $D_{2n} = \{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}$ ($r^0 = 1$)

  WRITE "S" BEFORE "R"

  a.) $1, r, \ldots, r^{n-1}$ are distinct rotations.

  b.) $r^n = s^2 = 1$ ← So $|r| = n$ ∧ $|s| = 2$

  c.) $r^{-1} = r^{n-1}$ & $s^{-1} = s$ ∵ $rr^{n-1} = r^n = 1$ ∧ $ss = s^2 = 1$

  d.) $s \neq r^i$ for ANY i

  e.) $sr^i \neq sr^j$ for $0 \leq i < j \leq n-1$ ∵ $r^i \neq r^j$ if $0 \leq i < j \leq n-1$

  To Commute s & r:

  f.) $rs = sr^{-1} = sr^{n-1}$

  g.) $r^i s = sr^{-i} = sr^{n-i}$, where $r^{-i} = (r^{-1})^i$

Ex.)

D_6	1	r	r^2	s	sr	sr^2
1	1	r	r^2	s	sr	sr^2
r	r	r^2	1	sr^2	s	sr
r^2	r^2	1	r	sr	sr^2	s
s	s	sr	sr^2	1	r	r^2
sr	sr	sr^2	s	r^2	1	r
sr^2	sr^2	s	sr	r	r^2	1

$(s)(sr) = s^2 r = r$

$(sr^2)(sr) = r^{-2} ssr = r^{-1} = r^2$

$(sr)(sr^2) = srr^{-2}s = sr^{-1}s$
$= ssr = r$

NOTE: D_{2n} is NOT Abelian!

Ex.)

D_8	1	r	r^2	r^3	s	sr	sr^2	sr^3
1	1	r	r^2	r^3	s	sr	sr^2	sr^3
r	r	r^2	r^3	1	sr^3	s	sr	sr^2
r^2	r^2	r^3	1	r	sr^2	sr^3	s	sr
r^3	r^3	1	r	r^2	sr	sr^2	sr^3	s
s	s	sr	sr^2	sr^3	1	r	r^2	r^3
sr	sr	sr^2	sr^3	s	r^3	1	r	r^2
sr^2	sr^2	sr^3	s	sr	r^2	r^3	1	r
sr^3	sr^3	s	sr	sr^2	r	r^2	r^3	1

MIQUELRIUS

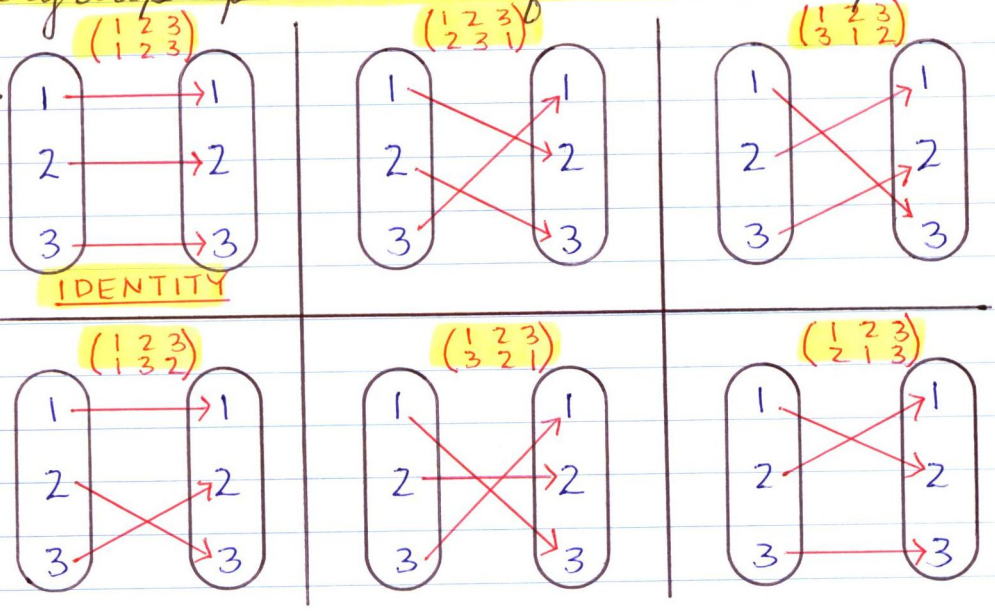
Tues. Oct 01 '13

Section 1.3: Symmetric Groups

Def: a **PERMUTATION** is a bijection from a set to itself.

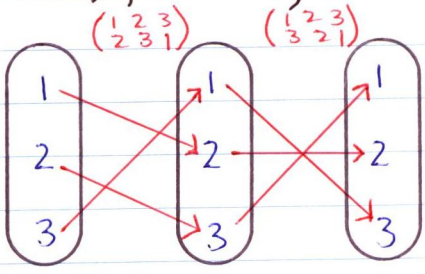
Def: The **SYMMETRIC GROUP S_n** of degree n is the group of permutations of $\{1, 2, \ldots, n\}$.
- The group operation is function composition.

Ex.) S_3:



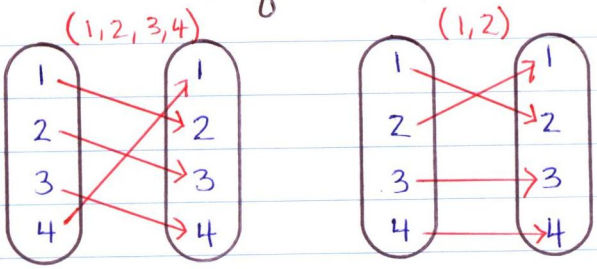
$$S_3 = \left\{ \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}, \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}, \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} \right\}$$

Ex.) In S_3, $\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$



CYCLE NOTATION: a **CYCLE** $\sigma = (a_1, a_2, \ldots, a_m)$ is an element of S_n s.t.
a.) $\sigma(a_i) = a_{i+1}$ for $1 \le i \le m-1$
b.) $\sigma(a_m) = a_1$
c.) Non-listed elements of $\{1, 2, \ldots, n\}$ are fixed by σ.

Ex.) In S_4...



$\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix} = (1,2,3,4)$

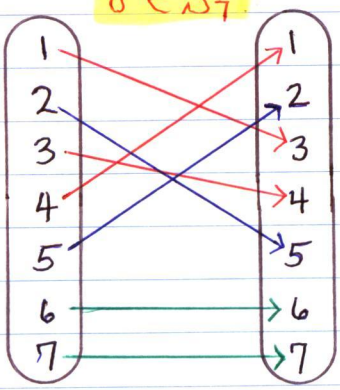
$\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix} = (1,2)$

Ex.) $S_3 = \{(1), (1,2,3), (1,3,2), (2,3), (1,3), (1,2)\}$

MIQUELRIUS

FACT: Any $\sigma \in S_n$ can be written as a product of disjoint cycles (no common elements).

Ex.) $\sigma \in S_7$



$\sigma = (1,3,4)(2,5)$

TRANSPOSITION = Length 2 Cycle.

NOTES:

1.) Order matters, but starting # doesn't.
- $(1,3,4) = (3,4,1) = (4,1,3)$
- $(2,5) = (5,2)$

2.) Transpositions are self-inverses.
- $(2,5)^{-1} = (2,5)$

3.) Disjoint cycles commute!
- $(1,3,4)(2,5) = (2,5)(1,3,4)$

FACT: S_n is NOT Abelian for $n \geq 3$.

Ex.) $(1,2)(1,3) = (1,3,2)$
$(1,3)(1,2) = (1,2,3)$

MIQUELRIUS

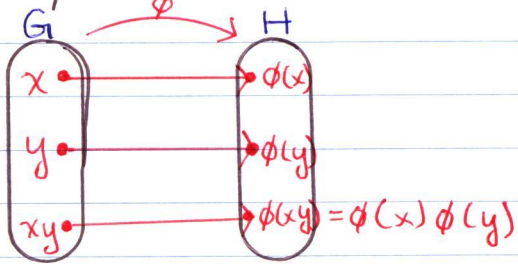
Thurs. Oct 03 '13

Section 1.6 Homomorphisms & Isomorphisms

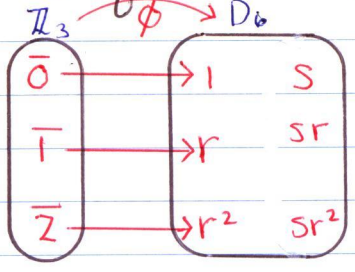
Def: Let G, H be groups. A function $\phi: G \to H$ is a **HOMOMORPHISM** if $\phi(xy) = \phi(x)\phi(y)$ $\forall x, y \in G$.

Def: An **ISOMORPHISM** is a bijective homomorphism (1-1 & ONTO).

- If $\exists$ an isomorphism between G & H, we say G is isomorphic to H, or $G \cong H$.



Ex.) Define $\phi: \mathbb{Z}_3 \to D_6$ by $\phi(\bar{a}) = r^a$ $\forall \bar{a} \in \mathbb{Z}_3$



Let $\bar{a}, \bar{b} \in \mathbb{Z}_3$

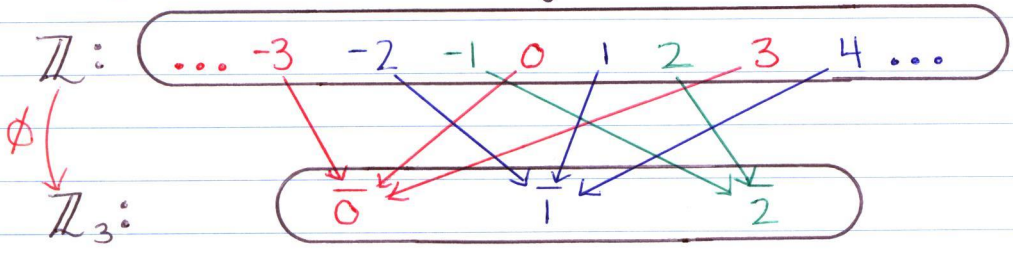
$\Rightarrow \phi(\bar{a}+\bar{b}) = \phi(\overline{a+b}) = r^{a+b} = r^a r^b$

$= \phi(\bar{a})\phi(\bar{b})$

$\therefore \phi$ is a Homomorphism

But ϕ is not Onto, so ϕ is not an isomorphism.
However, if $H = \{1, r, r^2\} \leq D_6$, then $\mathbb{Z}_3 \cong H$.

Ex.) Define $\phi: \mathbb{Z} \to \mathbb{Z}_3$ by $\phi(a) = \bar{a}$ $\forall a \in \mathbb{Z}$



Let $a, b \in \mathbb{Z}$

$\Rightarrow \phi(a+b) = \overline{a+b} = \bar{a} + \bar{b} = \phi(a) + \phi(b)$

$\therefore \phi$ is a homomorphism.

But ϕ is not 1-1, so ϕ is not an isomorphism.

MIQUELRIUS

NOTE: To show $G \ncong H$, find a **STRUCTURAL DIFFERENCE**, such as...

1.) $|G| \neq |H|$ ← $\nexists$ Bijection
   Ex.) $\mathbb{Z}_n \ncong \mathbb{Z}$, since $|\mathbb{Z}_n| < |\mathbb{Z}|$ (n ↘, ∞ ↙)

2.) G is Abelian, but H is not. ← See HW 1.6 #3
   Ex.) $\mathbb{Z}_6 \ncong S_3$, since S_3 is not Abelian.

3.) G is cyclic, but H is not. ← See HW 1.6 #6
   Ex.) $\mathbb{Z} \ncong \mathbb{Q}$, since $\mathbb{Q}$ is not cyclic.

4.) $\exists\, x \in G$ s.t. $|x| = k$, but not in H. ← See HW 1.6 #2b
   Ex.) $\langle \mathbb{R}\setminus\{0\}, \cdot \rangle \ncong \langle \mathbb{R}, + \rangle$, since $|-1| = 2$, but no $x \in \mathbb{R}$ has order 2.

5.) G is countable, but H is not. ← See HW 1.6 #5
   Ex.) $\mathbb{Q} \ncong \mathbb{R}$, since $\mathbb{R}$ is uncountable.

FACTS: Let $\phi: G \to H$ be a homomorphism.

a.) $\phi(x^n) = \phi(x)^n \quad \forall\, x \in G \wedge n \in \mathbb{Z}$

Pf: CASE 1: $n \geq 0$. Induct on n.

BASIC: $n = 0$. Let $x \in G$
$\Rightarrow \phi(x) = \phi(1_G x) = \phi(1_G)\phi(x)$
$\Rightarrow \phi(x^n) = \phi(x^0) = \phi(1_G) = 1_H = \phi(x)^0 = \phi(x)^n$

INDUCTIVE: Assume $\phi(x^n) = \phi(x)^n$ f.s. $n \geq 0$
$\Rightarrow \phi(x^{n+1}) = \phi(x^n x) = \phi(x^n)\phi(x) = \phi(x)^n \phi(x) = \phi(x)^{n+1}$

CASE 2: $n = -1$. Let $x \in G$
$\Rightarrow 1_H = \phi(1_G) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1})$, so $\phi(x)^{-1} = \phi(x^{-1})$.

CASE 3: $n < -1$. Let $m = -n$
$\Rightarrow \phi(x^n) = \phi(x^{-m}) = \phi[(x^m)^{-1}] = [\phi(x)^m]^{-1} = \phi(x)^{-m} = \phi(x)^n$ ▨

b.) Let $A \leq G$. Then $\phi(A) \leq H$ ← Use SUBGROUP CRITERION.

Pf: i.) $1_H \in \phi(A)$, since $1_G \in A$
ii.) Let $h, k \in \phi(A)$
$\Rightarrow \exists\, x, y \in A$ s.t. $\phi(x) = h \wedge \phi(y) = k$
$\Rightarrow hk^{-1} = \phi(x)\phi(y)^{-1} = \phi(x)\phi(y^{-1}) = \phi(xy^{-1}) \in \phi(A)$
$\therefore \phi(A) \leq H$ ▨

COROLLARY: $\phi(G) \leq H$

Pf: $G \leq G$, so $\phi(G) \leq H$ ▨

MIQUELRIUS

c.) If $B \leq H$, then $\phi^{-1}(B) \leq G$.

Pf: i.) $1_G \in \phi^{-1}(B)$, since $\phi(1_G) = 1_H \in B$

ii.) Let $x, y \in \phi^{-1}(B)$

$\Rightarrow \phi(x), \phi(y) \in B$

$\Rightarrow \phi(y^{-1}) = \phi(y)^{-1} \in B$, since $B \leq H$

$\Rightarrow \phi(xy^{-1}) = \phi(x)\phi(y^{-1}) \in B$

$\Rightarrow xy^{-1} \in \phi^{-1}(B)$ ▨

FACTS: Let $\phi: G \to H$ be an isomorphism.

a.) $\phi^{-1}: H \to G$ is an isomorphism.

Pf: i.) Assume $\phi^{-1}(h) = \phi^{-1}(k)$

$\phi(\phi^{-1}(h)) = \phi(\phi^{-1}(k))$

$h = k$

ii.) Let $x \in G$

$\Rightarrow \phi(x) = y$ f.s. $y \in H$

$\Rightarrow \phi^{-1}(y) = x$ $\because \phi$ is 1-1.

iii.) Let $h, k \in H$

$\Rightarrow \exists!\ x, y \in G$ s.t. $\phi(x) = h \wedge \phi(y) = k$

$\Rightarrow \phi^{-1}(hk) = \phi^{-1}(\phi(x)\phi(y)) = \phi^{-1}(\phi(xy)) = xy = \phi^{-1}(h)\phi^{-1}(k)$ ▨

b.) $|x| = |\phi(x)| \quad \forall x \in G$

Pf: Let $x \in G$. Suppose $|x| = m \wedge |\phi(x)| = n$

$\Rightarrow x^m = 1_G \wedge \phi(x)^n = 1_H$

Assume for contradiction that $m \neq n$.

CASE 1: $m < n$

$\Rightarrow x^m = 1_G$ but $\phi(x)^m \neq 1_H$

$\Rightarrow 1_H = \phi(1_G) = \phi(x^m) = \phi(x)^m \neq 1_H$ (*)

CASE 2: $n < m$

$\Rightarrow \phi(x)^n = 1_H$ but $x^n \neq 1_G$

$\Rightarrow 1_G = \phi^{-1}(1_H) = \phi^{-1}(\phi(x)^n) = \phi^{-1}(\phi(x^n)) = x^n \neq 1_G$ (*)

So $|x| = m = n = |\phi(x)|$ ▨

c.) G is Abelian iff H is Abelian.

Pf ($\Rightarrow$): Assume G is Abelian. Let $x, y \in G$

$\Rightarrow \phi(x)\phi(y) = \phi(xy) = \phi(yx) = \phi(y)\phi(x)$

$\Rightarrow H = \phi(G)$ is Abelian.

Pf ($\Leftarrow$): Assume H is Abelian. Let $h, k \in H$

$\Rightarrow \phi^{-1}(h)\phi^{-1}(k) = \phi^{-1}(hk) = \phi^{-1}(kh) = \phi^{-1}(k)\phi^{-1}(h)$

$\Rightarrow G = \phi^{-1}(H)$ is Abelian. ▨

M® MIQUELRIUS

d.) G & H have an equal number of elements of order n.

Pf: Let $A=\{x\in G: |x|=n\}$ & $B=\{y\in H: |y|=n\}$

CLAIM 1: $\phi(A)\subseteq B$

Pf: Let $a\in A$

$\Rightarrow n=|a|=|\phi(a)|$

$\Rightarrow \phi(a)\in B$

$\Rightarrow \phi(A)\subseteq B$

CLAIM 2: $B\subseteq\phi(A)$

Pf: Let $y\in B$

$\Rightarrow \exists x\in G$ s.t. $\phi(x)=y$

$\Rightarrow |x|=|\phi^{-1}(y)|=|y|=n$

$\Rightarrow x\in A$

$\Rightarrow y=\phi(x)\in\phi(A)$

$\Rightarrow B\subseteq\phi(A)$

$\therefore \phi(A)=B.$

$\Rightarrow |A|=|\phi(A)|=|B|$, since ϕ is 1-1 ▨

e.) G is cyclic iff H is cyclic.

Pf($\Rightarrow$): Assume G is cyclic

$\Rightarrow \exists a\in G$ s.t. $G=\langle a\rangle=\{\ldots, a^{-2}, a^{-1}, 1_G, a, a^2,\ldots\}$

$\Rightarrow \phi(G)=\{\ldots, \phi(a^{-2}), \phi(a^{-1}), \phi(1_G), \phi(a), \phi(a^2),\ldots\}$

$=\{\ldots, \phi(a)^{-2}, \phi(a)^{-1}, 1_H, \phi(a), \phi(a)^2,\ldots\}$

$=\langle\phi(a)\rangle$

$\Rightarrow H=\phi(G)=\langle\phi(a)\rangle$ is cyclic.

