Theorem 30

a) If G is an infinite cyclic group then $G \approx \mathbb{Z}$

b) If G is a finite cyclic group of order n then $G \approx \mathbb{Z}_n$

a) $G = \langle a \rangle$ define $\phi : G \to \mathbb{Z}$ by $\phi(a^k) = k$, $k \in \mathbb{Z}$

prove ϕ is an isom

b) $G = \langle a \rangle$ define $\phi : G \to \mathbb{Z}_n$

$\phi(a^k) = k \pmod n$, prove ϕ is an isom

$1^k = \overbrace{1 + 1 + 1 + \ldots + 1}^{k}$

Example 46 Let $G = \{1, -1, i, -i\}$, a group under complex multiplication

Recall $\phi : G \to \bar{G}$ isomorphism one-to-one, onto, OP: $\phi(ab) = \phi(a)\phi(b)$

Define $\phi : G \to \mathbb{Z}_4$ by $\phi(1) = 0$, $\phi(-1) = 1$, $\phi(i) = 2$, $\phi(-i) = 3$

a) Is ϕ an isomorphism?

ϕ is one-to-one and onto, OP $\phi(\underbrace{i \times -i}_{+ \bmod 4}) = \phi(1) = 0$

$\phi(\underbrace{i}_{=2}) + \phi(\underbrace{-i}_{=3}) = 2 + 3 = 5 \equiv 1 \pmod 4$

$0 \neq 1$, therefore it is not OP, not isomorphic

b) Is G isomorphic to $\mathbb{Z}_4$?

Note that $G = \langle i \rangle$ a cyclic group of order 4, so by Theorem 30 (above), says $G \approx \mathbb{Z}_4$, so answer is yes.

Important: Even if a certain ϕ is not an isomorphism does not mean the groups are not isomorphic.

Example 47 Show that $(\mathbb{Q}, +)$ and $(\mathbb{Q}^*, \times)$ are not isomorphic

Proof by contradiction, suppose $\phi : (\mathbb{Q}, +) \to (\mathbb{Q}^*, \times)$

$2 = \underset{\in \mathbb{Q}^*}{\phi(x)}$, $x \in \mathbb{Q}$ (onto)

$$= \phi\left(\tfrac{x}{2} + \tfrac{x}{2}\right)$$

$$\overset{\text{op}}{=} \phi\left(\tfrac{x}{2}\right) \cdot \phi\left(\tfrac{x}{2}\right)$$

$$= \left[\phi\left(\tfrac{x}{2}\right)\right]^2$$

So $2 = \underset{\in \mathbb{Q}^*}{\left[\phi\left(\tfrac{x}{2}\right)\right]^2}$ but $\sqrt{2} \notin \mathbb{Q}$

$\therefore$ Contradiction, $(\mathbb{Q}, +)$ and $(\mathbb{Q}, \cdot)$ are not isomorphic

Proposition 31 Suppose ϕ is an isomorphism from G to H. Let $n \in \mathbb{Z}$ and $a, b \in G$

$\phi : G \to H$

i) $\phi(e_a) = e_H$

ii) $\phi(a^n) = (\phi(a))^n$ Note: $n = -1$, $\phi(a^{-1}) = (\phi(a))^{-1}$

iii) $ab = ba \iff \phi(a)\phi(b) = \phi(b)\phi(a)$

iv) $G = \langle a \rangle \iff H = \langle \phi(a) \rangle$ ϕ takes a generator to a generator

v) $|a| = |\phi(a)|$

vi) $x^n = a$ has the same number of solutions in G as $x^n = \phi(a)$ does in H

vii) If G and H are finite then they have the same number of elements of each order

iii) Let $a, b \in G$

$\Rightarrow$ Suppose $ab = ba$, then $\phi(a)\phi(b) \overset{\text{op}}{=} \phi(ab) = \phi(ba) \overset{\text{op}}{=} \phi(b)\phi(a)$

