automorphism of group G

$=$ isomorphism $\Phi: G \to G$

Examples: (1) inner automorphism: α_a

Fix $a \in G$:

Define $\alpha_a(g) = aga^{-1}$

checked: α_a is an automorphism

If G abelian: $\alpha_a(g) = g \quad \forall g \in G$

i.e. $\alpha_a = id: G \to G$

(2) have seen:

$\Phi(x) = -x$ is an autom. of $(\mathbb{R}, +)$

and also of $(\mathbb{Z}, +)$

Determine all automorphisms of a cyclic group!

Theorem: (a) $G = (\mathbb{Z}, +)$

There are only two automorphisms, namely

$\alpha(k) = k$ for all $k \in \mathbb{Z}$

and $\alpha(k) = -k$

(b) If $G = \mathbb{Z}_n$, α an autom.

$\Rightarrow \exists\, j$ with $\gcd(j, n) = 1$ s.t.

$\alpha(k) = jk$ for all $k \in \mathbb{Z}_n$

in particular, we have exactly $\phi(n)$ automorphisms

where $\phi(n) = \#\{j,\ 0 < j < n,\ \gcd(j, n) = 1\}$

Example: $n=5$ $j=3$

$\alpha(k) = 3k \mod 5$

$\alpha(0) = 0$

$\alpha(1) = 3$

$\alpha(2) = 3 \cdot 2 = 6 \mod 5 = 1$

$\alpha(3) = 9 \mod 5 = 4$

$\alpha(4) = 12 \mod 5 = 2$

easy to see here: α is 1-1 and onto

proof of theorem:

crucial observation: if r is a generator of a cyclic group G and α is an autom of G

$\Rightarrow$ $\alpha(r)$ is a generator!

(a) $G = \mathbb{Z}$ α an autom. of $\mathbb{Z}$

possible generators of $\mathbb{Z}$: ± 1

by observation above: $\alpha(1) = \pm 1$

in general: $\alpha(k) = \alpha(\underbrace{1 + 1 + \dots + 1}_{k \text{ times}})$

↑ additive not.!

$= \alpha(1) + \alpha(1) + \dots + \alpha(1)$

$= k\,\alpha(1)$

$\alpha(1) = 1 \Rightarrow \alpha(k) = k \cdot 1 = k$ $\Rightarrow$ claim

$\alpha(1) = -1 \Rightarrow \alpha(k) = k \cdot (-1) = -k$

have already seen: these are indeed automorphisms of $\mathbb{Z}$

(b) $G = \mathbb{Z}_n$ again: 1 is a generator of $\mathbb{Z}_n$

$\Rightarrow$ $\alpha(1)$ must be a generator of $\mathbb{Z}_n$

let $\alpha(1) = j$

as in (a): $\alpha(k) = \alpha(1 + \dots + 1) = \underbrace{\alpha(j) + \dots \alpha(1)}_{k \text{ times}}$ (k-times)

$= k\alpha(1) = kj$

$\Rightarrow$ α already determined by $\alpha(1) = j$.

need to check: $\alpha(k) = jk$, $k = 0, 1, \dots n-1$

is an autom. of $\mathbb{Z}_n$.

to check 1-1 (and onto) recall:

$\gcd(j, n) = 1 \Rightarrow \exists\, s \in \mathbb{Z}_n$ s.t. $\boxed{sj \bmod n = 1}$

check 1-1: assume $\alpha(k) = \alpha(\ell) \Leftrightarrow jk = j\ell \bmod n$

multiply by $s \Rightarrow sjk = sj\ell \bmod n$

multipl. by $sj \bmod n$ = multipl. by $1 \bmod n \Rightarrow 1 \cdot k = 1 \cdot \ell \bmod n \Rightarrow$ 1-1 ✓

(aside: example: $n=5$ $j=2$ $\Rightarrow s=3$

$sj = 6 = 1 \bmod n$

$k=4$

$\Rightarrow sjk = 6\cdot 4 = 24 = 4 \bmod 5$

$= (1)\cdot 4 = 4 \bmod 5$

used $sj \bmod 5 = 1$ $= k$

hence in general $\boxed{sjk = k \bmod n}$

onto: given $\ell \in \mathbb{Z}_n$ need to find k s.t.

$\alpha(k) = \ell$ i.e. $\boxed{jk = \ell \bmod n}$

Recall: s is the inverse of $j \bmod n$ (for multiplication!)

solve for k by multiplying by $s = j^{-1}$

$\Rightarrow$ $(sj)k = s\ell \bmod n$ $\Rightarrow$ $\boxed{k = s\ell \bmod n}$

$\bmod n = 1$

Ex. $\alpha(k) = 2k$ $\quad j = 2$

$s = 3$

Find k s.t.

$$\alpha(k) = 3$$

$$\Leftrightarrow \quad 2k \bmod 5 = 3$$

Solution: multiply 3 by $2^{-1} = 3 \bmod 5$

$$3 \cdot 3 = 9 = 4 \bmod 5$$

$$\Rightarrow \boxed{k = 4}$$

indeed $\alpha(4) = 2 \cdot 4 = 8 = 3 \bmod 5$ ✓

have shown: 1-1 and auto preserve operation: $\boxed{\alpha(k) = jk}$

$$\alpha(k+e) = j(k+e) = jk + je \bmod n$$

$$= \alpha(k) + \alpha(e)$$

Remark: Our theorem classifies all autom. for any cyclic group.

Corollary. $G = \langle a \rangle$ cyclic. α an autom. of G

(a) if $\text{ord}(a) = \infty \Rightarrow$ only 2 possibilities for α

either $\alpha(a^k) = a^k$ for all $k \in \mathbb{Z}$

or $\alpha(a^k) = a^{-k}$ " " "

(b) If $\text{ord}(a) = n$

$\Rightarrow$ have $\phi(n)$ automorphisms α given by

$$\alpha(a^k) = a^{jk}, \text{ where } \gcd(j,n) = 1$$

proof. repeat proof of theorem for multiplicative notation)

(fancier way: we know that $\langle a \rangle \cong \mathbb{Z}$ or $\mathbb{Z}_n$

(only do it for $\mathbb{Z}_n$) $\Rightarrow$ if α an autom of $\langle a \rangle$ and $\phi: \mathbb{Z}_n \to \langle a \rangle$ isom.

$\Rightarrow$ can pull back autom. of $\langle a \rangle$ to autom. of $\mathbb{Z}_n$

α autom. of $\langle a \rangle$

$\phi(k) = a^k$

$\Rightarrow$ $\phi^{-1} \circ \alpha \circ \phi : \mathbb{Z}_n \to \mathbb{Z}_n$ autom.

$\Rightarrow$ $\phi^{-1} \circ \alpha \circ \phi(k) = jk$ for some j with $\gcd(j, n) = 1$

$\Rightarrow$ $\alpha \circ \phi(k) = \phi(jk)$

$\alpha(a^k) = a^{jk}$ $\Rightarrow$ claim.