Pf($\Leftarrow$): Assume H is cyclic

$\Rightarrow \exists b\in H$ s.t. $H=\langle b\rangle=\{\ldots, b^{-2}, b^{-1}, 1_H, b, b^2,\ldots\}$

$\Rightarrow \phi^{-1}(H)=\{\ldots, \phi^{-1}(b^{-2}), \phi^{-1}(b^{-1}), \phi^{-1}(1_H), \phi^{-1}(b), \phi^{-1}(b^2),\ldots\}$

$=\{\ldots, \phi^{-1}(b)^{-2}, \phi^{-1}(b)^{-1}, 1_G, \phi^{-1}(b), \phi^{-1}(b)^2,\ldots\}$

$=\langle\phi^{-1}(b)\rangle$

$\Rightarrow G=\phi^{-1}(H)=\langle\phi^{-1}(b)\rangle$ is cyclic. ▨

M® MIQUELRIUS

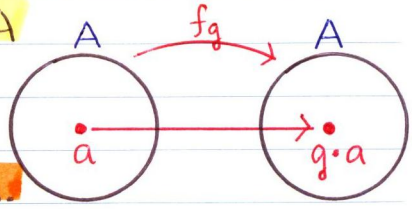
Thurs. Oct 03 '13

Section 1.7 Group Actions

Def: A **GROUP ACTION** of a group G on a set A is a map $f: G \times A \to A$ (written as $g \cdot a$ for $g \in G$ & $a \in A$) s.t.

1.) $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a \quad \forall\, g_1, g_2 \in G$ & $a \in A$

2.) $1 \cdot a = a \quad \forall\, a \in A$, where $e = 1$ in G.



The fixed g makes a function $f_g: A \to A$.

GROUP CONJUGATION: Let G be a group, & make G act on itself. Let $g \cdot a = gag^{-1}$ for $g \in G$ & $a \in A = G$.

↖ so $A = G$

CLAIM: Group Conjugation is a Group Action.

Pf: 1.) Let $g_1, g_2 \in G$ & $a \in A = G$

$$\Rightarrow g_1 \cdot (g_2 \cdot a) = g_1 \cdot (g_2 a g_2^{-1}) = g_1 (g_2 a g_2^{-1}) g_1^{-1}$$
$$= (g_1 g_2) a (g_1 g_2)^{-1} = (g_1 g_2) \cdot a$$

2.) Let $a \in A = G$

$$\Rightarrow 1 \cdot a = 1a1^{-1} = 1a1 = a$$

$\therefore$ Group Conjugation is a Group Action ▨

Ex.) Let $G = A = D_6$. Define $\sigma \cdot a$ by $\sigma a \sigma^{-1} \quad \forall\, \sigma, a \in D_6$

FIXED $\sigma \in G = D_6$

Let $\sigma = sr$, so $\sigma \cdot a = (sr)a(sr)^{-1}$

1.) $(sr)1(sr)^{-1} = 1$

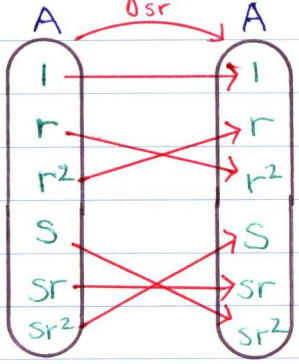
2.) $(sr)r(sr)^{-1} = sr^2r^{-1}s^{-1} = srs = r^2$

3.) $(sr)r^2(sr)^{-1} = srr^2r^{-1}s^{-1} = sr^2s = r$

4.) $(sr)s(sr)^{-1} = srsr^{-1}s^{-1} = r^{-2}s = sr^2$

5.) $(sr)sr(sr)^{-1} = sr$

6.) $(sr)sr^2(sr)^{-1} = srsr^2r^{-1}s^{-1} = srsrs = r^{-1}rs = s$



OBSERVE: The group action σ_{sr} permutes the elements of $A = D_6$.

MIQUELRIUS

Ch 2: SUBGROUPS

Tues. Oct 01 '13

Section 2.1: Definition & Examples of Subgroups

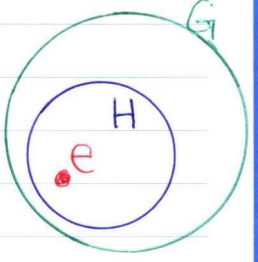
Def: Let G be a group. A subset $H \subseteq G$ is a **SUBGROUP** of G if H is a group under the binary operation of G. ← Denoted $H \leq G$

a.) Since H inherits associativity from G, we confirm...

1.) **NONEMPTINESS:** $H \neq \emptyset$

2.) **CLOSURE:** $\forall\, a, b \in H,\ ab \in H$

3.) **INVERSES:** $\forall\, a \in H,\ a^{-1} \in H$



b.) Properties (1), (2), & (3) imply $e \in H$.

Pf: Assume (1), (2), & (3)

$\Rightarrow \exists\, x, y \in H$ By (1)

$\Rightarrow x^{-1} \in H$ By (3)

$\Rightarrow e = xx^{-1} \in H$ By (2) ▨

c.) Properties (2) & (3) together form the Subgroup Criterion.

Thm (SUBGROUP CRITERION): Let $H \subseteq G$. Then $H \leq G$ iff the following hold:

1.) $H \neq \emptyset$

2.) $\forall\, x, y \in H,\ xy^{-1} \in H$

Pf ($\Rightarrow$): Assume $H \leq G$

a.) $H \neq \emptyset$, since $e \in H$ (cIdentity)

b.) Let $x, y \in H$ By (a)

$\Rightarrow y^{-1} \in H$ (cInverses)

$\Rightarrow xy^{-1} \in H$ ▨ (cClosure)

Pf ($\Leftarrow$): Assume Properties (1) & (2) hold.

a.) H is Associative $\because$ G is associative.

b.) Let $x \in H$, since $H \neq \emptyset$ By (1)

$\Rightarrow xe = xx^{-1} \in H$ By (2)

c.) Let $x \in H$ By (1)

$\Rightarrow x^{-1} = ex^{-1} \in H$ By (2) & (b)

d.) Let $x, y \in H$ By (1)

$\Rightarrow y^{-1} \in H$ By (c)

$\Rightarrow xy = x(y^{-1})^{-1} \in H$ By (2)

$\therefore H \leq G$ ▨

M® MIQUELRIUS

Ex.) $D_6 = \{1, r, r^2, s, sr, sr^2\}$, $H = \{1, r, r^2\} \leq D_6$

Confirm $H \leq D_6$ by making a Group Table.

H	1	r	r^2
1	1	r	r^2
r	r	r^2	1
r^2	r^2	1	r

1.) $H \neq \emptyset$

2.) H is closed under $\circ$

3.) $1^{-1} = 1$, $(r^2)^{-1} = r$, $r^{-1} = r^2$

$\therefore H \leq D_6$

↖ cln fact $H \cong \mathbb{Z}_3$

Ex.) $D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$, $H = \{1, r^2, s, sr^2\} \leq D_8$

H	1	r^2	s	sr^2
1	1	r^2	s	sr^2
r^2	r^2	1	sr^2	s
s	s	sr^2	1	r^2
sr^2	sr^2	s	r^2	1

1.) $H \neq \emptyset$

2.) H is closed under $\circ$

3.) $1^{-1} = 1$, $(r^2)^{-1} = r^2$, $s^{-1} = s$, $(sr^2)^{-1} = sr^2$

$\therefore H \leq D_8$

↖ cln fact, $H \cong \mathbb{Z}_2 \times \mathbb{Z} \cong V$

NOTE: H is actually ABELIAN, even though D_8 is not!

FACT: Every group G has AT LEAST 2 subgroups.

1.) TRIVIAL: $H = \{e\} \leq G$

2.) IMPROPER: $H = G \leq G$

M® MIQUELRIUS

Thurs. Oct03 '13

Section 2.2 Centralizers, Normalizers, Stabilizers, & Kernels

Def: Let G be a group & let $A \subseteq G$ be nonempty. Then the **CENTRALIZER** of A in G is defined by...

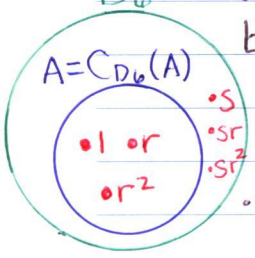
CONJUGATION BY g

$$C_G(A) = \{g \in G : ga = ag \ \forall a \in A\} = \{g \in G : gag^{-1} = a \ \forall a \in A\}$$

↑ Take all $g \in G$ that COMMUTE w/ ALL $a \in A$

Ex.) $G = D_6 = \{1, r, r^2, s, sr, sr^2\}$. $A = \{1, r, r^2\}$

D_6



a.) $r^i r^j = r^{i+j} = r^{j+i} = r^j r^i$, so $r^i \in C_{D_6}(A) \ \forall \ 0 \le i \le 2$

b.) $(sr^i)r(sr^i)^{-1} = sr^i r sr^i = sr^{i+1}sr^i = r^{-1} \neq r$

$\Rightarrow sr^i$ does NOT commute w/ $r \in A$ for any $0 \le i \le 2$

$\Rightarrow sr^i \notin C_{D_6}(A)$

$\therefore C_{D_6}(A) = \{1, r, r^2\} = A$

FACTS: For any group G & nonempty $A \subseteq G$...

a.) $e \in C_G(A)$

Pf: Let $a \in A$

$\Rightarrow eae^{-1} = eae = a$

$\Rightarrow e \in C_G(A)$ ▨

b.) $C_G(A) \le G$

Pf: Let $a \in A$

i.) $e \in C_G(A)$, so $C_G(A) \neq \emptyset$ By (a)

ii.) Let $x, y \in C_G(A)$

$\Rightarrow xax^{-1} = a \ \wedge \ yay^{-1} = a$

$\Rightarrow y^{-1}(yay^{-1})y = y^{-1}ay$

$\Rightarrow a = y^{-1}ay$

$\Rightarrow (xy^{-1})a(xy^{-1})^{-1} = xy^{-1}ayx^{-1} = xax^{-1} = a$ (a)

$\Rightarrow xy^{-1} \in C_G(A)$ ▨

c.) If G is Abelian, then $C_G(A) = G$

Pf: Let G be Abelian. Let $g \in G$

$\Rightarrow gag^{-1} = gg^{-1}a = a \ \forall a \in A$

$\Rightarrow g \in C_G(A)$

$\Rightarrow G \subseteq C_G(A)$

$\Rightarrow G = C_G(A)$ ▨ By (b)

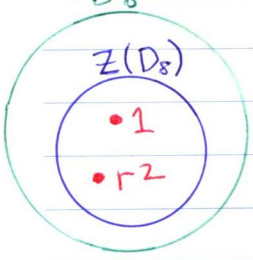
M® MIQUELRIUS

Def: Let G be a group. The **CENTER** of G is defined by...

$$Z(G) = \{g \in G : gh = hg \ \forall h \in G\}$$

↖ Take all $g \in G$ that COMMUTE w/ ALL $h \in G$.

Ex.) $G = D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$



a.) $(sr^i)r = sr^{i+1} \neq sr^{i-1} = sr^{-1}r^i = r(sr^i)$ for $0 \leq i \leq 3$

b.) $(r^i)s = sr^{-i} \neq s(r^i)$ if $i \neq 2$

c.) $(r^2)r^i = r^{2+i} = r^{i+2} = r^i(r^2)$

& $(r^2)sr^i = sr^{-2}r^i = sr^{-2+i} = sr^{i-2} = sr^i r^{-2} = sr^i(r^2)$

for $0 \leq i \leq 3$

d.) $1\sigma = \sigma 1 \ \forall \sigma \in D_8$

$\therefore Z(D_8) = \{1, r^2\}$ (In fact, $Z(D_{2n}) = \{1, r^{n/2}\}$ for even n.)

FACT: Let G be a group.

a.) $e \in Z(G)$

Pf: Let $g \in G$

$\Rightarrow eg = g = ge$, so $e \in Z(G)$ ▨

b.) $Z(G) \leq G$

Pf: $Z(G) = C_G(G) \leq G$ ▨

c.) If G is Abelian, then $G = Z(G)$

Pf: Let G be Abelian. Let $g \in G$

$\Rightarrow gh = hg \ \forall h \in G$

$\Rightarrow g \in Z(G)$

$\Rightarrow G \subseteq Z(G)$

$\Rightarrow G = Z(G)$ ▨ By (b)

d.) $Z(G)$ is ALWAYS Abelian.

Pf: Let $g, h \in Z(G)$

$\Rightarrow gh = hg$

$\Rightarrow Z(G)$ is Abelian. ▨

e.) $Z(G) \leq C_G(A)$ for any $A \subseteq G$

Pf: Let $x \in Z(G)$

$\Rightarrow xa = ax \ \forall a \in A$ Since $A \subseteq G$

$\Rightarrow x \in C_G(A)$

$\Rightarrow Z(G) \leq C_G(A)$ ▨ Since $Z(G)$ is a Group.

MIQUELRIUS

Def: Let G be a group & let $A \subseteq G$ be non-empty. Then the **NORMALIZER** of A in G is defined by...

$$N_G(A) = \{g \in G : gAg^{-1} = A\}, \text{ where } gAg^{-1} = \{gag^{-1} : a \in A\}$$

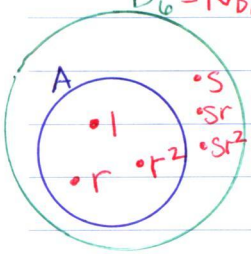
CAUTION: Not the same as $C_G(A)$ — CONJUGATE by g — g is FIXED

STRATEGY: For a fixed $g \in G$, define $\phi_g : A \to G$ by $\phi_g(a) = gag^{-1}$ ("conjugate each $a \in A$ by g") to see if $g \in N_G(A)$.

$\phi_g(A) = A \iff g \in N_G(A)$

Ex.) $G = D_6 = \{1, r, r^2, s, sr, sr^2\}$. Let $A = \{1, r, r^2\}$

$D_6 = N_{D_6}(A)$

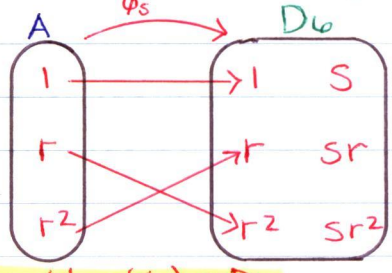


$\phi_s(1) = s(1)s^{-1} = 1$

$\phi_s(r) = s(r)s^{-1} = r^{-1} = r^2$

$\phi_s(r^2) = s(r^2)s^{-1} = r^{-2} = r$

$\therefore sAs^{-1} = A$, so $s \in N_{D_6}(A)$



↑ In fact, $N_{D_6}(A) = D_6$

FACTS: For any group G & any nonempty $A \subseteq G$...

a.) $e \in N_G(A)$

Pf: Let $a \in A$

$\Rightarrow eae^{-1} = eae = a$

$\Rightarrow eAe^{-1} = A$, so $e \in N_G(A)$ ▨

b.) $N_G(A) \leq G$

Pf: i.) $e \in N_G(A)$, so $N_G(A) \neq \emptyset$ By (a)

ii.) Let $x, y \in N_G(A)$

$\Rightarrow xAx^{-1} = A \wedge yAy^{-1} = A$

$\Rightarrow y^{-1}(yAy^{-1})y = y^{-1}Ay$

$\Rightarrow A = y^{-1}Ay$

$\Rightarrow (xy^{-1})A(xy^{-1})^{-1} = (xy^{-1})A(yx^{-1}) = xAx^{-1} = A$

$\Rightarrow xy^{-1} \in N_G(A)$ ▨

c.) If G is Abelian, then $N_G(A) = G$

Pf: Let G be Abelian. Let $g \in G$

$\Rightarrow gag^{-1} = gg^{-1}a = a \ \forall \ a \in A$

$\Rightarrow gAg^{-1} = A$

$\Rightarrow g \in N_G(A)$

$\Rightarrow G \subseteq N_G(A)$

$\Rightarrow G = N_G(A)$ ▨ By (b)

MIQUELRIUS

d.) $C_G(A) \leq N_G(A) \leq G$

Pf: From (b), we know $N_G(A) \leq G$

CLAIM: $C_G(A) \subseteq N_G(A)$

Pf: Let $x \in C_G(A)$

$\Rightarrow xax^{-1} = a \quad \forall\, a \in A$

$\Rightarrow xAx^{-1} = A$

$\Rightarrow x \in N_G(A)$

By the Claim, since $C_G(A)$ & $N_G(A)$ are groups (Proven Earlier) under the same operation, we have $C_G(A) \leq N_G(A)$

$\therefore C_G(A) \leq N_G(A) \leq G$ ▨

Def: Suppose group G acts on set A. Let $a \in A$.

1.) The **STABILIZER** of a in G is the set

$$G_a = \{g \in G : g \cdot a = a\}$$

FACT: $G_a \leq G$

Pf: Let $a \in A$

i.) $1 \in G_a$, since $1 \cdot a = a$

ii.) Let $x, y \in G_a$

$\Rightarrow x \cdot a = a \;\wedge\; y \cdot a = a$

$\Rightarrow a = 1 \cdot a = (y^{-1}y) \cdot a = y^{-1} \cdot (y \cdot a) = y^{-1} \cdot a$

$\Rightarrow (xy^{-1}) \cdot a = x \cdot (y^{-1} \cdot a) = x \cdot a = a$

$\Rightarrow xy^{-1} \in G_a$ ▨

2.) The **ORBIT** of a in G is $G \cdot a = \{g \cdot a : g \in G\}$

Ex.) $G = S_3$, $A = X_3 = \{1, 2, 3\}$, $\sigma \cdot i = \sigma(i)$.

$$(S_3)_1 = \{\sigma \in S_3 : \sigma \cdot 1 = 1\} = \{e, (2,3)\}$$

$$S_3 \cdot 1 = \{e \cdot 1, (1,2) \cdot 1, (2,3) \cdot 1, (1,3) \cdot 1, (1,2,3) \cdot 1, (1,3,2) \cdot 1\}$$
$$= \{1, 2, 1, 3, 2, 3\}$$
$$= X_3$$

MIQUELRIUS

Ex.) $G = D_6 = \{1, r, r^2, s, sr, sr^2\}$ acts on itself by conjugation.

a.) $1 \cdot r = 1r1^{-1} = r$ $\quad s \cdot r = srs^{-1} = r^2$

$r \cdot r = rrr^{-1} = r$ $\quad (sr) \cdot r = (sr)r(sr)^{-1} = r^2$

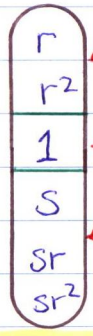
$r^2 \cdot r = r^2rr^{-2} = r$ $\quad (sr^2) \cdot r = (sr^2)r(sr^2)^{-1} = r^2$

$\therefore (D_6)_r = \{1, r, r^2\}$

b.) $D_6 \cdot r = \{1 \cdot r, r \cdot r, r^2 \cdot r, s \cdot r, (sr) \cdot r, (sr^2) \cdot r\}$

$= \{r, r, r, r^2, r^2, r^2\}$

$= \{r, r^2\}$



$D_6 \cdot 1 = \{1\}$

$D_6 \cdot s = \{1 \cdot r, r \cdot s, r^2 \cdot s, s \cdot s, (sr) \cdot s, (sr^2) \cdot s\}$

$= \{s, sr, sr^2, s, sr^2, sr\}$

$= \{s, sr, sr^2\}$

NOTE: The orbits PARTITION D_6!

M® MIQUELRIUS

Tues. Oct 08 '13

Section 2.3 Cyclic Groups

Def: Let G be a group. Let $a \in G$.

1.) The **CYCLIC SUBGROUP** generated by a is

$$\langle a \rangle = \{a^n : n \in \mathbb{Z}\} = \{\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots\}$$

2.) We say G is cyclic if $\exists\, a \in G$ s.t. $G = \langle a \rangle$.
- The **GENERATOR** of G is a.