$\Leftarrow$ Suppose $\phi(a)\phi(b) = \phi(b)\phi(a)$ WTS $ab = ba$

Then $\phi(ab) \overset{\text{op}}{=} \phi(a)\phi(b)$

$= \phi(b)\phi(a) \overset{\text{op}}{=} \phi(ba)$

So $\phi(ab) = \phi(ba)$, ϕ is one to one so $ab = ba$ ∎

Proposition 32 Suppose ϕ is an isomorphism from G to H

i) ϕ^{-1} is an isom from H to G

ii) G is Abelian iff H is abelian

iii) G is cyclic iff H is cyclic

iv) If $K \leq G$ then $\phi(K) = \{\phi(x) \mid x \in K\}$ is a subgroup of H

v) $|G| = |H|$

vi) If ψ is an isomorphism from H to a group F then $\psi \circ \phi$ is an isomorphism from G to F

vii) $\phi(Z(G)) = Z(H)$

i) $\phi: G \to H$ is an isomorphism, since ϕ is a bijection, ϕ^{-1} exists and it is also a bijection. Now is ϕ^{-1} OP?

Suppose $h_1, h_2 \in H$, WTS $\phi^{-1}(h_1 h_2) = \phi^{-1}(h_1)\,\phi^{-1}(h_2)$

There exists $g_1, g_2 \in G$ st $\phi(g_1) = h_1$

$\phi(g_2) = h_2$ since ϕ is onto

Then: $\phi^{-1}(h_1 h_2) = \phi^{-1}(\phi(g_1)\,\phi(g_2)) = \phi^{-1}(\phi(g_1 g_2)) = g_1 g_2$

$\phi^{-1}(h_1)\,\phi^{-1}(h_2) = \phi^{-1}(\phi(g_1))\,\phi^{-1}(\phi(g_2)) = g_1 g_2$

So $\phi^{-1}(h_1 h_2) = \phi^{-1}(h_1)\,\phi(h_2)$ so ϕ^{-1} is OP, so ϕ^{-1} is isomorphic

Example 48 Which of the following groups are isomorphic to which? isom classes

A_4

G = subgroup of S_{15} generated by $a = \langle a \rangle$ where $a = (123\ldots12)$

$\mathbb{Z}_{12}$

D_6

S_4

$G \approx \mathbb{Z}_{12}$ because $\mathbb{Z}_{12}$ is cyclic of order 12 and G is cyclic of order 12, so they are isomorphic by Theorem 30b

Also $|A_4| = \frac{4!}{2} = 12$ $\quad |\mathbb{Z}_{12}| = 12$ $\quad |D_6| = 12$ $\quad |S_4| = 4! = 24$ $\quad |G| = 12$

So S_4 cannot be isom to any others

D_6 is not cyclic so $D_6 \not\approx \mathbb{Z}_{12}$, $D_6 \not\approx G$

A_4 is not cyclic so $A_4 \not\approx \mathbb{Z}_{12}$, $A_4 \not\approx G$

The largest possible order of an element in D_6 is 6

In A_4 has no element of order 6, so $A_4 \not\approx D_6$

Chapter 7

Suppose H is a subgroup of G, how are $|H|$ and $|G|$ related, Clearly $|H| \leq |G|$.

Let $G = S_3 = \{e, (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$ $\quad e = (1) = (1)(2)(3)$

The subgroups of S_3 are:

$H_0 = S_3$ $\quad H_1 = \{e\}$ $\quad H_2 = \{e, (1\,2)\}$ $\quad H_3 = \{e, (1\,3)\}$

$H_4 = \{e, (2\,3)\}$ $\quad H_5 = \{e, (1\,2\,3), (1\,3\,2)\}$

It seems like (at least in this example) $|H|$ divides $|S_3|$, can this be true in general? Let's examine $H_2 = \{e, (1\,2)\}$, $H = \{e, (1\,2)\} \leq S_3$