FACTS: Let $a \in G$

a.) $\langle a \rangle \leq G$

Pf: i.) $e = a^0 \in \langle a \rangle$

ii.) Let $x, y \in G$

$\Rightarrow x = a^n \wedge y = a^m$ f.s. $m, n \in \mathbb{Z}$

$\Rightarrow y^{-1} = (a^m)^{-1} = a^{-m} \in \langle a \rangle$

$\Rightarrow xy^{-1} = a^n a^{-m} = a^{n-m} \in \langle a \rangle$ ▨

b.) $\langle a \rangle = \langle a^{-1} \rangle$

Pf: $\langle a \rangle = \{\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots\}$

$= \{\ldots, a^2, a, e, a^{-1}, a^{-2}, \ldots\}$

$= \{\ldots, (a^{-1})^{-2}, (a^{-1})^{-1}, e, a^{-1}, (a^{-1})^2, \ldots\} = \langle a^{-1} \rangle$ ▨

c.) Every cyclic group is Abelian.

Pf: Let G be cyclic, & let $x, y \in G$.

$\Rightarrow \exists\, a \in G$ s.t. $G = \langle a \rangle$

$\Rightarrow x = a^k \wedge y = a^l$ f.s. $k, l \in \mathbb{Z}$

$\Rightarrow xy = a^k a^l = a^{k+l} = a^{l+k} = a^l a^k = yx$ ▨

Ex.) $\mathbb{Z}$ is Cyclic.

$$\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$
$$2\mathbb{Z} = \langle 2 \rangle = \langle -2 \rangle = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$$

Ex.) $\mathbb{Z}_n$ is Cyclic.

$$\mathbb{Z}_n = \langle \bar{1} \rangle = \langle \overline{n-1} \rangle = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$$

FACT: $\mathbb{Z}_n = \langle \bar{a} \rangle$ iff $\gcd(a, n) = 1$, since $|\bar{a}| = \dfrac{n}{\gcd(a, n)}$

M® MIQUELRIUS

DIVISION ALGORITHM: Let $a, b \in \mathbb{Z}$ w/ $b > 0$. Then $\exists!\ q, r \in \mathbb{Z}$ s.t. $a = bq + r$, where $0 \leq r < b$.

Thm: Any subgroup of a Cyclic Group is Cyclic.

Pf: Assume G is cyclic & let $H \leq G$.

$\Rightarrow \exists\ a \in G$ s.t. $G = \langle a \rangle$

TRIVIAL CASE: $H = \{e\} = \langle e \rangle$ is Cyclic.

CASE 2: $H \neq \{e\}$

$\Rightarrow \exists\ x \in H$ s.t. $x \neq e$

$\Rightarrow x = a^k$ f.s. $k \in \mathbb{Z}^*$

Since $x^{-1} = a^{-k} \in H$, $\exists$ a positive power of a in H. Let m be the smallest positive power of a in H, so $a^m \in H$.

CLAIM: $H = \langle a^m \rangle$

Pf ($\supseteq$): $\langle a^m \rangle = \{\ldots, a^{-2m}, a^{-m}, e, a^m, a^{2m}, \ldots\} \subseteq H$, since $a^m \in H$ & H is closed under inversion.

Pf ($\subseteq$): Let $h \in H$

$\Rightarrow h = a^l$ f.s. $l \in \mathbb{Z}$, since $h \in G$

Divide m into l w/ the Division Algorithm, so $\exists!\ q, r \in \mathbb{Z}$ s.t. $l = mq + r$, where $0 \leq r < m$.

$\Rightarrow a^l = a^{mq+r} = (a^m)^q a^r$

$\Rightarrow a^r = a^l (a^m)^{-q} \in H$, since $a^l, (a^m)^{-q} \in H$

If $r \neq 0$, then r would be a positive power of a & $r < m$, which is impossible. So $r = 0$.

$\Rightarrow h = a^l = (a^m)^q \in \langle a^m \rangle$

$\therefore H = \langle a^m \rangle$ ▨

Ex.) $\mathbb{Z}$ is Cyclic, so $H \leq \mathbb{Z}$ is Cyclic also.

$\langle n \rangle = \{\ldots, -2n, -n, 0, n, 2n, \ldots\} = n\mathbb{Z}$, $n \in \mathbb{N}$

$\langle 0 \rangle = \{0\}$

$\langle 1 \rangle = \{\ldots, -2, -1, 0, 1, 2, \ldots\} = \mathbb{Z}$

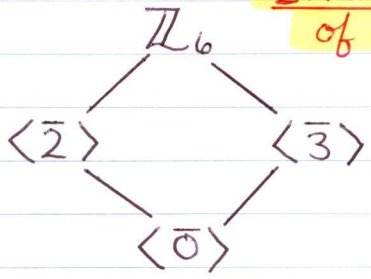
NOTE: These are the only possibilities.

MIQUELRIUS

Ex.) Find all subgroups of $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

$\langle \bar{0} \rangle = \{\bar{0}\}$
$\langle \bar{1} \rangle = \langle \bar{5} \rangle = \mathbb{Z}_6$
$\langle \bar{2} \rangle = \langle \bar{4} \rangle = \{\bar{0}, \bar{2}, \bar{4}\}$
$\langle \bar{3} \rangle = \{\bar{0}, \bar{3}\}$

LATTICE of $\mathbb{Z}_6$



Lemma: Let G be a group & $a \in G$.

a.) If $|a| = n < \infty$, then $\langle a \rangle = \{e, a, \ldots, a^{n-1}\}$
  i.) $a^h \neq a^k$ if $0 \leq h < k \leq n-1$
  ii.) $|\langle a \rangle| = n$

b.) If $|a| = \infty$, then $\langle a \rangle = \{\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots\}$
  i.) $a^h \neq a^k$ if $h \neq k$
  ii.) $|\langle a \rangle| = \infty$

Pf: Let $x \in G$

a.) FINITE CASE: Let $S = \{e, x, x^2, \ldots, x^{n-1}\}$
  i.) $S \subseteq \langle x \rangle = \{x^l : l \in \mathbb{Z}\}$
  ii.) Let $x^m \in \langle x \rangle$, where $m \in \mathbb{Z}$
    Divide n into m. By the Division Algorithm,
    $\exists!\ q, r \in \mathbb{Z}$ s.t. $m = nq + r$ s.t. $0 \leq r < n$.
    $\Rightarrow x^m = x^{nq+r} = (x^n)^q x^r = e^q x^r = x^r \in S$, since $0 \leq r < n$.
    $\Rightarrow \langle x \rangle \subseteq S$
  $\therefore \langle x \rangle = S$
  iii.) Assume $x^h = x^k$, where $0 \leq h < k \leq n-1$
    $\Rightarrow x^{k-h} = x^k x^{-h} = x^h x^{-h} = e$
    $\Rightarrow |x| < n$, since $0 < k-h < n$ ⊛
    $\therefore x^h \neq x^k$ ▨

b.) INFINITE CASE: Let $S = \{\ldots, x^{-2}, x^{-1}, e, x, x^2, \ldots\}$
  i.) By def., $\langle x \rangle = \{x^l : l \in \mathbb{Z}\} = \{\ldots, x^{-2}, x^{-1}, e, x, x^2, \ldots\}$
  $\therefore \langle x \rangle = S$
  ii.) Assume $x^h = x^k$ where $h < k$
    $\Rightarrow x^{k-h} = x^k x^{-h} = x^h x^{-h} = e$
    $\Rightarrow |x| < \infty$, since $k-h < \infty$ ⊛
    $\therefore x^h \neq x^k$ ▨

MIQUELRIUS

FACT: Suppose $|x| = n$ & $x^m = e$ w/ $m > 0$. Then $n \mid m$.

Thm: Let G be cyclic.

1.) If $|G| = \infty$, then $G \cong \mathbb{Z}$

Pf: Assume $G = \langle x \rangle = \{\ldots, x^{-2}, x^{-1}, e, x, x^2, \ldots\}$ is infinite.

$\Rightarrow x^h \neq x^k$ if $h \neq k$ ← By the Lemma.

Define $\phi: G \to \mathbb{Z}$ by $\phi(x^a) = a$.

$\Rightarrow \phi$ is 1-1, Onto, & Well-Defined ← By the Lemma

Let $x^a, x^b \in G$

$\Rightarrow \phi(x^a x^b) = \phi(x^{a+b}) = a + b = \phi(x^a) + \phi(x^b)$ ▨

2.) If $|G| = n < \infty$, then $G \cong \mathbb{Z}_n$

Pf: Assume $G = \langle x \rangle = \{e, x, x^2, \ldots, x^{n-1}\}$ is finite, where $|x| = n$

$\Rightarrow x^h \neq x^k$ if $0 \leq h < k \leq n-1$ ← By the Lemma.

Define $\phi: G \to \mathbb{Z}_n$ by $\phi(x^a) = \overline{a}$

CLAIM: ϕ is Well-Defined

Pf: Suppose $x^h = x^k$ w/ $h < k$

$\Rightarrow x^{k-h} = e$

$\Rightarrow n \mid k-h$

$\Rightarrow k - h = nk$ f.s. $k \in \mathbb{Z}$

$\Rightarrow k \equiv h \pmod{n}$

$\Rightarrow \overline{k} = \overline{h}$

$\Rightarrow \phi(x^h) = \phi(x^k)$

So ϕ is Well-Defined, 1-1, & Onto ← By Claim + Lemma

Let $x^a, x^b \in G$, where, $a, b \in G$

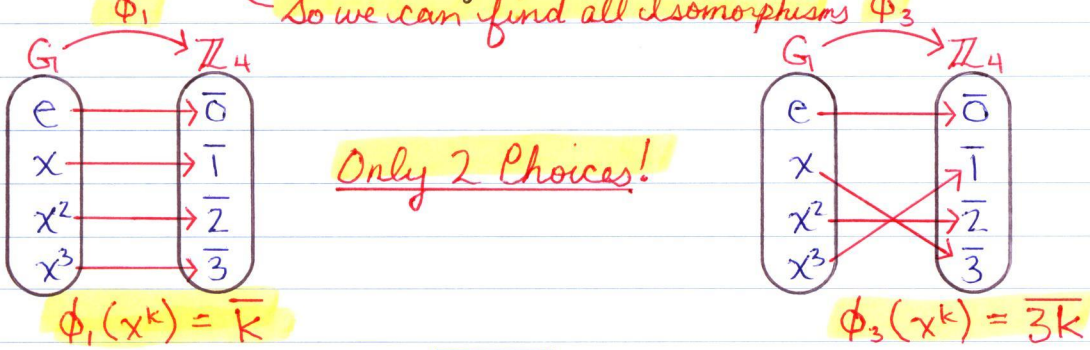
$\Rightarrow \phi(x^a x^b) = \phi(x^{a+b}) = \overline{a+b} = \overline{a} + \overline{b} = \phi(x^a) + \phi(x^b)$

↖ Well-Defined. ▨

FACT: If $\phi: G \to \mathbb{Z}_n$ where $G = \{e, x, \ldots, x^{n-1}\}$ is an isomorphism, then $\phi(x^k) = \overline{ka}$, where $\gcd(a, n) = 1$.

↖ So we can find all isomorphisms ϕ_3

Ex.)



MIQUELRIUS

Prop: Let G be a group & let $x \in G$ have finite order n. Then $|x^a| = \frac{n}{\gcd(a,n)}$, where $a \geq 0$.

Prop: Suppose $G = \langle x \rangle$, where $|x| = n$. Then $G = \langle y \rangle$ iff $y = x^a$ w/ $\gcd(a,n) = 1$, where $1 \leq a \leq n-1$.

Pf (1): Assume $|x| = n \wedge x^m = 1$
$\Rightarrow \exists r, s \in \mathbb{Z}$ s.t. $d = mr + ns$, where $d = \gcd(m,n)$ by Euclidean Algorithm
$\Rightarrow x^d = x^{mr+ns} = (x^m)^r (x^n)^s = 1^r 1^s = 1$
$\Rightarrow n = d$ $\because 1 \leq d \leq n$ & n = Least Positive Integer s.t. $x^n = 1$
$\Rightarrow n | m$ ▨

Pf (2): Assume $|x| = n$. Let $y = x^a$ & $d = \gcd(a,n)$.
$\Rightarrow d | n \wedge d | a$
Let $b = \frac{n}{d} \wedge c = \frac{a}{d}$. NOTE: $b > 0$ $\because n > 0 \wedge d > 0$
$\Rightarrow \gcd(b,c) = \gcd(\frac{n}{d}, \frac{a}{d}) = 1$

CLAIM 1: $|y| | b$
Pf: $y^b = (x^a)^b = (x^{dc})^b = (x^{db})^c = (x^n)^c = 1^c = 1$
$\Rightarrow |y| | b$ By (1)

CLAIM 2: $b | |y|$
Pf: Let $k = |y|$
$\Rightarrow x^{ak} = y^k = 1$
$\Rightarrow n | ak$ By (1)
$\Rightarrow db | dck$
$\Rightarrow b | ck$
$\Rightarrow b | k$ $\because \gcd(b,c) = 1$, so $b | |y|$

$\therefore |x^a| = |y| = k = b = \frac{n}{d} = \frac{n}{\gcd(a,n)}$ ▨
↖ $\because b, k > 0$ & divide each other

COROLLARY: $|\bar{a}| = \frac{n}{\gcd(a,n)}$ in $\mathbb{Z}_n$
Pf: $|\bar{1}| = n$, so $|\bar{a}| = |\underbrace{\bar{1} + \bar{1} + \ldots + \bar{1}}_{a}| = \frac{n}{\gcd(a,n)}$ ▨

Pf (3): Suppose $|x| = n \wedge \langle x \rangle = G$
Then $G = \langle x^a \rangle$ (for $1 \leq a \leq n-1$)
$\Leftrightarrow |x^a| = n$
$\Leftrightarrow \frac{n}{\gcd(a,n)} = n$
$\Leftrightarrow \gcd(a,n) = 1$ ▨

MIQUELRIUS

Thurs. Oct 10 '13

Section 2.4 Generating Sets

Def: Let G be a group, & let $a_1, a_2, \ldots, a_n \in G$. Then the **SUBGROUP OF G GENERATED BY $a_1, \ldots, a_n$** is

$$\langle a_1, a_2, \ldots, a_n \rangle = \left\{ a_{i_1}^{\varepsilon_1} a_{i_2}^{\varepsilon_2} \cdots a_{i_n}^{\varepsilon_n} : 1 \le i_1, \ldots, i_k \le n,\ \varepsilon_1, \ldots, \varepsilon_k \in \mathbb{Z} \right\}$$

We say G is **FINITELY GENERATED** if $\exists\, a_1, \ldots, a_n \in G$ s.t. $G = \langle a_1, a_2, \ldots, a_n \rangle$.

Ex.) $\{a_1^5 a_2^3 a_3^{-1000},\ a_1 a_2 a_1^{-1}\} \subseteq \langle a_1, a_2, a_3 \rangle$

Ex.) $D_{2n} = \langle r, s \rangle$ but not cyclic.

M® MIQUELRIUS

Ch 3: QUOTIENT GROUPS & HOMOMORPHISMS

Tues. Oct 15 '13

Section 3.1 Definitions & Examples (Kernels & Cosets)

Def: Let $\phi: G \to H$ be a homomorphism.

1.) The **KERNEL** of ϕ is $\ker(\phi) = \{g \in G : \phi(g) = 1_H\}$

2.) The **IMAGE** of ϕ is $\text{im}(\phi) = \phi(G) = \{\phi(g) : g \in G\}$

CREATING HOMOMORPHISMS: Define $\phi: \mathbb{Z}_n \to G$ by...

1.) $\phi(\bar{1}) = x$, where $|x| \mid n$.

2.) $\phi(\bar{a}) = x^a \quad \forall\, \bar{a} \in \mathbb{Z}_n$

Then ϕ is a Homomorphism.

NOTE: For $\phi: \mathbb{Z} \to G$, map 1 to ANY $x \in G$.

Pf: Define $\phi: \mathbb{Z}_n \to G$ by $\phi(\bar{a}) = x^a$, where $|x| \mid n$.

a.) Let $\bar{a} = \bar{b}$

$\Rightarrow a \equiv b \pmod n$

$\Rightarrow a = kn + b$ f.s. $k \in \mathbb{Z}$

$\because n = m|x|$ f.s. $m \in \mathbb{Z}^+$ $\Rightarrow x^a = x^{kn+b} = x^{nk}x^b = x^b$

$\Rightarrow \phi(\bar{a}) = \phi(\bar{b})$

b.) Let $\bar{a}, \bar{b} \in \mathbb{Z}_n$

$\Rightarrow \phi(\bar{a} + \bar{b})$

$= \phi(\overline{a+b})$

$= x^{a+b}$

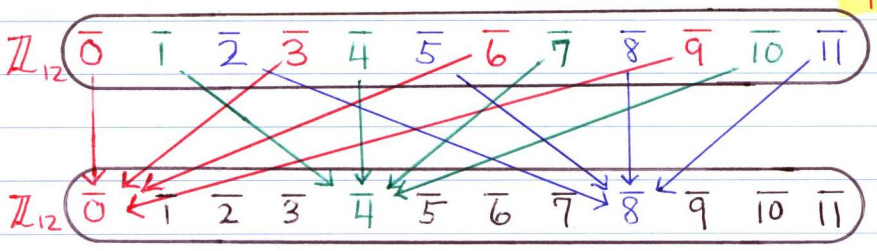
$= x^a x^b$

$= \phi(\bar{a})\phi(\bar{b})$

$\therefore \phi$ is Well-Defined & a Homomorphism. ▨

GENERAL CASE: $\phi: \mathbb{Z}_n \to \mathbb{Z}_n$ where $\phi(\bar{a}) = \overline{ax}$ if $|\bar{x}| \mid n$.

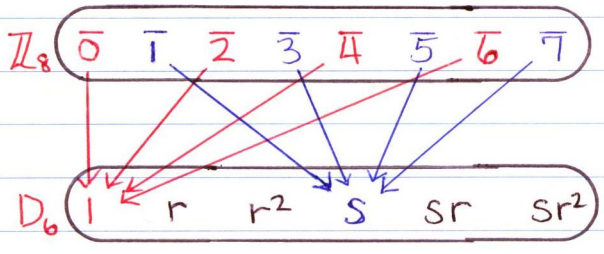
Ex.) $\phi: \mathbb{Z}_{12} \to \mathbb{Z}_{12}$, where $\phi(\bar{1}) = \bar{4}$ ($|\bar{4}| = 3$)



$\ker(\phi) = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$

$\text{im}(\phi) = \{\bar{0}, \bar{4}, \bar{8}\}$

Ex.) $\phi: \mathbb{Z}_8 \to D_6$, where $\phi(\bar{1}) = s$ ($|s| = 2$)



$\ker(\phi) = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$

$\text{im}(\phi) = \{1, s\}$

Thm: If $\phi: G \to H$ is a Homomorphism & $x \in G$, then $|\phi(x)| \mid |x|$.

Pf: For $x \in G$, $1_H = \phi(1_G) = \phi(x^{|x|}) = \phi(x)^{|x|}$

$\Rightarrow |\phi(x)| \mid |x|$ ▨ (also, $|\phi(x)| \mid |G|$ by Lagrange)

M® MIQUELRIUS

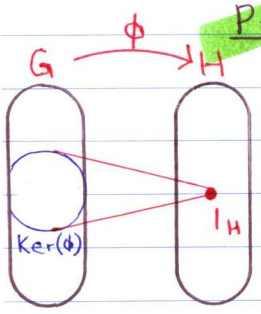
FACTS: Let $\phi: G \to H$ be a Group Homomorphism.

1.) $\phi(x^n) = \phi(x)^n \quad \forall x \in G,\ n \in \mathbb{Z}$ ← Proven in 1.6

a.) $\phi(1_G) = 1_H$

b.) $\phi(x^{-1}) = \phi(x)^{-1} \quad \forall x \in G$

2.) $Ker(\phi) \leq G$

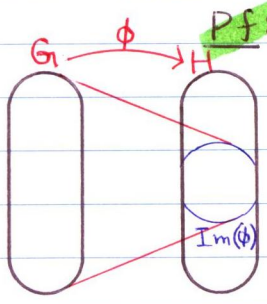


Pf: a.) $\phi(1_G) = 1_H$
$\Rightarrow 1_G \in Ker(\phi)$
$\Rightarrow Ker(\phi) \neq \emptyset$

b.) Let $x, y \in Ker(\phi)$
$\Rightarrow \phi(x) = 1_H \wedge \phi(y) = 1_H$
$\Rightarrow \phi(xy^{-1}) = \phi(x)\phi(y^{-1}) = \phi(x)\phi(y)^{-1} = 1_H 1_H^{-1} = 1_H$
$\Rightarrow xy^{-1} \in Ker(\phi)$

$\therefore Ker(\phi) \leq G$ ▨

3.) $Im(\phi) \leq H$



Pf: a.) $1_H = \phi(1_G) \in Im(\phi)$
$\Rightarrow Im(\phi) \neq \emptyset$

b.) Let $h, k \in Im(\phi)$
$\Rightarrow \exists\, x, y \in G$ s.t. $\phi(x) = h \wedge \phi(y) = k$
$\Rightarrow hk^{-1} = \phi(x)\phi(y)^{-1} = \phi(x)\phi(y^{-1}) = \phi(xy^{-1}) \in Im(\phi)$

$\therefore Im(\phi) \leq H$ ▨

4.) If H is finite, then $|\phi(x)| \,||\, |H| \quad \forall x \in G$

Pf: Assume H is finite. Let $x \in G$
$\Rightarrow |\phi(x)| = n$ is finite
$\Rightarrow \langle \phi(x) \rangle = \{1_H, \phi(x), \phi(x)^2, \ldots, \phi(x)^{n-1}\} \leq H$
$\Rightarrow |\langle \phi(x) \rangle| = n = |\phi(x)|$
$\Rightarrow |\phi(x)| \,||\, |H|$ by Lagrange's Thm ▨

Def: Let $H \leq G$ & $a, b \in G$

1.) a is **RIGHT CONGRUENT** to b Modulo H if $ab^{-1} \in H$.
Notation: $a \equiv_r b \pmod{H}$

2.) a is **LEFT CONGRUENT** to b Modulo H if $a^{-1}b \in H$
Notation: $a \equiv_\ell b \pmod{H}$

M® MIQUELRIUS

Thm: Let $H \leq G$

1.) Right & left congruence modulo H are equivalence relations on G.

Pf (R): Let $H \leq G$

a.) REFLEXIVE: Let $a \in G$

$\Rightarrow aa^{-1} = 1_G \in H$

$\Rightarrow a \equiv_r a \pmod{H}$

b.) SYMMETRIC: Assume $a \equiv_r b \pmod{H}$

$\Rightarrow ab^{-1} = h$ f.s. $h \in H$

$\Rightarrow ba^{-1} = (ab^{-1})^{-1} = h^{-1} \in H$

$\Rightarrow b \equiv_r a \pmod{H}$

c.) TRANSITIVE: Assume $a \equiv_r b \pmod{H} \wedge b \equiv_r c \pmod{H}$

$\Rightarrow ab^{-1} = h_1 \wedge bc^{-1} = h_2$ f.s. $h_1, h_2 \in H$

$\Rightarrow a = h_1 b \wedge c^{-1} = b^{-1} h_2$

$\Rightarrow ac^{-1} = h_1 b b^{-1} h_2 = h_1 h_2 \in H$

$\Rightarrow a \equiv_r c \pmod{H}$ ▨ (Proven similarly for Left Congruence)

2.) The equivalence classes of $a \in H$ are COSETS of H.

a.) RIGHT COSET: $Ha = \{ha : h \in H\}$ under Right Congruence.

b.) LEFT COSET: $aH = \{ah : h \in H\}$ under Left Congruence.

Pf (L): $\bar{a} = \{b \in G : a \equiv_\ell b \pmod{H}\}$

$= \{b \in G : a^{-1}b \in H\}$

$= \{b \in G : a^{-1}b = h$ f.s. $h \in H\}$

$= \{b \in G : b = ah$ f.s. $h \in H\}$

$= \{ah : h \in H\} = aH$ ▨ (Proven Similarly for Right Cosets)

3.) $|Ha| = |H| = |aH| \ \forall a \in G$

Pf(L): Define $f : H \to aH$ by $f(h) = ah \ \forall h \in H$

a.) Assume $f(h_1) = f(h_2)$

$\Rightarrow ah_1 = ah_2$

$\Rightarrow h_1 = h_2$

$\therefore f$ is 1-1

b.) Let $k \in aH$

$\Rightarrow k = ah$ f.s. $h \in H$

$\Rightarrow f(h) = ah = k \in aH$

$\therefore f$ is Onto

$\therefore |H| = |aH|$ ▨ (Proven Similarly for Right Cosets) ← Equally!

COROLLARY: G is partitioned by its left (or right) cosets of H in G.

Pf: Equivalence Classes partition G. ▨

M® MIQUELRIUS

NOTATION: Let $H \leq G$

$G/H = \{aH : a \in G\}$ = The set of all left cosets of H in G.

$H\backslash G = \{Ha : a \in G\}$ = The set of all right cosets of H in G.

FACT: Let $H \leq G$ & $x, y \in G$. The following are equivalent.

a.) $xH = yH$
b.) $x^{-1}y \in H$
c.) $y^{-1}x \in H$
d.) $x \in yH$
e.) $y \in xH$

Ex.) $G = D_6 = \{1, r, r^2, s, sr, sr^2\}$, $H = \{1, s\}$

$H = \{1, s\} = sH$
$rH = \{r, sr^2\} = sr^2H$
$r^2H = \{r^2, sr\} = srH$
$D_6/H = \{H, rH, r^2H\}$

D_6	
1 s	H
r sr^2	rH
r^2 sr	r^2H

$H = \{1, s\} = Hs$
$Hr = \{r, sr\} = Hsr$
$Hr^2 = \{r^2, sr^2\} = Hsr^2$
$H\backslash D_6 = \{H, Hr, Hr^2\}$

D_6	
1 s	H
r sr	Hr
r^2 sr^2	Hr^2

NOTE: $rH = Hr$, $\therefore H \trianglelefteq D_6$ ← D_6 is Partitioned Evenly →

Def: Let $H \leq G$. If $gH = Hg$ $\forall g \in G$, then H is a **NORMAL SUBGROUP** of G, denoted $H \trianglelefteq G$.

Thm: Let $H \leq G$. The following are equivalent.

1.) $gH = Hg$ $\forall g \in G$
2.) $gHg^{-1} \subseteq H$ $\forall g \in G$
3.) $gHg^{-1} = H$ $\forall g \in G$

Pf (1) ⇒ (2): Assume $gH = Hg$ $\forall g \in G$. Let $a \in G$ & let $x \in aHa^{-1}$

$\Rightarrow x = aha^{-1}$ f.s. $h \in H$
$\Rightarrow ah \in aH = Ha$
$\Rightarrow ah = h'a$ f.s. $h' \in H$
$\Rightarrow x = aha^{-1} = h'aa^{-1} = h' \in H$, so $aHa^{-1} \subseteq H$ ▨

Pf (2) ⇒ (3): Assume $gHg^{-1} \subseteq H$ $\forall g \in G$. Let $a \in G$.

$\Rightarrow aHa^{-1} \subseteq H \wedge a^{-1}Ha \subseteq H$

Let $h \in H$

$\Rightarrow h = (aa^{-1})h(aa^{-1}) = a(a^{-1}ha)a^{-1}$

Since $a^{-1}Ha \subseteq H$, we know $a^{-1}ha = h'$ f.s. $h' \in H$

$\Rightarrow h = ah'a^{-1} \in aHa^{-1}$
$\Rightarrow H \subseteq aHa^{-1}$, so $H = aHa^{-1}$ ▨

M® MIQUELRIUS

Pf (3) $\Rightarrow$ (1): Assume $gHg^{-1} = H \ \forall g \in G$. Let $a \in G$

$\Rightarrow aHa^{-1} = H \ \wedge \ a^{-1}Ha = H$

($\subseteq$): Let $x \in aH$

$\Rightarrow x = ah$ f.s. $h \in H$

Since $aha^{-1} \in aHa^{-1} = H$, we know $aha^{-1} = h'$ f.s. $h' \in H$

$\Rightarrow ah = h'a$

$\Rightarrow x = ah = h'a \in Ha$, so $aH \subseteq Ha$

($\supseteq$): Let $y \in Ha$

$\Rightarrow y = ha$ f.s. $h \in H$

Since $a^{-1}ha \in a^{-1}Ha = H$, we know $a^{-1}ha = h'$ f.s. $h' \in H$

$\Rightarrow ha = ah'$

$\Rightarrow y = ha = ah' \in aH$, so $Ha \subseteq aH$

$\therefore aH = Ha$ ▨

PROP 5: Let $H \leq G$. The operation $(aH)(bH) = (ab)H$ is Well-Defined iff $H \trianglelefteq G$.

Pf ($\Rightarrow$): Assume Well-Defined. Let $a \in G \ \wedge \ h \in H$

$\Rightarrow 1H = hH \ \wedge \ a^{-1}H = a^{-1}H$ in G/H

$\Rightarrow (ha^{-1})H = (1a^{-1})H = a^{-1}H$

$\Rightarrow ha^{-1} \in (ha^{-1})H = a^{-1}H$

$\Rightarrow ha^{-1} = a^{-1}h'$ f.s. $h' \in H$

$\Rightarrow aha^{-1} = h' \in H$

$\Rightarrow aHa^{-1} \subseteq H$, so $H \trianglelefteq G$ ▨

Pf ($\Leftarrow$): Assume $H \trianglelefteq G$. Let $a_1, a_2 \in a_1H \ \wedge \ b_1, b_2 \in b_1H$

$\Rightarrow a_2 = a_1h_1 \ \wedge \ b_2 = b_1h_2$ f.s. $h_1, h_2 \in H$

$\Rightarrow a_2b_2 = (a_1h_1)(b_1h_2) = a_1(b_1b_1^{-1})h_1b_1h_2 = (a_1b_1)(b_1^{-1}h_1b_1)h_2$

$= (a_1b_1)h'h_2$ f.s. $h' \in H$

$\Rightarrow a_2b_2 \in (a_1b_1)H$, since $h'h_2 \in H$

$\Rightarrow (a_1b_1)H = (a_2b_2)H$

$\therefore$ The operation $(aH)(bH) = (ab)H$ is Well-Defined. ▨

NOTE: If $H \trianglelefteq G$, then G/H is a Group under this operation.

a.) $1_{G/H} = H$, since $(aH)(H) = (a1_G)H = aH$

b.) $(aH)^{-1} = a^{-1}H$, since $(aH)(a^{-1}H) = (aa^{-1})H = 1_GH = H$.

c.) $(aH)^{\alpha} = a^{\alpha}H \ \forall \alpha \in \mathbb{Z}$

d.) $|aH| \mid |a|$, where $|aH|$ is the order of aH in G/H.

M® MIQUELRIUS

Section 3.2 More on Cosets & Lagrange's Thm

Def: If $H \leq G$, then the **INDEX** of H in G (denoted $|G:H|$) is the number of left (or right) cosets of H in G.

Ex.) $|D_6 : \{1, s\}| = 3$

LAGRANGE'S THM: If G is finite & $H \leq G$, then $|G| = |G:H||H|$. In particular, $|H||G|$.

Pf: Let $H \leq G$, where G is finite. Let $r = |G:H|$
$\Rightarrow \exists\, g_1, g_2, \ldots, g_r \in G$ s.t. $G/H = \{g_1H, g_2H, \ldots, g_rH\}$
$\Rightarrow g_iH \cap g_jH = \emptyset$ if $i \neq j$ & $G = \bigcup_{i=1}^{r} g_iH$, since left cosets of H are equivalence classes of $\equiv_\ell$ on G.
$\Rightarrow |G| = \sum_{i=1}^{r} |g_iH| = \sum_{i=1}^{r} |H| = r|H| = |G:H||H|$, since $|g_iH| = |H|\ \forall i$

$\therefore |H||G|$ ▨

COROLLARY 1: If G is finite & $x \in G$, then $|x||G|$. Also, $x^{|G|} = 1_G$

Pf: Let $|x| = n$ in a finite group G.
$\Rightarrow \langle x \rangle = \{1_G, x, \ldots, x^{n-1}\}$ & $|\langle x \rangle| = n$ by the Lemma.
$\Rightarrow n||G|$ by Lagrange
$\Rightarrow |G| = nk$ f.s. $k \in \mathbb{Z}$
$\Rightarrow x^{|G|} = x^{nk} = (x^n)^k = 1_G^k = 1_G$ ▨

COROLLARY 2: Let G be a group of size p, where p is prime. Then G is Cyclic & $G \cong \mathbb{Z}_p$. Also, if $x \in G$ s.t. $x \neq 1_G$, then $G = \langle x \rangle$.

Pf: Suppose $|G| = p$ f.s. prime p.
$\Rightarrow p > 1$
$\Rightarrow \exists x \in G$ s.t. $x \neq 1_G$
$\Rightarrow |x| \geq 2$
By Corollary 1, $|x|p$, since $p = |G|$
$\Rightarrow |x| = p$, since $|x| \neq 1$
$\Rightarrow \langle x \rangle = \{1_G, x, \ldots, x^{p-1}\} = G$, since $|G| = p$
$\Rightarrow G \cong \mathbb{Z}_p$, since G is Cyclic of size p. ▨

MIQUELRIUS

FACTS: Let G be a group. Let $H \leq G$.

1.) If G is Abelian, then $H \trianglelefteq G$.

Pf: Let G be Abelian. Let $a \in G$

$\Rightarrow aH = \{ah : h \in H\} = \{ha : h \in H\} = Ha$

$\therefore H \trianglelefteq G$ ▨

2.) If $|G:H| = 2$, then $H \trianglelefteq G$

Pf: Assume $|G:H| = 2$. Let $a \in G$

CASE 1: $a \in H$

$\Rightarrow aH = H = Ha$, since $aH = H$ iff $a \in H$ iff $Ha = H$

CASE 2: $a \notin H$

$\Rightarrow aH \neq H \wedge Ha \neq H$

$\Rightarrow aH = Ha$, since G/H has only 2 elements

$\therefore H \trianglelefteq G$ ▨

3.) $Z(G) \trianglelefteq G$

Pf: Let $a \in G$

$\Rightarrow aZ(G) = \{az : z \in Z(G)\} = \{za : z \in Z(G)\} = Z(G)a$

$\therefore Z(G) \trianglelefteq G$ ▨

Ex.) Show $\mathbb{Z}_2 \times \mathbb{Z}_4 / \langle(\bar{0}, \bar{1})\rangle \cong \mathbb{Z}_2$

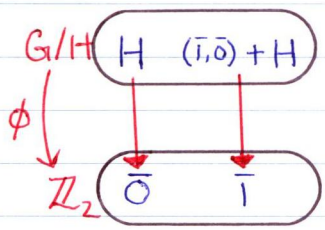
Pf: Let $G = \mathbb{Z}_2 \times \mathbb{Z}_4 \wedge H = \langle(\bar{0}, \bar{1})\rangle$

$\Rightarrow G$ is Abelian

$\Rightarrow H \trianglelefteq G$

$\Rightarrow G/H$ is a Group

Since $|G:H| = \frac{|G|}{|H|} = \frac{8}{4} = 2$ is prime, $G/H \cong \mathbb{Z}_2$ ▨



Ex.) Show $D_8 / \langle r^2 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

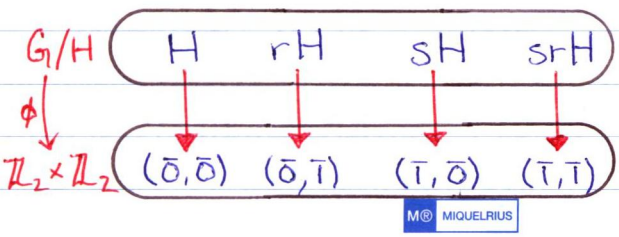
Pf: Let $G = D_8 \wedge H = \langle r^2 \rangle = \{1, r^2\}$

$\Rightarrow Z(G) = H$ (See HW 2.2 #7)

$\Rightarrow H \trianglelefteq G$

$\Rightarrow G/H$ is a Group

Since $|G:H| = \frac{|G|}{|H|} = \frac{8}{2} = 4$ & every non-identity coset has order 2, $G/H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ ▨



M® MIQUELRIUS

Tues. Oct 22 '13

Section 3.3 The Isomorphism Theorems

FIRST ISOMORPHISM THM: Let $\phi: G \to H$ be a homomorphism,

1.) $\ker(\phi) \trianglelefteq G$

Pf: Let $K = \ker(\phi)$. Let $a \in G$ & $k \in K$

$\Rightarrow \phi(aka^{-1}) = \phi(a)\phi(k)\phi(a)^{-1} = \phi(a)\phi(a)^{-1} = 1_H$

$\Rightarrow aka^{-1} \in K$

$\Rightarrow aKa^{-1} \subseteq K$, so $K \trianglelefteq G$ ▨

2.) $G/\ker(\phi) \cong \text{im}(\phi)$

Pf: Let $K = \ker(\phi)$. Define $\Psi: G/K \to \text{im}(\phi)$ by $\Psi(aK) = \phi(a)$ $\forall\, aK \in G/K$.

a.) Let $a_1K = a_2K$, where $a_1, a_2 \in G$

$\Rightarrow a_1^{-1}a_2 \in K$

$\Rightarrow \phi(a_1)^{-1}\phi(a_2) = \phi(a_1^{-1})\phi(a_2) = \phi(a_1^{-1}a_2) = 1_H$

$\Rightarrow \phi(a_2) = \phi(a_1)$

$\Rightarrow \Psi(a_1K) = \Psi(a_2K)$

$\therefore \Psi$ is Well-Defined

b.) Assume $\Psi(a_1K) = \Psi(a_2K)$

$\Rightarrow \phi(a_1) = \phi(a_2)$

$\Rightarrow 1_H = \phi(a_1)^{-1}\phi(a_2) = \phi(a_1^{-1})\phi(a_2) = \phi(a_1^{-1}a_2)$

$\Rightarrow a_1^{-1}a_2 \in K$

$\Rightarrow a_1K = a_2K$

$\therefore \Psi$ is 1-1

c.) Let $b \in \text{im}(\phi)$

$\Rightarrow \exists\, a \in G$ s.t. $\phi(a) = b$

$\Rightarrow \Psi(aK) = \phi(a) = b \in \text{im}(\phi)$

$\therefore \Psi$ is Onto

d.) Let $a_1K, a_2K \in G/K$

$\Rightarrow \Psi[(a_1K)(a_2K)] = \Psi[(a_1a_2)K] = \phi(a_1a_2) = \phi(a_1)\phi(a_2)$

$= \Psi(a_1K)\Psi(a_2K)$

$\therefore \Psi$ is a Homomorphism.

$\therefore G/\ker(\phi) \cong \text{im}(\phi)$ ▨

STRATEGY: To show $G/K \cong H$...