Choose an element in S_3, which is not in H: eg (13)

Then let $A = \{(1\,3)e, (1\,3)(1\,2)\}$

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

Now choose an element in S_3 which is not in H, nor in A, eg (2 3)

Let $B = \{(2\,3)e, (2\,3)(1\,2)\}$

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

Now $|S_3| = |H| + |A| + |B|$

So $|S_3| = 3|H|$ so $|H|$ divides $|S_3|$

We used H to partition S_3 into sets of size $|H|$ so that $|H|$ divides $|S_3|$

Generalize the ideas to prove that in general, the order of a subgroup must divide the order of a group

Definition Suppose G is a group $a \in G$ and H a non-empty subset of G

i) Define $aH = \{ah \mid h \in H\}$ If H is a subgroup of G, we say that aH is the left coset of H in G, containing a. Then a is a coset representative

ii) Define $Ha = \{ha \mid h \in H\}$ ... right coset

iii) Define $aHa^{-1} = \{aha^{-1} \mid h \in H\}$ ... double coset

We write $|aH|$ to mean the size, even if its not a subgroup

Warning A coset is not necessarily a subgroup

Example 50 Consider $D_3 = \{R_0, R_{120}, R_{240}, F_V, F_R, F_L\}$

$H = \{R_0, F_V\}$ Find $R_{120}H$, HR_{120}, and $F_R H$

$R_{120}H = \{R_{120}R_0, R_{120}F_V\} = \{R_{120}, F_R\}$

$HR_{120} = \{R_0 R_{120}, F_V R_{120}\} = \{R_{120}, F_L\}$ Notice $R_{120}H \neq HR_{120}$

$F_R H = \{F_R R_0, F_R F_V\} = \{F_R, R_{120}\}$

Lemma 33 Suppose G is a group, $a, b \in G$, H a subgroup of G, then

i) $a \in aH$

ii) $aH = H \iff a \in H$

iii) $(ab)H = a(bH)$ and $H(ab) = (Ha)b$

iv) $aH = bH \iff a \in bH$

v) $aH = bH \iff a^{-1}b \in H$

vi) For all $a, b \in G$ either $aH = bH$ or $aH \cap bH = \emptyset$ (disjoint)

vii) $|aH| = |bH|$

viii) $aH = Ha \iff H = aHa^{-1}$

ix) aH is a subgroup of $G \iff a \in H$

vi) Let $a, b \in G$ suppose $aH \cap bH \neq \emptyset$, WTS $aH = bH$

so $\exists\ c \in aH \cap bH$, then $c \in aH \iff cH = aH$

$c \in bH \qquad cH = bH$

$\Rightarrow aH = bH$

vii) Define $\phi : aH \to bH$ by $\phi(ah) = bh$ for $h \in H$

Onto If $bh_1 \in bH$ then $\phi(ah_1) = bh_1$, so its onto

One to One Suppose $\phi(ah_1) = \phi(ah_2)$

$\Rightarrow bh_1 = bh_2$

$\Rightarrow h_1 = h_2$

$\Rightarrow ah_1 = ah_2$

So its one-to-one, so its a bijection so $|aH| = |bH|$ ■

Example 51 Consider $G = \mathbb{Z}$, subgroup $H = 3\mathbb{Z} = \{3n \mid n \in \mathbb{Z}\} = \langle 3 \rangle$

What are the left cosets? How many are there?

Operation is $+$ so aH is often written $a + H$, $H = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$

$0 + H = H$

$1 + H = \{1 + h \mid h \in H\} = \{1 + 3n \mid n \in \mathbb{Z}\} = \{x \in \mathbb{Z} \mid x \equiv 1 \bmod 3\}$

$2 + H = \{2 + h \mid h \in H\} = \{x \in \mathbb{Z} \mid x \equiv 2 \bmod 3\}$

$3 + H = H$

$4 + H = 1 + H$

So there are only 3 distinct left cosets