1.) Define a homomorphism $\phi: G \to H$ s.t. $K = \ker(\phi)$ & $H = \text{im}(\phi)$

2.) Prove ϕ is a Homomorphism (Well-Defined if needed)

3.) Prove ϕ is Onto H (so $H = \text{im}(\phi)$) & $K = \ker(\phi)$

MIQUELRIUS

FACT: Let $\phi: G \to H$ be a Homomorphism. Let $K = \ker(\phi)$. Then $gK = \{x \in G : \phi(x) = \phi(g)\} = Kg$.

Pf: Let $g \in G$. Let $S = \{x \in G : \phi(x) = \phi(g)\}$

Pf ($\subseteq$): Let $a \in gK$

$\Rightarrow a = gk$ f.s. $k \in K$

$\Rightarrow \phi(a) = \phi(gk) = \phi(g)\phi(k) = \phi(g)1_H = \phi(g)$

$\Rightarrow a \in S$

Pf ($\supseteq$): Let $b \in S$

$\Rightarrow \phi(b) = \phi(g) = \phi(g)1_H = \phi(g)\phi(k) = \phi(gk) \in \phi(gK)$ f.s. $k \in K$

$\Rightarrow b \in gK$

Since $K \trianglelefteq G$, we know $S = gK = Kg$ ▨

Ex.) $\mathbb{Z}_8$: $\bar{0}\ \bar{1}\ \bar{2}\ \bar{3}\ \bar{4}\ \bar{5}\ \bar{6}\ \bar{7}$ $\quad \ker(\phi) = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$

ϕ

D_8: $1\ r\ r^2\ r^3\ s\ sr\ sr^2\ sr^3$ $\quad \mathrm{im}(\phi) = \{1, s\}$

$\mathbb{Z}_8/K = \{K, \bar{1}+K\}$, so define $\psi: \mathbb{Z}_8/K \to \{1, s\}$ by $\psi(K) = 1$ and $\psi(\bar{1}+K) = s$

$\therefore \mathbb{Z}_8/K \cong \{1, s\} \cong \mathbb{Z}_2$

Ex.) For an odd prime p, $\bar{x} \in \mathbb{Z}_p^\times$ is a Quadratic Residue if $\bar{x} = \bar{u}^2$ for some $\bar{u} \in \mathbb{Z}_p^\times$. Prove half of $\mathbb{Z}_p^\times$ are Quadratic Residues.

Pf: Let p be an odd prime. Define $\phi: \mathbb{Z}_p^\times \to \mathbb{Z}_p^\times$ by $\phi(\bar{a}) = \bar{a}^2$

1.) $\phi(\bar{a}\bar{b}) = \phi(\overline{ab}) = \overline{ab}^2 = \bar{a}^2\bar{b}^2 = \phi(\bar{a})\phi(\bar{b}) \quad \forall\, \bar{a}, \bar{b} \in \mathbb{Z}_p^\times$

2.) $\mathrm{im}(\phi) = \{\phi(\bar{a}) : \bar{a} \in \mathbb{Z}_p^\times\} = \{\bar{a}^2 : \bar{a} \in \mathbb{Z}_p^\times\}$

3.) Let $\bar{k} \in \ker(\phi)$

$\Rightarrow \bar{k}^2 = \bar{1}$

$\Rightarrow (\bar{k}+\bar{1})(\bar{k}+\overline{-1}) = \bar{k}^2 + \overline{-1} = \bar{0}$

$\Rightarrow p \mid (k+1)(k-1)$

$\Rightarrow p \mid k+1 \ \vee\ p \mid k-1$

$\Rightarrow \bar{k}+\bar{1} = \overline{k+1} = \bar{0} \ \vee\ \bar{k}+\overline{-1} = \overline{k-1} = \bar{0}$

$\Rightarrow \bar{k} = \overline{-1} = \overline{p-1} \ \vee\ \bar{k} = \bar{1}$

$\Rightarrow |\ker(\phi)| = |\{\bar{1}, \overline{p-1}\}| = 2$

$\Rightarrow |\mathrm{im}(\phi)| = |\mathbb{Z}_p^\times / \ker(\phi)| = \frac{1}{2}|\mathbb{Z}_p^\times| = \frac{p-1}{2}$ ▨

MIQUELRIUS

"Correspondence / Lattice Thm"

FOURTH ISOMORPHISM THM: Let $K \trianglelefteq G$. Define $\pi: G \to G/K$ by $\pi(a) = aK$. Then π defines a bijection between the following sets:

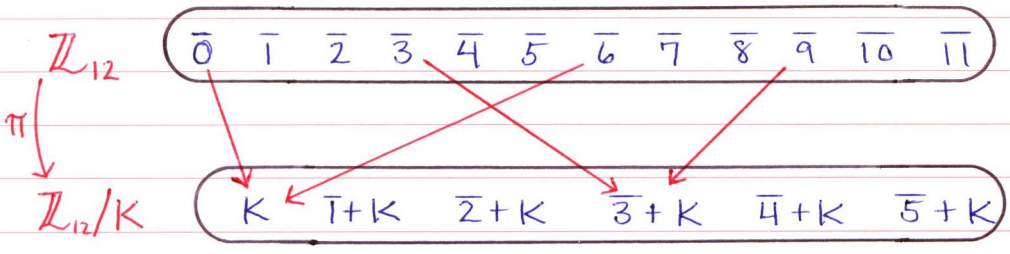
$$S = \{H \leq G : K \subseteq H\} = \{K, H_1, H_2, \dots, G\}$$
$$\pi \downarrow \qquad\qquad \updownarrow \qquad \updownarrow \qquad \updownarrow \qquad\qquad \updownarrow \qquad \pi^{-1} \uparrow$$
$$T = \{\overline{H} : \overline{H} \leq G/K\} = \{\overline{K}, \overline{H_1}, \overline{H_2}, \dots, \overline{G}\}$$
$$\{K\} \quad H_1/K \quad H_2/K \quad G/K$$

So $H \longmapsto \pi(H) = \{hK : h \in H\} = H/K$

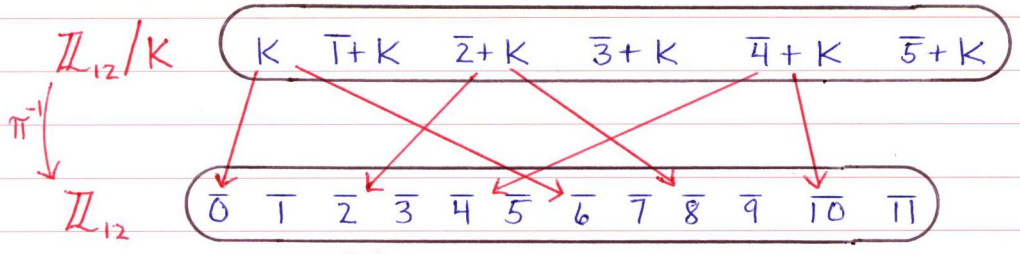
& $H \longmapsto \pi^{-1}(\overline{H}) = \{a \in G : \pi(a) \in \overline{H}\} = \{a \in G : aK \in \overline{H}\}$

Ex.) $G = \mathbb{Z}_{12}$, $K = \langle \overline{6} \rangle = \{\overline{0}, \overline{6}\}$

If $H_1 = \langle \overline{3} \rangle = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\} \leq \mathbb{Z}_{12}$
then $\overline{H_1} = \langle \overline{3} + K \rangle = \{K, \overline{3} + K\} \leq \mathbb{Z}_{12}/K$



If $\overline{H_2} = \langle \overline{2} + K \rangle = \{K, \overline{2}+K, \overline{4}+K\} \leq \mathbb{Z}_{12}/K$
then $\pi^{-1}(\overline{H_2}) = \langle \overline{2} \rangle = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\} \leq \mathbb{Z}_{12}$



$$\therefore S = \{K, \langle \overline{3} \rangle, \langle \overline{2} \rangle, \mathbb{Z}_{12}\} \quad (\langle \overline{6} \rangle = K)$$
$$\updownarrow \qquad \updownarrow \qquad \updownarrow \qquad \updownarrow$$
$$\& \; T = \{\langle K \rangle, \langle \overline{3} + K \rangle, \langle \overline{2} + K \rangle, \mathbb{Z}_{12}/K\}$$
$$= \{K, \langle \overline{3} \rangle / K, \langle \overline{2} \rangle / K, \mathbb{Z}_{12}/K\}$$

MIQUELRIUS

Thurs. Oct 24 '13

Section 3.4 Composition Series

Def: A group G is a **SIMPLE GROUP** if $|G|>1$ & the only normal subgroups of G are $\{1_G\}$ & G.

Ex.) $\mathbb{Z}_6$ is NOT simple, since $\langle\bar{3}\rangle \trianglelefteq \mathbb{Z}_6$
$\mathbb{Z}_7$ is simple, since the only subgroups of $\mathbb{Z}_7$ are $\{\bar{0}\}$ and $\mathbb{Z}_7$.

Thm: $\mathbb{Z}_n$ is Simple iff n is prime.

Pf: Since $\mathbb{Z}_n$ is Abelian, every subgroup of $\mathbb{Z}_n$ is Normal.

($\Rightarrow$): Assume n is NOT prime.
$\Rightarrow n=ab$ f.s. $a,b\in\mathbb{Z}^+$ s.t. $1<a\leq b<n$
$\Rightarrow \langle\bar{a}\rangle=\{\bar{0},\bar{a},\overline{2a},\ldots,\overline{(b-1)a}\}$
$\Rightarrow 1<b=|\langle\bar{a}\rangle|=|\{\bar{0},\bar{a},\ldots,\overline{(b-1)a}\}|<n$
$\Rightarrow \langle\bar{a}\rangle\neq\mathbb{Z}_n \wedge \langle\bar{a}\rangle\neq\{\bar{0}\}$
$\Rightarrow \mathbb{Z}_n$ is not Simple

($\Leftarrow$): Assume n is prime. Let $H\leq\mathbb{Z}_n$. Let $|H|=m$
$\Rightarrow m|n$ by Lagrange
$\Rightarrow m=1$ or n
$\Rightarrow H=\{\bar{0}\}$ or $\mathbb{Z}_n$
$\Rightarrow \mathbb{Z}_n$ is Simple. ▨

In general, a finite cyclic group G is simple iff $|G|$ is prime.

MIQUELRIUS

Thurs. Oct 24 '13

Section 3.5 Transpositions & the Alternating Group

Def: a 2-Cycle is a **TRANSPOSITION**:

FACTS:

1.) Any $\sigma \in S_n$ is a product of transpositions.

Pf: Let $\sigma \in S_n$

$\Rightarrow \sigma$ is the product of disjoint cycles, say $\tau_1, \tau_2, \ldots, \tau_k$

CLAIM: τ_i is the product of transpositions $\forall\, 1 \le i \le k$

Pf: $\tau_i = (a_1, a_2, \ldots, a_{m-1}, a_m) = (a_1, a_m)(a_1, a_{m-1}) \cdots (a_1, a_2)$

$\therefore \sigma = \tau_1 \tau_2 \cdots \tau_k$ is a product of transpositions. ▨

2.) Cycles commute iff they are disjoint.

3.) The representation of σ as a product of transpositions is NOT unique, but the parity is the same for ANY product of transpositions equalling σ.

Def: Let $\sigma \in S_n$

1.) σ is **EVEN** if σ is the product of an even # of transpositions.

2.) σ is **ODD** if σ is the product of an odd # of transpositions.

Let $\varepsilon: S_n \to \mathbb{Z}_2$ be defined by $\varepsilon(\sigma) = \begin{cases} \bar{0} & \sigma \text{ is Even} \\ \bar{1} & \sigma \text{ is Odd} \end{cases}$

1.) ε is a Homomorphism

2.) $\ker(\varepsilon) = \{\sigma \in S_n : \sigma \text{ is Even}\}$

3.) $\text{im}(\varepsilon) = \{\bar{0}, \bar{1}\} = \mathbb{Z}_2$

Def: $\ker(\varepsilon) \le S_n$ is the **ALTERNATING GROUP**, denoted A_n, of Even Permutations.

1.) By the 1st Isomorphism Thm, $S_n / A_n \cong \mathbb{Z}_2$

2.) $|S_n : A_n| = \frac{|S_n|}{|A_n|} = 2$, so $|A_n| = \frac{1}{2}|S_n| = \frac{n!}{2}$

Ex.) $S_3 = \{e, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$

$= \{(1,2)(1,2), (1,2), (1,3), (2,3), (1,3)(1,2), (1,2)(1,3)\}$

Ex.) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 12 & 13 & 3 & 1 & 11 & 9 & 5 & 10 & 6 & 4 & 7 & 8 & 2 \end{pmatrix}$

$= (1, 12, 8, 10, 4)(2, 13)(5, 11, 7)(6, 9)$

$= (1,4)(1,10)(1,8)(1,12)(2,13)(5,7)(5,11)(6,9) \in A_{13}$

MIQUELRIUS

Ch 4: GROUP ACTIONS

Tues. Oct 29 '13

Sec 4.3 Groups Acting on Themselves by Conjugation: Class Eqn.

Def: Two elements $a, b \in G$ are **CONJUGATE** if $\exists\, g \in G$ s.t. $gag^{-1} = b$. The **CONJUGACY CLASS** of $x \in G$ is the set $\{gxg^{-1} : g \in G\}$.

NOTE: If the group action of G on G is defined by $g \cdot x = gxg^{-1}$, then the Conjugacy Class of $x \in G$ is the **ORBIT** of x:

$G \cdot x = \{g \cdot x : g \in G\} = \{gxg^{-1} : g \in G\}$

SEE PAGE 42 PROOF

PROP 10: Let $\sigma, \tau \in S_n$. Suppose the disjoint cycle decomp of σ is $(a_1, a_2, \ldots, a_{k_1})(b_1, b_2, \ldots, b_{k_2})\ldots$ Then:

$$\tau\sigma\tau^{-1} = (\tau(a_1), \tau(a_2), \ldots, \tau(a_{k_1}))(\tau(b_1), \tau(b_2), \ldots, \tau(b_{k_2}))\ldots$$

(k_1 and k_2 mark the lengths of the two cycles)

$\therefore$ $\sigma_1, \sigma_2 \in S_n$ are Conjugate *iff* their disjoint cycles have equal length!

Ex.) Find the conjugacy classes of S_3.

$S_3 \cdot 1 = \{\sigma 1 \sigma^{-1} : \sigma \in S_n\} = \{1\}$

$S_3 \cdot (1,2) = \{(1,2), (1,3), (2,3)\} = \{\sigma \in S_n : \sigma \text{ is Length 2}\}$

$S_3 \cdot (1,2,3) = \{(1,2,3), (1,3,2)\} = \{\sigma \in S_n : \sigma \text{ is Length 3}\}$

Ex.) $\sigma = (1,2,3)$ $\tau = (2,3)$

$\tau\sigma\tau^{-1} = (\tau(1), \tau(2), \tau(3)) = (1,3,2)$

Ex.) $\sigma = (1,5)(3,4)(6,7,8,9)$ $\tau = (1,3,6)$

$\tau\sigma\tau^{-1} = (\tau(1), \tau(5))(\tau(3), \tau(4))(\tau(6), \tau(7), \tau(8), \tau(9))$

$= (3,5)(6,4)(1,7,8,9)$

PROP: Let G act on A. The relation $a \sim b$ *iff* $a = g \cdot b$ f.s. $g \in G$ is an Equivalence Relation on A.

(The ORBIT of $a \in A$)

1.) The Equivalence Class of $a \in A$ is $G \cdot a = \{g \cdot a : g \in G\}$

2.) $|G \cdot a| \overset{\text{Size of Conjugacy Class}}{=} |G : G_a| = |G / G_a| = \frac{|G|}{|G_a|}$

MIQUELRIUS

Ex.) $S_3 \cdot (1,2) = \{(1,2), (1,3), (2,3)\}$

$(S_3)_{(1,2)} = \{1, (1,2)\}$ ← These fix $(1,2)$

$\therefore S_3 \cdot (1,2) = \dfrac{|S_3|}{|(S_3)_{(1,2)}|} = \dfrac{6}{2} = 3$

Thm (CLASS EQUATION): Let G be finite. Let $a_1, a_2, \dots, a_r$ be representatives of the distinct conjugacy classes NOT contained in $Z(G)$.

Then $|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(a_i)|$ ← SIZE OF CONJUGACY CLASS OF a_i

NOTE 1: $C_G(a_i) = \{g \in G : g a_i g^{-1} = a_i\} = \{g \in G : g \cdot a_i = a_i\} = G_{a_i}$

NOTE 2: $|G : C_G(a_i)| = \dfrac{|G|}{|G_{a_i}|} = |G \cdot a_i|$ ← CONJUGACY CLASS OF a_i

$\therefore |G| = |Z(G)| + \sum_{i=1}^{r} |G \cdot a_i|$

Pf: Let $Z(G) = \{1, z_2, \dots, z_m\}$. Let $K_1, K_2, \dots, K_r$ be the conjugacy classes of G not contained in $Z(G)$. Let $a_i \in K_i$ $\forall i$, so $K_i = G \cdot a_i = \{g a_i g^{-1} : g \in G\}$

$\Rightarrow$ The distinct CC's of G are $\{1\}, \{z_2\}, \dots, \{z_m\}, K_1, \dots, K_r$

Since conjugation is an E.R., the CC's are pairwise disjoint & collectively exhaustive of G.

$$\therefore |G| = \sum_{i=1}^{m} 1 + \sum_{i=1}^{r} |K_i| = |Z(G)| + \sum_{i=1}^{r} |G \cdot a_i| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(a_i)| \quad \blacksquare$$

Thm: Let P be a group of size p^α, where p prime & $\alpha \geq 1$. Then $|Z(P)| > 1$.

Pf: Let $P = p^\alpha$, where p is prime & $\alpha \geq 1$. Let $a_1, a_2, \dots, a_r$ be representatives of distinct CC's of P not in $Z(P)$.

$\Rightarrow |P| = |Z(P)| + \sum_{i=1}^{r} \frac{|P|}{|C_P(a_i)|}$

By Lagrange, $|C_P(a_i)|$ divides $|P|$

$\Rightarrow |C_P(a_i)| \mid p^\alpha$

$\Rightarrow |C_P(a_i)| = p^{\alpha - k_i}$, where $k_i \neq 0$ since $a_i \notin Z(P)$

$\Rightarrow p$ divides $\frac{|P|}{|C_P(a_i)|} = p^{\alpha - (\alpha - k_i)} = p^{k_i} \neq 1$

$\Rightarrow p$ divides $|P| - \sum_{i=1}^{r} \frac{|P|}{|C_P(a_i)|} = |Z(P)|$

$\therefore |Z(P)| > 1$, since $p > 1$ $\blacksquare$

M® MIQUELRIUS

Ex.) $S_3 = \{1, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$

$Z(S_3) = \{1\}$

Other CC's: $\{(1,2), (1,3), (2,3)\}$ (K_1, a_1) & $\{(1,2,3), (1,3,2)\}$ (K_2, a_2)

$\therefore S_3 = |Z(S_3)| + |S_3 \cdot (1,2)| + |S_3 \cdot (1,2,3)| = 1 + 3 + 2 = 6$

PROOF OF PROPOSITION: Let G act on A.

1.) The relation $a \sim b$ iff $a = g \cdot b$ f.s. $g \in G$ is an E.R.

Pf: a.) $a \in A$

$\Rightarrow a = 1 \cdot a$, so $a \sim a$

b.) $a \sim b$

$\Rightarrow a = g \cdot b$ f.s. $g \in G$

$\Rightarrow g^{-1} \cdot a = g^{-1} \cdot (g \cdot b) = (g^{-1}g) \cdot b = 1 \cdot b = b$, so $b \sim a$

c.) $a \sim b \wedge b \sim c$

$\Rightarrow a = g_1 \cdot b \wedge b = g_2 \cdot c$ f.s. $g_1, g_2 \in G$

$\Rightarrow a = g_1 \cdot (g_2 \cdot c) = (g_1 g_2) \cdot c$, so $a \sim c$

$\therefore \bar{a} = \{b \in A : b \sim a\} = \{b \in A : b = g \cdot a \text{ f.s. } g \in G\} = \{g \cdot a : g \in G\} = G \cdot a$ ▨

2.) $|G \cdot a| = |G/G_a| = \frac{|G|}{|G_a|}$

Pf: Define $\psi : G/G_a \to G \cdot a$ by $\psi(gG_a) = g \cdot a \ \forall \ gG_a \in G/G_a$

a.) $g_1 G_a = g_2 G_a$

$\Rightarrow g_2^{-1} g_1 = g_a$ f.s. $g_a \in G_a$ (so $g_1 g_a^{-1} = g_2$)

$\Rightarrow g_a \cdot a = a$

$\Rightarrow g_a^{-1} \cdot a = a \ \because g_a^{-1} \cdot a = g_a^{-1} \cdot (g_a \cdot a) = (g_a^{-1} g_a) \cdot a = 1 \cdot a = a$

$\Rightarrow \psi(g_1 G_a) = g_1 \cdot a = g_1 \cdot (g_a^{-1} \cdot a) = (g_1 g_a^{-1}) \cdot a = g_2 \cdot a = \psi(g_2 G_a)$

$\therefore \psi$ is Well-Defined

b.) $\psi(g_1 G_a) = \psi(g_2 G_a)$

$\Rightarrow g_1 \cdot a = g_2 \cdot a$

$\Rightarrow (g_2^{-1} g_1) \cdot a = g_2^{-1} \cdot (g_1 \cdot a) = g_2^{-1} \cdot (g_2 \cdot a) = (g_2^{-1} g_2) \cdot a = 1 \cdot a = a$

$\Rightarrow g_2^{-1} g_1 \in G_a$

$\Rightarrow g_1 G_a = g_2 G_a \quad \therefore \psi$ is 1-1

c.) Let $g \cdot a \in G \cdot a$

$\Rightarrow gG_a \in G/G_a$

$\Rightarrow \psi(gG_a) = g \cdot a \in G \cdot a \ \therefore \psi$ is Onto

$\therefore |G \cdot a| = |G/G_a| = \frac{|G|}{|G_a|}$ ▨

M® MIQUELRIUS

LEMMA FOR CAUCHY'S THM

PROP: Let G be finite & Abelian. Let p be prime s.t. $p \mid |G|$. Then $\exists\, x \in G$ s.t. $|x| = p$.

Pf: Let G be finite & Abelian. Let p be prime s.t. $p \mid |G|$. Induct on $|G|$.

BASIC: $|G| = 2$

$\Rightarrow G = \{1_G, x\}$ where $x \neq 1_G$

$\Rightarrow x^2 = 1_G$, so $|x| = 2$.

INDUCTIVE: Suppose $|G| > 2$ & the result holds $\forall$ groups of size less than $|G|$.

Case 1: $|G| = p$

$\Rightarrow G \cong \mathbb{Z}_p$, so any $x \in G \setminus \{1_G\}$ has order p.

Case 2: $|G| > p$. Let $x \in G \setminus \{1_G\}$

a.) If $p \mid |x|$, then $|x| = pn$ f.s. $n \in \mathbb{Z}^+$

$\Rightarrow (x^n)^p = x^{|x|} = 1_G$

Suppose $(x^n)^k = 1_G$ where $0 < k < p$

$\Rightarrow x^{nk} = 1_G$, where $0 < nk < np = |x|$, a contradiction.

$\therefore |x^n| = p$

b.) Suppose $p \nmid |x|$. Let $N = \langle x \rangle = \{1_G, x, x^2, \ldots, x^{|x|}\} \leq G$

$\Rightarrow N \trianglelefteq G$, since G is Abelian (so G/N is a Group)

$\Rightarrow p \nmid |N|$, since $|x| = |N|$

$\Rightarrow p \mid |G/N|$ since $|G| = |G/N||N|$

Since $x \neq 1_G$, we know $|N| > 1$

$\Rightarrow |G/N| = \frac{|G|}{|N|} < |G|$

$\Rightarrow \exists\, y \in G$ s.t. $|yN| = p$ in G/N (by Inductive Hypothesis)

$\Rightarrow yN \neq N$, so $y \notin N$

Since $N = (yN)^p = y^p N$, we know $y^p \in N$

$\Rightarrow \langle y^p \rangle \subseteq \langle y \rangle$, but $\langle y^p \rangle \neq \langle y \rangle$

$\Rightarrow |y^p| < |y|$

$\Rightarrow \frac{|y|}{\gcd(|y|, p)} < |y|$

$\Rightarrow \gcd(|y|, p) > 1$

$\Rightarrow \gcd(|y|, p) = p$

$\Rightarrow p \mid |y|$, so $|y| = pl$ f.s. $l \in \mathbb{Z}^+$

$\Rightarrow |y^l| = p$ (like in Case 2a) ▨

PROOF OF PROP 10: Let $\sigma = (a_1, a_2, \ldots, a_m) \in S_n$. Let $\tau \in S_n$.

$\Rightarrow \tau\sigma\tau^{-1}(\tau(a_i)) = \tau\sigma(a_i) = \tau(a_{i+1})$

$\Rightarrow \tau\sigma\tau^{-1} = (\tau(a_1), \tau(a_2), \ldots, \tau(a_m))$ ▨

M® MIQUELRIUS

CAUCHY'S THM: If G is finite & p is a prime s.t. $p \mid |G|$, then G has an order-p element.

Pf: Let G be finite & $p \mid |G|$. Induct on $|G|$.

BASIC: $|G| = 2$

$\Rightarrow$ G has an order-2 element by Prop. ← Lemma

INDUCTIVE: Suppose $|G| > 2$ & Cauchy holds $\forall$ group of size less than $|G|$. Let $x \in G \setminus Z(G)$. ← Assume this ∵ if G is Abelian, then we are done.

$\Rightarrow \frac{|G|}{|C_G(x)|} = |G : C_G(x)| > 1$

$\Rightarrow |G| > |C_G(x)|$

Case 1: $p \mid |C_G(x)|$

$\Rightarrow \exists\, y \in C_G(x) \subseteq G$ s.t. $|y| = p$ (by Inductive Hypothesis)

Case 2: $p \nmid |C_G(x)|$

$\Rightarrow p \mid |G : C_G(x)|$ since $|G| = |G : C_G(x)||C_G(x)|$

Let $a_1, a_2, \ldots, a_r$ represent the r distinct CC's of G not in $Z(G)$.

$\Rightarrow |G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(a_i)|$

$\Rightarrow p \mid |Z(G)|$, since $a_i \notin Z(G)\ \forall i$

$\Rightarrow \exists\, z \in Z(G) \subseteq G$ s.t. $|z| = p$ ∵ $Z(G)$ is Abelian ▨

Thm: If $|G| = p^2$ f.s. prime p, then G is Abelian.

Pf: Let $|G| = p^2$ f.s. prime p.

$\Rightarrow |Z(G)| \neq 1$ by Prev. Thm.

$\Rightarrow |Z(G)| = p$ or p^2 by Lagrange

Case 1: $|Z(G)| = p$. We know $Z(G) \trianglelefteq G$, so $G/Z(G)$ is a Group.

$\Rightarrow |G/Z(G)| = \frac{p^2}{p} = p$

$\Rightarrow G/Z(G) \cong \mathbb{Z}_p$

$\Rightarrow \exists\, aZ(G) \in G/Z(G)$ s.t. $G/Z(G) = \langle aZ(G) \rangle = \{[aZ(G)]^k : k \in \mathbb{Z}\}$

$= \{a^k Z(G) : k \in \mathbb{Z}\}$

$\Rightarrow G = \{a^k z : k \in \mathbb{Z} \wedge z \in Z(G)\}$

Let $x, y \in G$, so $x = a^k z_1 \wedge y = a^h z_2$ f.s. $h, k \in \mathbb{Z}$ & $z_1, z_2 \in Z(G)$

$\Rightarrow xy = (a^k z_1)(a^h z_2) = z_2 a^k a^h z_1 = z_2 a^{k+h} z_1 = z_2 a^{h+k} z_1 = z_2 a^h a^k z_1$

$= a^h z_2 a^k z_1 = yx$

$\Rightarrow G$ is Abelian

$\Rightarrow |G| = |Z(G)| = p$, which is contradictory.

Case 2: $|Z(G)| = p^2$

$\Rightarrow |Z(G)| = |G|$

$\Rightarrow G = Z(G)$ is Abelian. ▨

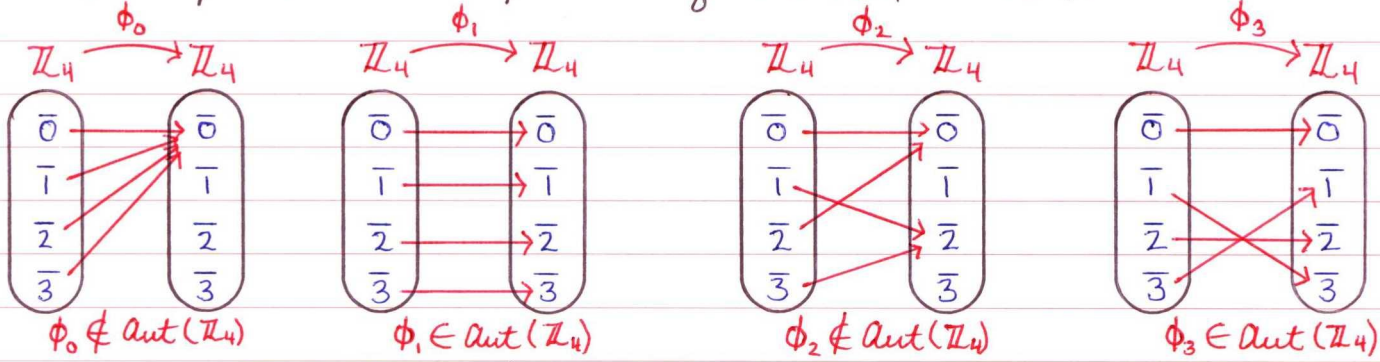
M® MIQUELRIUS

Tues. Nov 12 '13

Section 4.4 Automorphisms

Def: Let G be a group. An isomorphism $\phi: G \to G$ is an AUTOMORPHISM of G. The set of all automorphisms of G is denoted $Aut(G)$.

Ex.) Compare Homomorphisms from $\mathbb{Z}_4$ to $\mathbb{Z}_4$.



$\therefore Aut(\mathbb{Z}_4) = \{\phi_1, \phi_3\}$ NOTE: $\phi_a \in Aut(\mathbb{Z}_n)$ iff $\gcd(a,n)=1$

FACT: $Aut(G)$ is a Group under $\circ$. (the AUTOMORPHISM GROUP)

1.) The identity element of $Aut(G)$ is the identity map $i: G \to G$ given by $i(x) = x \ \forall x \in G$.

2.) The inverse of $\phi \in Aut(G)$ is $\phi^{-1}: G \to G$.

Pf: Let G be a Group.

1.) Let $\phi_1, \phi_2 \in Aut(G)$
$\Rightarrow \phi_1: G \to G$ & $\phi_2: G \to G$ are isomorphisms
$\Rightarrow \phi_1 \circ \phi_2: G \to G$ is an isomorphism
$\Rightarrow \phi_1 \circ \phi_2 \in Aut(G)$

2.) Function Composition is Associative

3.) $i(x) = i(y) \Rightarrow x = y$ | Let $x \in G \Rightarrow i(x) = x \in G$ | Let $x, y \in G \Rightarrow i(xy) = xy = i(x)i(y)$
$\therefore i \in Aut(G)$

4.) Let $\phi \in Aut(G)$
$\Rightarrow \phi: G \to G$ is an isomorphism
$\Rightarrow \phi^{-1}: G \to G$ is an isomorphism
$\Rightarrow \phi^{-1} \in Aut(G)$

$\therefore Aut(G)$ is a Group. ▨

MIQUELRIUS

PROP 16: Let G be a finite cyclic Group of size n. Then $Aut(G) \cong \mathbb{Z}_n^\times$.

Pf: Let $G = \langle x \rangle = \{1_G, x, \ldots, x^{n-1}\}$. Define $\phi_a : G \to G$ by $\phi_a(x^h) = (x^h)^a$ $\forall\, x^h \in G$, where $1 \le a \le n-1$.

CLAIM: $\phi_a \in Aut(G)$ iff $\gcd(a,n) = 1$.

Pf: $\phi_a(G) = \phi_a(\langle x \rangle) = \{\phi_a(x^h) : h \in \mathbb{Z}\} = \{x^{ha} : h \in \mathbb{Z}\} = \langle x^a \rangle$

So ϕ_a is bijective iff $|x^a| = n$ iff $\frac{n}{\gcd(a,n)} = n$ iff $\gcd(a,n) = 1$

Now let $x^h, x^k \in G$

$\Rightarrow \phi_a(x^h x^k) = \phi_a(x^{h+k}) = (x^{h+k})^a = x^{ha+ka} = (x^h)^a (x^k)^a$

$= \phi_a(x^h)\,\phi_a(x^k)$

$\therefore Aut(G) = \{\phi_a : \gcd(a,n) = 1, \text{ where } 1 \le a \le n-1\}$

Now define $\chi : Aut(G) \to \mathbb{Z}_n^\times$ by $\chi(\phi_a) = \bar{a}$ $\forall\, \phi_a \in Aut(G)$

1.) Let $\bar{a} \in \mathbb{Z}_n^\times$

$\Rightarrow \gcd(a,n) = 1 \wedge 1 \le a \le n-1$

$\Rightarrow \phi_a \in Aut(G)$

$\Rightarrow \chi(\phi_a) = \bar{a} \in \mathbb{Z}_n^\times$, so χ is Onto (and therefore 1-1)

Since $|Aut(G)| = |\mathbb{Z}_n^\times|$

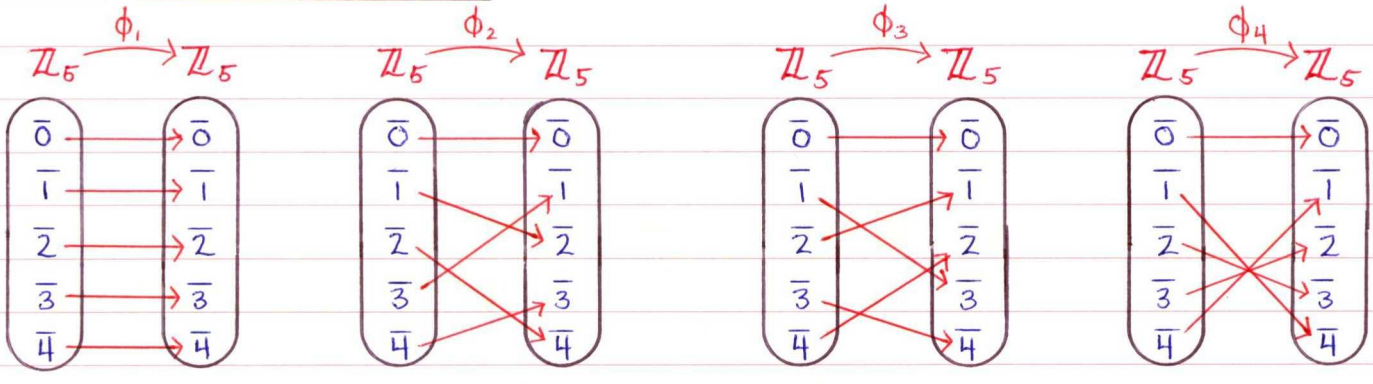
2.) Let $\phi_a, \phi_b \in Aut(G)$. Let $x^h \in G$.

$\Rightarrow (\phi_a \circ \phi_b)(x^h) = \phi_a(\phi_b(x^h)) = \phi_a(x^{hb}) = x^{hab} = \phi_{ab}(x^h)$

$\Rightarrow \chi(\phi_a \circ \phi_b) = \chi(\phi_{ab}) = \overline{ab} = \bar{a}\bar{b} = \chi(\phi_a)\chi(\phi_b)$

$\therefore Aut(G) \cong \mathbb{Z}_n^\times$ ▨

Ex.) $Aut(\mathbb{Z}_5) \cong \mathbb{Z}_5^\times$:



$Aut(\mathbb{Z}_5)$	ϕ_1	ϕ_2	ϕ_3	ϕ_4
ϕ_1	ϕ_1	ϕ_2	ϕ_3	ϕ_4
ϕ_2	ϕ_2	ϕ_4	ϕ_1	ϕ_3
ϕ_3	ϕ_3	ϕ_1	ϕ_4	ϕ_2
ϕ_4	ϕ_4	ϕ_3	ϕ_2	ϕ_1

$\mathbb{Z}_5^\times$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

$\therefore Aut(\mathbb{Z}_5) \cong \mathbb{Z}_5^\times$

MIQUELRIUS

PROP: Let $H \leq G$. Then $N_G(H)/C_G(H)$ is isomorphic to a subgroups of $Aut(H)$.

Pf: Let $H \leq G$. For a fixed $g \in N_G(H)$, define $\phi_g : H \to H$ by $\phi_g(h) = ghg^{-1}$ $\forall h \in H$. Define $\Psi : N_G(H) \to Aut(H)$ by $\Psi(g) = \phi_g$.

$\Rightarrow H \trianglelefteq N_G(H)$, since $N_G(H) = \{g \in G : gHg^{-1} = H\}$

1.) $\underline{\phi_g \in Aut(H)}$:

$clm(\Psi) \leq Aut(H)$

a.) Assume $\phi_g(h_1) = \phi_g(h_2)$

$\Rightarrow gh_1g^{-1} = gh_2g^{-1}$

$\Rightarrow h_1 = h_2$

b.) Let $h \in H$

$\Rightarrow g^{-1}hg \in H$ $\because H \trianglelefteq N_G(H)$ & $g^{-1} \in N_G(H)$

$\Rightarrow \phi_g(g^{-1}hg) = g(g^{-1}hg)g^{-1} = h \in H$

c.) Let $h_1, h_2 \in H$

$\Rightarrow \phi_g(h_1h_2) = g(h_1h_2)g^{-1} = (gh_1g^{-1})(gh_2g^{-1}) = \phi_g(h_1)\,\phi_g(h_2)$

2.) $\underline{\Psi \text{ is a Homomorphism}}$: Let $a, b \in N_G(H)$. Let $h \in H$

$\Rightarrow (\phi_a \circ \phi_b)(h) = \phi_a(\phi_b(h)) = \phi_a(bhb^{-1}) = abhb^{-1}a^{-1} = (ab)h(ab)^{-1} = \phi_{ab}(h)$

$\Rightarrow \Psi(ab) = \phi_{ab} = \phi_a \circ \phi_b = \Psi(a) \circ \Psi(b)$

3.) $\underline{Ker(\Psi) = C_G(H)}$:

($\subseteq$): $Ker(\Psi) = \{g \in N_G(H) : \Psi(g) = i$, where i is the identity map$\}$

$= \{g \in N_G(H) : \phi_g(x) = x \ \forall x \in H\}$

$= \{g \in N_G(H) : gxg^{-1} = x \ \forall x \in H\} \subseteq C_G(H)$

($\supseteq$): Let $y \in C_G(H) \subseteq N_G(H)$

$\Rightarrow yxy^{-1} = x \ \forall x \in H$

$\Rightarrow y \in \{g \in N_G(H) : gxg^{-1} = x \ \forall x \in H\} = Ker(\Psi)$

$\Rightarrow C_G(H) \subseteq Ker(\Psi)$

$\therefore Ker(\Psi) = C_G(H)$.

$\therefore$ By the F.I.T., $N_G(H)/C_G(H) = N_G(H)/Ker(\Psi) \cong clm(\Psi) \leq Aut(H)$ ▨

COROLLARY: If $H \trianglelefteq G$, then $G/C_G(H)$ is isomorphic to a subgroup of $Aut(H)$.

Pf: Suppose $H \trianglelefteq G$.

$\Rightarrow N_G(H) = G$ $\because N_G(H) = \{g \in G : gHg^{-1} = H\} = G$

$\Rightarrow G/C_G(H)$ is isomorphic to a subgroup of $Aut(H)$ by the Prop. ▨

MIQUELRIUS

Thurs. Nov 14 '13

Section 4.5 Sylow's Theorem

Def: Let G be a Group. Let p be prime.

1.) A group of size p^α $(\alpha \geq 0)$ is a **P-GROUP**.

2.) A subgroup of G that is a p-Group is a **P-SUBGROUP** of G.

3.) If $|G| = p^\alpha m$ where $p \nmid m$, then a subgroup of size p^α is a **SYLOW P-SUBGROUP** of G.

Notation: Let $|G| = p^\alpha m$, where $p \nmid m$.

1.) $Syl_p(G)$ = The set of all Sylow p-subgroups of G.

2.) $|Syl_p(G)| = n_p(G)$ or just n_p.

Ex.) $|\mathbb{Z}_{12}| = 2^2 \cdot 3$ ← Size $2^2 = 4$

$Syl_2(\mathbb{Z}_{12}) = \{\langle \bar{3} \rangle\}$ & $n_2(\mathbb{Z}_{12}) = 1$

$Syl_3(\mathbb{Z}_{12}) = \{\langle \bar{4} \rangle\}$ & $n_3(\mathbb{Z}_{12}) = 1$

↖ Size $3^1 = 3$

SYLOW'S THM: Let $|G| = p^\alpha m$, where $p \nmid m$.

1.) $\exists$ a Sylow p-SG of G.

2.) If P is a Sylow p-SG of G & Q is ANY p-SG of G, then $\exists\, g \in G$ s.t. $Q \leq gPg^{-1}$

a.) If Q is a Sylow p-SG of G, then $\exists\, g \in G$ s.t. $Q = gPg^{-1}$ since $|gPg^{-1}| = |P| = p^\alpha$.

b.) To find Sylow p-SG's of G, conjugate P by each $g \in G$.

3.) $n_p(G) \equiv 1 \pmod p$ & $n_p(G) \mid m$.

↖ $p \mid n_p(G) - 1$

Ex.) $|D_{12}| = 2^2 \cdot 3$

1.) $P = \{1, r^3, s, sr^3\}$ is a Sylow 2-SG of G.

2.) $Q = \{1, sr^2\} \leq \{1, r^3, sr^2, sr^5\} = (sr)P(sr)^{-1}$

3.) $n_2(D_{12}) \equiv 1 \pmod 2$, so $n_2(D_{12}) = 1, 3, 5, 7, \ldots$

$n_2(D_{12}) \mid 3$, so $n_2(D_{12}) = 1$ or 3

But $n_2(D_{12}) \neq 1$ ($\because$ we know 2 of them), so $n_2(D_{12}) = 3$

In fact, $Syl_2(D_{12}) = \{P, (sr)P(sr)^{-1}, (sr^2)P(sr^2)^{-1}\}$

LEMMA: If P is the UNIQUE Sylow p-SG of G, then $P \trianglelefteq G$.

Pf: Let P be the unique Sylow p-SG of G. Let $g \in G$.

$\Rightarrow gPg^{-1}$ is also a Sylow p-SG of G.

$\Rightarrow gPg^{-1} = P$, since $n_p(G) = 1$

$\Rightarrow P \trianglelefteq G$ ▨

NOTE: For $P \in Syl_p(G)$, $n_p(G) = 1$ iff $gPg^{-1} = P\ \forall g \in G$ iff $P \trianglelefteq G$

MIQUELRIUS

NOT GIVEN ABELIAN!

PROVE: If $|G|=15$, then G is cyclic.

Pf: Assume $G=15=3\cdot 5$

$\Rightarrow \exists$ subgroups P & Q s.t. $|P|=3 \wedge |Q|=5$ by Sylow 1

$\Rightarrow P$ & Q are cyclic by Lagrange

$\Rightarrow \exists x\in P \wedge y\in Q$ s.t. $|x|=3 \wedge |y|=5$

CLAIM 1: $P\cap Q=\{1_G\}$

Pf: Since $P\leq G \wedge Q\leq G$, we have $P\cap Q\leq G$

$\Rightarrow P\cap Q\leq P \wedge P\cap Q\leq Q$

$\Rightarrow |P\cap Q|\,|3 \wedge |P\cap Q|\,|5$

$\Rightarrow |P\cap Q|=1$

$\Rightarrow P\cap Q=\{1_G\}$

CLAIM 2: $P\trianglelefteq G \wedge Q\trianglelefteq G$

Pf: a.) $n_3(G)\equiv 1 \pmod 3 \wedge n_3(G)\,|\,5$ by Sylow 3

$\Rightarrow n_3(G)=1$ or 5

$\Rightarrow n_3(G)=1$, since $5\not\equiv 1 \pmod 3$

$\Rightarrow P\trianglelefteq G$ by Lemma

b.) $n_5(G)\equiv 1 \pmod 5 \wedge n_5(G)\,|\,3$ by Sylow 3

$\Rightarrow n_5(G)=1$ or 3

$\Rightarrow n_5(G)=1$, since $3\not\equiv 1 \pmod 5$

$\Rightarrow Q\trianglelefteq G$ by Lemma

CLAIM 3: $xy=yx$

Pf: Consider $x^{-1}y^{-1}xy$

a.) $x^{-1}y^{-1}x\in Q$, since $y^{-1}\in Q$ & $Q\trianglelefteq G$

$\Rightarrow (x^{-1}y^{-1}x)y\in Q$

b.) $y^{-1}xy\in P$, since $x\in P$ & $P\trianglelefteq G$

$\Rightarrow x^{-1}(y^{-1}xy)\in P$

$\therefore x^{-1}y^{-1}xy\in P\cap Q$

$\Rightarrow x^{-1}y^{-1}xy=1_G$

$\Rightarrow xy=yx$

CLAIM H: $G=\langle xy\rangle$

Pf: $(xy)^{15}=(xy)(xy)\dots(xy)=x^{15}y^{15}=(x^3)^5(y^5)^3=1_G$

$\Rightarrow |xy|\,|15$

a.) $(xy)^1\neq 1_G$, since $x\neq y^{-1}$ (or else $1_G=x^3=y^{-3}=y^2$)

b.) $(xy)^3=x^3y^3=y^3\neq 1_G$

c.) $(xy)^5=x^5y^5=x^5=x^2\neq 1_G$

$\therefore |xy|=15=|G|$, so G is cyclic ▨

M® MIQUELRIUS

PROVE: If $|G| = 255$, then G is Abelian.

Pf: Let $|G| = 255 = 3 \cdot 5 \cdot 17$

$\Rightarrow \begin{cases} \exists H \leq G \text{ s.t. } |H| = 17 \text{ by Sylow 1} \\ n_{17} \equiv 1 \pmod{17} \wedge n_{17} \mid 15 \text{ by Sylow 3} \end{cases}$

$\Rightarrow n_{17} = 1, 3, 5, \text{ or } 15$

$\Rightarrow n_{17} = 1$, since $3, 5, 15 \not\equiv 1 \pmod{17}$

$\Rightarrow H \trianglelefteq G$ by Lemma

$\Rightarrow G/C_G(H)$ is isomorphic to a subgroups of $Aut(H)$

Since $|H| = 17$, we have $Aut(H) \cong Aut(\mathbb{Z}_{17}) \cong \mathbb{Z}_{17}^{\times} = \{\bar{1}, \bar{2}, \ldots, \bar{16}\}$

$\Rightarrow |Aut(H)| = 16$

$\Rightarrow |G/C_G(H)| \mid 16$

$\Rightarrow \frac{255}{|C_G(H)|} = \frac{3 \cdot 5 \cdot 17}{|C_G(H)|}$ divides 16

$\Rightarrow |C_G(H)| = 255 = |G|$

$\Rightarrow C_G(H) = G$

$\Rightarrow H \leq Z(G)$

$\Rightarrow |H| \mid |Z(G)|$

$\Rightarrow 17 \mid |Z(G)|$

$\Rightarrow |Z(G)| = 17, 51, 85, \text{ or } 255$ (since $|Z(G)| \mid 255$)

$\Rightarrow |G/Z(G)| = \frac{255}{17}, \frac{255}{51}, \frac{255}{85}, \text{ or } \frac{255}{255}$

$\Rightarrow |G/Z(G)| = 15, 5, 3, \text{ or } 1$

$\Rightarrow G/Z(G)$ is cyclic

$\Rightarrow G$ is Abelian. ▨

MIQUELRIUS

Ch 5: DIRECT/SEMIDIRECT PRODUCTS

Tues. Nov 19 '13

Sec 5.2 Fundamental Thm of Finitely Generated Abelian Groups

Def: Let $G_1, G_2, \dots, G_n$ be groups. The **DIRECT PRODUCT** $G_1 \times G_2 \times \dots \times G_n = \{(g_1, g_2, \dots, g_n) : g_i \in G_i \ \forall i\}$ is a group w/ the operation $(g_1, g_2, \dots, g_n)(g_1', g_2', \dots, g_n') = (g_1g_1', g_2g_2', \dots, g_ng_n')$

1.) The identity is $(1_{G_1}, 1_{G_2}, \dots, 1_{G_n})$

2.) $(g_1, g_2, \dots, g_n)^{-1} = (g_1^{-1}, g_2^{-1}, \dots, g_n^{-1})$

CLASSIFYING FINITE ABELIAN GROUPS: Suppose G is a finite Abelian Group. Then $G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_s}$ where...

1.) $n_j \geq 2 \ \forall \ 1 \leq j \leq s$

2.) $n_{i+1} | n_i \ \forall \ 1 \leq i \leq s-1$ ← So $n_1 \geq n_2 \geq \dots \geq n_s$

3.) $|G| = n_1 n_2 \dots n_s$

If $G \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_t}$ satisfy Conditions 1-3, then $s = t$ & $m_1 = n_1, m_2 = n_2, \dots, m_t = n_s$ ← So the expression is UNIQUE.

FACTS: Assume Conditions 1-3.

1.) Every prime divisor of $|G|$ divides n_1:

Pf: Suppose $p \mid |G|$, where p is prime.

$\Rightarrow p \mid n_1 n_2 \dots n_s$

$\Rightarrow p \mid n_i$ f.s. $1 \leq i \leq s$

But $n_i \mid n_{i-1}, n_{i-1} \mid n_{i-2}, \dots, n_2 \mid n_1$

$\Rightarrow p \mid n_1$ ▨

2.) $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ iff $\gcd(m,n) = 1$:

Pf: Let $\ell = \text{lcm}(m,n)$ ∧ $d = \gcd(m,n)$

($\Rightarrow$): Assume $d \neq 1$. Let $(\bar{a}, \bar{b}) \in \mathbb{Z}_m \times \mathbb{Z}_n$

$\Rightarrow (\bar{a}, \bar{b})^{\ell} = (\bar{a}^{\ell}, \bar{b}^{\ell}) = (\bar{0}, \bar{0})$, since $m \mid \ell$ ∧ $n \mid \ell$

$\Rightarrow |(\bar{a}, \bar{b})| \leq \ell = \frac{mn}{d} < mn$

$\Rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$ is not Cyclic.

$\Rightarrow \mathbb{Z}_m \times \mathbb{Z}_n \neq \mathbb{Z}_{mn}$

($\Leftarrow$): Assume $d = 1$

$\Rightarrow |(\bar{1}, \bar{1})| = \text{lcm}(m,n) = \frac{mn}{d} = \frac{mn}{1} = mn$

$\Rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$ is Cyclic

$\Rightarrow \mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$

$\therefore \mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ iff $\gcd(m,n) = 1$ ▨

MIQUELRIUS

3.) $G_1 \times G_2 \cong G_2 \times G_1$:

Pf: Define $\phi: G_1 \times G_2 \to G_2 \times G_1$ by $\phi((a,b)) = (b,a)$

a.) $\phi((a,b)) = \phi((c,d))$
$\Rightarrow (b,a) = (d,c)$
$\Rightarrow b=d \wedge a=c$
$\Rightarrow (a,b) = (c,d)$

b.) Let $(b,a) \in G_2 \times G_1$
$\Rightarrow a \in G_1 \wedge b \in G_2$
$\Rightarrow (a,b) \in G_1 \times G_2$
$\Rightarrow \phi((a,b)) = (b,a) \in G_2 \times G_1$

c.) Let $(a,b), (c,d) \in G_1 \times G_2$
$\Rightarrow \phi((a,b)(c,d)) = \phi((ac,bd)) = (bd,ac) = (b,a)(d,c)$
$= \phi((a,b))\phi((c,d))$

$\therefore G_1 \times G_2 \cong G_2 \times G_1$ ▨

Ex.) Classify Abelian groups of size 12.

$|G| = 12 = 2^2 \cdot 3$

2	3
2,0	1,0
1,1	

G is isomorphic to one of the following:
1.) $\mathbb{Z}_{2^2 \cdot 3} = \mathbb{Z}_{12}$
2.) $\mathbb{Z}_{2 \cdot 3} \times \mathbb{Z}_2 = \mathbb{Z}_6 \times \mathbb{Z}_2$

Ex.) Classify Abelian groups of size 360.

$|G| = 2^3 \cdot 3^2 \cdot 5$

2	3	5
3,0,0	2,0,0	1,0,0
2,1,0	1,1,0	
1,1,1		

G is isomorphic to one of the following:
1.) $\mathbb{Z}_{2^3 \cdot 3^2 \cdot 5} = \mathbb{Z}_{360}$
2.) $\mathbb{Z}_{2^3 \cdot 3 \cdot 5} \times \mathbb{Z}_3 = \mathbb{Z}_{120} \times \mathbb{Z}_3$
3.) $\mathbb{Z}_{2^2 \cdot 3^2 \cdot 5} \times \mathbb{Z}_2 = \mathbb{Z}_{180} \times \mathbb{Z}_2$
4.) $\mathbb{Z}_{2^2 \cdot 3 \cdot 5} \times \mathbb{Z}_{2 \cdot 3} = \mathbb{Z}_{60} \times \mathbb{Z}_6$
5.) $\mathbb{Z}_{2 \cdot 3^2 \cdot 5} \times \mathbb{Z}_2 \times \mathbb{Z}_2 = \mathbb{Z}_{90} \times \mathbb{Z}_2 \times \mathbb{Z}_2$
6.) $\mathbb{Z}_{2 \cdot 3 \cdot 5} \times \mathbb{Z}_{2 \cdot 3} \times \mathbb{Z}_2 = \mathbb{Z}_{30} \times \mathbb{Z}_6 \times \mathbb{Z}_2$

Ex.) Recall if $|G| = p^2$, then G is Abelian
$\Rightarrow G \cong \mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$

MIQUELRIUS

Tues. Nov 19 '13

Section 5.4 Recognizing Direct Products

Def: Let G be a group. The **COMMUTATOR SUBGROUP G'** of G is the subgroup of G generated by all elements of the form $x^{-1}y^{-1}xy$ where $x, y \in G$.

NOTATION: $G' = \langle \{x^{-1}y^{-1}xy : x, y \in G\} \rangle$

Ex.) $D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$

$r^{-1}s^{-1}rs = sr^2s = r^{-2} = r^2 \in D_8'$

$(sr)^{-1}r^{-1}(sr)r = sr\,r^{-1}sr^2 = r^2 \in D_8'$

$(r^{-1}s^{-1}rs)((sr)^{-1}r^{-1}(sr)r) = r^2r^2 = 1 \in D_8'$

NOTE: $D_{2n}' = \langle r^2 \rangle$

FACT: G is Abelian *iff* $G' = \{1_G\}$

Pf ($\Rightarrow$): Assume G is Abelian

$\Rightarrow G' = \langle \{x^{-1}y^{-1}xy : x, y \in G\} \rangle = \langle \{x^{-1}xy^{-1}y : x, y \in G\} \rangle$

$= \langle \{1_G\} \rangle = \{1_G\}$

Pf ($\Leftarrow$): Assume $G' = \{1_G\}$

$\Rightarrow x^{-1}y^{-1}xy = 1_G \;\forall\; x, y \in G$

$\Rightarrow xy = yx$

$\Rightarrow G$ is Abelian

$\therefore$ G is Abelian *iff* $G' = \{1_G\}$ ▨

PROP 7: Let G be a Group.

1.) $G' \trianglelefteq G$:

Pf: Let $a \in G' \wedge g \in G$

$\Rightarrow gag^{-1}a^{-1} \in G'$

$\Rightarrow gag^{-1} = (gag^{-1}a^{-1})a \in G'$

$\Rightarrow gG'g^{-1} \subseteq G'$, so $G' \trianglelefteq G$ ▨

2.) G/G' is Abelian:

Pf: Let $xG', yG' \in G/G'$, where $x, y \in G$

$\Rightarrow (yx)^{-1}(xy) = x^{-1}y^{-1}xy \in G'$

$\Rightarrow (xG')(yG') = (xy)G' = (yx)G' = (yG')(xG')$, so G/G' is Abelian. ▨

3.) If $H \trianglelefteq G \wedge G/H$ is Abelian, then $G' \leq H$:

Pf: Assume $H \trianglelefteq G \wedge G/H$ is Abelian. Let $x, y \in G$

$\Rightarrow (xy)H = (xH)(yH) = (yH)(xH) = (yx)H$

$\Rightarrow x^{-1}y^{-1}xy = (yx)^{-1}(xy) \in H$

$\Rightarrow$ All generators of G' are in H, so $G' \leq H$ ▨

MIQUELRIUS

Ex.) Classify groups of size 45.

LEMMA: If $|G|=45$, then G is Abelian.

Pf: Let $|G|=45=3^2\cdot 5$

$\Rightarrow \exists P\in Syl_5(G) \wedge \exists Q\in Syl_3(G)$ by Sylow 1

CLAIM 1: $P\cap Q=\{1_G\}$

Pf: Since $P\leq G \wedge Q\leq G$, we have $P\cap Q\leq G$

$\Rightarrow P\cap Q\leq P \wedge P\cap Q\leq Q$

$\Rightarrow |P\cap Q|\,|\,5 \wedge |P\cap Q|\,|\,9$

$\Rightarrow |P\cap Q|=1$

$\Rightarrow P\cap Q=\{1_G\}$

CLAIM 2: $P\trianglelefteq G \wedge Q\trianglelefteq G$

Pf: a.) $n_5(G)\equiv 1 \pmod 5 \wedge n_5(G)\,|\,9$ by Sylow 3

$\Rightarrow n_5(G)=1$ (since $3,9\not\equiv 1 \pmod 5$)

$\Rightarrow P\trianglelefteq G$ (so G/P is a Group)

b.) $n_3(G)\equiv 1 \pmod 3 \wedge n_3(G)\,|\,5$ by Sylow 3

$\Rightarrow n_3(G)=1$ (since $5\not\equiv 1 \pmod 3$)

$\Rightarrow Q\trianglelefteq G$ (so G/Q is a Group)

CLAIM 3: G is Abelian

Pf: a.) $|G/P|=\frac{45}{5}=9=3^2$

$\Rightarrow G/P$ is Abelian

$\Rightarrow G'\leq P$, since $P\trianglelefteq G$

b.) $|G/Q|=\frac{45}{9}=5$

$\Rightarrow G/Q\cong \mathbb{Z}_5$ is Cyclic (therefore Abelian)

$\Rightarrow G'\leq Q$, since $Q\trianglelefteq G$

By (a) & (b), we have $G'\leq P\cap Q=\{1_G\}$

$\Rightarrow G'=\{1_G\}$

$\Rightarrow G$ is Abelian ▨

By the Lemma, we find all Abelian groups of size 45:

3	5
2,0	1,0
1,1	

$\therefore$ G is isomorphic to one of the following:

a.) $\mathbb{Z}_{3^2\cdot 5} = \mathbb{Z}_{45}$

b.) $\mathbb{Z}_{3\cdot 5}\times\mathbb{Z}_3 = \mathbb{Z}_{15}\times\mathbb{Z}_3$

MIQUELRIUS

Thm: Let p & q be primes s.t. $p<q$ & $q \not\equiv 1 \pmod{p}$.

A.) If $|G| = p^2q$, then G is Abelian:

Pf: Let $|G| = p^2q$

$\Rightarrow \exists P \in Syl_p(G) \wedge \exists Q \in Syl_q(G)$

1.) $P \cap Q = \{1_G\}$: $P \cap Q \leq G$

$\Rightarrow P \cap Q \leq P \wedge P \cap Q \leq Q$

$\Rightarrow |P \cap Q| \mid p^2 \wedge |P \cap Q| \mid q$

$\Rightarrow |P \cap Q| = 1$, so $P \cap Q = \{1_G\}$

2.) $P \trianglelefteq G \wedge Q \trianglelefteq G$:

a.) $n_p \equiv 1 \pmod{p} \wedge n_p \mid q$

$\Rightarrow n_p = 1$, since $q \not\equiv 1 \pmod{p}$

$\Rightarrow gPg^{-1} = P \ \forall g \in G$, so $P \trianglelefteq G$

b.) $n_q \equiv 1 \pmod{q} \wedge n_q \mid p^2$

$\Rightarrow n_q = 1$, p, or p^2

But $p<q$ & $q \neq p+1$, so $q \nmid p-1 \wedge q \nmid p+1$

$\Rightarrow q \nmid p^2 - 1$

$\Rightarrow n_q = 1$, since $p, p^2 \not\equiv 1 \pmod{q}$

$\Rightarrow gQg^{-1} = Q \ \forall g \in G$, so $Q \trianglelefteq G$

3.) G is Abelian:

a.) $|G/P| = \frac{p^2q}{p^2} = q$

$\Rightarrow G/P \cong \mathbb{Z}_q$ by Lagrange

$\Rightarrow G/P$ is Cyclic (therefore Abelian)

$\Rightarrow G' \leq P$

b.) $|G/Q| = \frac{p^2q}{q} = p^2$

$\Rightarrow G/Q$ is Abelian by Class Equation

$\Rightarrow G' \leq Q$

By (a) & (b), we have $G' \leq P \cap Q = \{1_G\}$, so $G' = \{1_G\}$

$\therefore G$ is Abelian. ▨

NOTE: G is isomorphic to either $\mathbb{Z}_{p^2q}$ or $\mathbb{Z}_{pq} \times \mathbb{Z}_p$ by the Fundamental Theorem of Finitely Generated Abelian Groups.

MIQUELRIUS

B.) If $|G| = pq$, then G is Cyclic:

Pf: Let $|G| = pq$

$\Rightarrow \exists P \in Syl_p(G) \wedge \exists Q \in Syl_q(G)$

1.) $P \cap Q = \{1_G\}$: $P \cap Q \leq G$

$\Rightarrow P \cap Q \leq P \wedge P \cap Q \leq Q$

$\Rightarrow |P \cap Q| \mid p \wedge |P \cap Q| \mid q$

$\Rightarrow |P \cap Q| = 1$, so $P \cap Q = \{1_G\}$

2.) $P \trianglelefteq G \wedge Q \trianglelefteq G$:

a.) $n_p \equiv 1 \pmod p \wedge n_p \mid q$

$\Rightarrow n_p = 1$, since $q \not\equiv 1 \pmod p$

$\Rightarrow gPg^{-1} = P \ \forall g \in G$, so $P \trianglelefteq G$

b.) $n_q \equiv 1 \pmod q \wedge n_q \mid p$

$\Rightarrow n_q = 1$ or p

But $p < q$, so $q \nmid p - 1$

$\Rightarrow n_q = 1$, since $p \not\equiv 1 \pmod q$

$\Rightarrow gQg^{-1} = Q \ \forall g \in G$, so $Q \trianglelefteq G$

3.) G is Abelian:

a.) $|G/P| = \frac{pq}{p} = q$

$\Rightarrow G/P \cong \mathbb{Z}_q$

$\Rightarrow G/P$ is Cyclic (therefore Abelian)

$\Rightarrow G' \leq P$

b.) $|G/Q| = \frac{pq}{q} = p$

$\Rightarrow G/Q \cong \mathbb{Z}_p$

$\Rightarrow G/Q$ is Cyclic (therefore Abelian)

$\Rightarrow G' \leq Q$

By (a) & (b), $G' \leq P \cap Q = \{1_G\}$, so G is Abelian.

4.) G is Cyclic: Let $x \in P \setminus \{1_G\} \wedge y \in Q \setminus \{1_G\}$. Let $n = |xy|$

OR USE FTOFGAG $\Rightarrow |x| = p \wedge |y| = q$ by Lagrange

$\Rightarrow (xy)^{pq} = (x^p)^q (y^q)^p = 1_G 1_G = 1_G$

$\Rightarrow n \mid pq$

$\Rightarrow n = 1, p, q,$ or pq

a.) If $n = 1$, then $xy = 1_G$ (so $x = y^{-1}$)

$\Rightarrow 1_G = x^p = y^{-p} = y^{q-p}$, a C.D. since $0 < q - p < q$

b.) If $n = p$, then $1_G = (xy)^p = x^p y^p = y^p$, a C.D. since $0 < p < q$

c.) If $n = q$, then $1_G = (xy)^q = x^q y^q = x^q$, a C.D. since $p \nmid q$

$\therefore |xy| = n = pq = |G|$, so $G = \langle xy \rangle$ is Cyclic ▨

M® MIQUELRIUS

Thm: Let p, q, r be primes s.t. the following hold:

1.) $p < q < r$

2.) $q \not\equiv 1 \pmod{p}$, $r \not\equiv 1 \pmod{p}$, $r \not\equiv 1 \pmod{q}$, & $pq \not\equiv 1 \pmod{r}$

Then any group of size pqr is Abelian.

Pf: Let $|G| = pqr$ following Conditions (1) & (2).

$\Rightarrow n_r \equiv 1 \pmod{r} \wedge n_r \mid pq$

$\Rightarrow n_r = 1$, since $r \nmid p-1$, $r \nmid q-1$, & $pq \not\equiv 1 \pmod{r}$

$\Rightarrow \exists! R \in Syl_r(G)$

$\Rightarrow R \trianglelefteq G$

Since $|R| = r$ is prime, we know $|Aut(R)| = |Aut(\mathbb{Z}_r)| = |\mathbb{Z}_r^\times| = r-1$

Since $R \trianglelefteq G$, we know $G/C_G(R)$ is isomorphic to a subgroup of $Aut(R)$.

$\Rightarrow \frac{|G|}{|C_G(R)|} = \frac{pqr}{|C_G(R)|}$ divides $r-1$

But $p \nmid r-1$, $q \nmid r-1$, & $r \nmid r-1$, so $|C_G(R)| = pqr = |G|$

$\Rightarrow C_G(R) = G$

$\Rightarrow$ Every element of G commutes w/ every element of R

$\Rightarrow R \leq Z(G)$

$\Rightarrow r \mid |Z(G)|$ (and $|Z(G)| \mid pqr$)

$\Rightarrow |Z(G)| = r, pr, qr,$ or pqr

$\Rightarrow |G/Z(G)| = pq, q, p,$ or 1 ← SEE PREVIOUS THM

$\Rightarrow G/Z(G)$ is cyclic

$\Rightarrow G$ is Abelian ▨

M® MIQUELRIUS

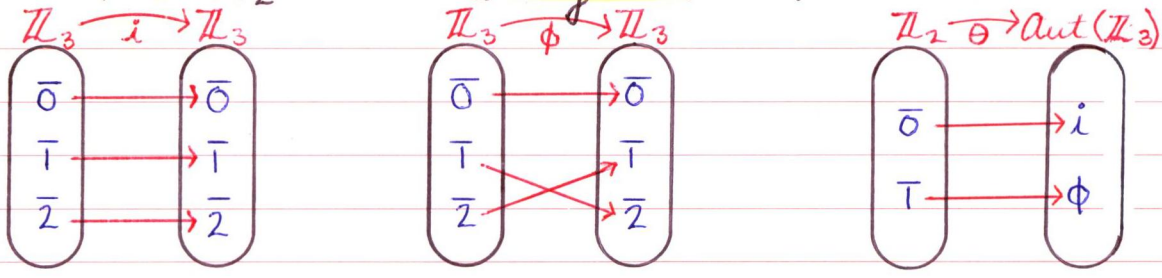
Thurs. Dec05 '13

Section 5.5 Semidirect Products

Def: Let G & K be groups. Let $\theta: K \to Aut(G)$ be a Homomorphism. Define an operation on $G \times K$ by $(g_1, k_1) * (g_2, k_2) = (g_1[\theta(k_1)](g_2), k_1 k_2)$.
($\theta(k_1)$ changes $g_2 \to$ A.M. of G)

Then the set $G \times K$ under this operation is the **SEMIDIRECT PRODUCT** of G & K, denoted $G \rtimes_\theta K$ or just $G \rtimes K$.
↖ Generalization of Direct Product

Ex.) Define $i: \mathbb{Z}_3 \to \mathbb{Z}_3$ by $i(\bar{a}) = \bar{a}$ $\forall \bar{a} \in \mathbb{Z}_3$ $\therefore i \in Aut(\mathbb{Z}_3)$
& $\phi: \mathbb{Z}_3 \to \mathbb{Z}_3$ by $\phi(\bar{a}) = -\bar{a}$ $\forall \bar{a} \in \mathbb{Z}_3$ $\therefore \phi \in Aut(\mathbb{Z}_3)$
& $\theta: \mathbb{Z}_2 \to Aut(\mathbb{Z}_3)$ by $\theta(\bar{0}) = i$ & $\theta(\bar{1}) = \phi$



CLAIM: $\mathbb{Z}_3 \rtimes_\theta \mathbb{Z}_2 \cong D_6$ ← In General, $\mathbb{Z}_n \rtimes_\theta \mathbb{Z}_2 \cong D_{2n}$

Pf: Let $1 = (\bar{0}, \bar{0})$, $r = (\bar{1}, \bar{0})$, $s = (\bar{0}, \bar{1})$

1.) $r^3 = 1$: $r = (\bar{1}, \bar{0})$

$\Rightarrow r^2 = (\bar{1}, \bar{0}) * (\bar{1}, \bar{0}) = (\bar{1} + [\theta(\bar{0})](\bar{1}), \bar{0} + \bar{0}) = (\bar{1} + i(\bar{1}), \bar{0})$
$= (\bar{1} + \bar{1}, \bar{0}) = (\bar{2}, \bar{0})$

$\Rightarrow r^3 = (\bar{2}, \bar{0}) * (\bar{1}, \bar{0}) = (\bar{2} + [\theta(\bar{0})](\bar{1}), \bar{0} + \bar{0}) = (\bar{2} + i(\bar{1}), \bar{0})$
$= (\bar{2} + \bar{1}, \bar{0}) = (\bar{0}, \bar{0}) = 1$

2.) $s^2 = 1$: $s = (\bar{0}, \bar{1})$

$\Rightarrow s^2 = (\bar{0}, \bar{1}) * (\bar{0}, \bar{1}) = (\bar{0} + [\theta(\bar{1})](\bar{0}), \bar{1} + \bar{1}) = (\bar{0} + \phi(\bar{0}), \bar{0})$
$= (\bar{0} + \bar{0}, \bar{0}) = (\bar{0}, \bar{0}) = 1$

3.) $rs = sr^{-1}$:

a.) $rs = (\bar{1}, \bar{0}) * (\bar{0}, \bar{1}) = (\bar{1} + [\theta(\bar{0})](\bar{0}), \bar{0} + \bar{1}) = (\bar{1} + i(\bar{0}), \bar{1})$
$= (\bar{1} + \bar{0}, \bar{1}) = (\bar{1}, \bar{1})$

b.) $sr^{-1} = (\bar{0}, \bar{1}) * (\bar{1}, \bar{0})^{-1} = (\bar{0}, \bar{1}) * (\bar{2}, \bar{0}) = (\bar{0} + [\theta(\bar{1})](\bar{2}), \bar{1} + \bar{0})$
$= (\bar{0} + \phi(\bar{2}), \bar{1}) = (\bar{0} + \bar{1}, \bar{1}) = (\bar{1}, \bar{1})$

$\therefore \mathbb{Z}_3 \rtimes_\theta \mathbb{Z}_2 \cong D_6$ ▨

$$\mathbb{Z}_3 \rtimes_\theta \mathbb{Z}_2 = \{(\bar{0},\bar{0}), (\bar{1},\bar{0}), (\bar{2},\bar{0}), (\bar{0},\bar{1}), (\bar{2},\bar{1}), (\bar{1},\bar{1})\}$$
$$\updownarrow \quad \updownarrow \quad \updownarrow \quad \updownarrow \quad \updownarrow \quad \updownarrow$$
$$D_6 = \{1, r, r^2, s, sr, sr^2\}$$

M® MIQUELRIUS

CH. 6: FURTHER TOPICS IN GROUP THEORY

Thurs. Dec 05 '13

Section 6.1 Solvable Groups

Def: A group G is **SOLVABLE** if $\exists$ a chain of subgroups $\{1_G\} = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \dots \trianglelefteq G_s = G$ s.t. G_{i+1}/G_i is Abelian for all $0 \le i \le s-1$

FACTS: Let G be a Group.

1.) $\{1_G\} \trianglelefteq G$:

Pf: Let $a \in G$

$\Rightarrow a\{1_G\}a^{-1} = \{a1_Ga^{-1}\} = \{aa^{-1}\} = \{1_G\}$

$\Rightarrow \{1_G\} \trianglelefteq G$ ▨

2.) $G/\{1_G\} \cong G$:

Pf: Define $\phi: G \to G$ by $\phi(x) = x \ \forall x \in G$

a.) Let $x, y \in G$

$\Rightarrow \phi(xy) = xy = \phi(x)\phi(y)$, so ϕ is a Homomorphism

b.) $\ker(\phi) = \{x \in G : \phi(x) = 1_G\} = \{x \in G : x = 1_G\} = \{1_G\}$

c.) For $x \in G$, $\phi(x) = x \in G$, so ϕ is Onto

$\therefore$ By F.I.T., $G/\{1_G\} \cong G$ ▨

3.) *If G is Abelian, then it is Solvable:*

Pf: Let G be Abelian.

a.) $\{1_G\} \trianglelefteq G$ by (1)

b.) $G/\{1_G\} \cong G$ is Abelian

$\therefore G$ is Solvable ▨

4.) *D_{2n} is Solvable:*

Pf: We know $\langle r \rangle \trianglelefteq D_{2n}$, since $|D_{2n} : \langle r \rangle| = \frac{2n}{n} = 2$

$\Rightarrow \{1\} \trianglelefteq \langle r \rangle \trianglelefteq D_{2n}$

a.) $\langle r \rangle/\{1\} \cong \langle r \rangle$ is Cyclic ($\therefore$ Abelian)

b.) $D_{2n}/\langle r \rangle = \{\langle r \rangle, s\langle r \rangle\} \cong \mathbb{Z}_2$ is Cyclic ($\therefore$ Abelian)

$\therefore D_{2n}$ is Solvable ▨

5.) For $n \ge 5$, S_n is NOT Solvable.

NOTATION: Let G be a Group & G' be its Commutator Subgroup. Then $G^{(0)} = G$, $G'' = (G')' = G^{(2)}$, & $G^{(n)} = (G^{(n-1)})'$

Thm: G is Solvable iff $G^{(n)} = \{1_G\}$ f.s. $n \ge 0$

M® MIQUELRIUS

PROP 10: Let G be a Group & $N \trianglelefteq G$. If N & G/N are both Solvable, then G is Solvable.

Thm: Every p-Group is Solvable.

Pf: Let p be prime. Let $|G| = p^\alpha$ s.s. $\alpha \geq 1$. Induct on α.

BASIC: $\alpha = 1 \leftarrow |G| = p$

$\Rightarrow G \cong \mathbb{Z}_p$ is Cyclic ($\therefore$ Abelian)

$\Rightarrow G$ is Solvable.

INDUCTIVE: Assume the Claim is true $\forall\ 1 \leq k < \alpha$. Let $|G| = p^\alpha$.

By Lagrange & Class Equation, we have $|Z(G)| | p^\alpha \wedge |Z(G)| > 1$.

$\Rightarrow Z(G) = p^{\alpha - a}$ s.s. $0 \leq a \leq \alpha - 1$

CASE 1: $a = 0$

$\Rightarrow Z(G) = p^{\alpha - 0} = p^\alpha = G$

$\Rightarrow G$ is Abelian ($\therefore$ Solvable)

CASE 2: $1 \leq a \leq \alpha - 1$

i.) $Z(G)$ is Abelian ($\therefore$ Solvable)

ii.) $Z(G) \trianglelefteq G$

$\Rightarrow G/Z(G)$ is a Group of size $p^{\alpha-(\alpha-a)} = p^a < p^\alpha = |G|$

$\Rightarrow G/Z(G)$ is Solvable by Induction Hypothesis

By (i) & (ii), G is Solvable.

$\therefore$ If $|G| = p^\alpha$ for any $\alpha \geq 1$, then G is Solvable. ▨

COROLLARY: If $|G| = 3^3 \cdot 11^4$, then G is Solvable.

Pf: Let $|G| = 3^3 \cdot 11^4$

$$\Rightarrow \begin{cases} \exists\ P \in Syl_{11}(G) \\ n_{11} \equiv 1 \pmod{11} \wedge n_{11} | 27 \end{cases}$$

$\Rightarrow n_{11} = 1$, since $3, 9, 27 \not\equiv 1 \pmod{11}$

$\Rightarrow P \trianglelefteq G$

a.) P is Solvable, since P is an 11-group

b.) $|G/P| = \frac{3^3 \cdot 11^4}{11^4} = 3^3$

$\Rightarrow G/P$ is a 3-group

$\Rightarrow G/P$ is Solvable

By (a) & (b), G is Solvable ▨

← BURNSIDE THEOREM

GENERAL CASE: If $|G| = p^\alpha q^\beta$ s.s. primes $p \neq q$, then G is Solvable.

MIQUELRIUS