Previously in math 103a

G group, $\underline{Aut(G)} = \{$ all automorphisms of $G\}$

Inner automorphism: $a \in G$, $\varphi_a : G \to G$

$\varphi_a(x) = axa^{-1}$

Thm. $Aut(G)$ & $Inn(G)$ are groups under composition.

An intriguing isomorphisms

Thm. $Aut(\mathbb{Z}_n) \approx U(n)$.

$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ addition mod n

$U(n) = \{k : 1 \le k < n, \gcd(k, n) = 1\}$ mult. mod n.

Useful facts about isomorphism $\varphi : G \to \bar{G}$

(a) $\varphi(e) = \bar{e}$ e identity $\in G$, $\bar{e}$ identity $\in \bar{G}$

(b) If G cyclic generated by a, then $\bar{G}$ cyclic generated by $\varphi(a)$ & φ is completely determined by the choice of $\varphi(a)$.

(c) $H \le G \Rightarrow \varphi(H) \le \bar{G}$

(d) $ab = ba \Rightarrow \varphi(a)\varphi(b) = \varphi(b)\varphi(a)$; G abelian $\Rightarrow \bar{G}$ abelian

Idea of proof of Thm

Try to define $\Phi : U(n) \longrightarrow Aut(\mathbb{Z}_n)$ (*)

by $\Phi(j)(k) = (jk) \bmod n$ (**)

To simplify notation, write φ_j for $\Phi(j)$

Need to show:

① $\forall j \in U(n)$, $\varphi_j : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$ is an isomorphism, i.e. $\varphi_j \in Aut(\mathbb{Z}_n)$

this will show that Φ is as in (*), a mapping from $U(n)$ to $Aut(\mathbb{Z}_n)$

② Show Φ is 1-1.

③ Show Φ is onto $Aut(\mathbb{Z}_n)$.

④ Show that Φ preserves operations

i.e. $\Phi((j_1 j_2 \bmod n)(k)) = \varphi_{j_1} \circ \varphi_{j_2}(k)$

To prove ① → ④, need to understand $Aut(\mathbb{Z}_n)$

Ex: $n = 12$. $\mathbb{Z}_{12}$ is cyclic with generators

$\{k : 1 \le k < 12, \gcd(k, 12) = 1\} = U(12)$

Reason: $k \in \mathbb{Z}_n$ is a generator $\Leftrightarrow |k| = |\mathbb{Z}_n| = n$

We've shown: $|k| = \frac{n}{\gcd(n,k)}$

$U(12) = \{1, 5, 7, 11\}$ generators of $\mathbb{Z}_{12}$

Property (b) of facts about isomorphisms says if $\varphi: \mathbb{Z}_{12} \longrightarrow \mathbb{Z}_{12}$ is an automorphism Then $\varphi(1) = 1$ or 5 or 7 or 11

and also, the choice of $\varphi(1)$ determines φ.

Suppose $\varphi(1) = 5$. Then

$\varphi(2) = \varphi(1+1) = 5+5 = 10$
$\varphi(3) = 15 \bmod 12 = 3$
$\varphi(4) = 3+5 = 8$
$\varphi(5) = (8+5) \bmod 12 = 1$
$\varphi(6) = 1+5 = 6$
$\varphi(7) = 6+5 = 11$
$\varphi(8) = 16 \bmod 5 = 4$
$\varphi(9) = 9$
$\varphi(10) = 2$
$\varphi(11) = 7$

$\varphi(0) = 0$
identity $\longmapsto$ identity

i.e. $\varphi(h) = (\underbrace{5+5+\cdots 5}_{k}) \bmod 12$

$= 5k \bmod 12$

In general, any automorphism of $\mathbb{Z}_n$ is of the form φ_j, where $j \in U(n)$ with $\varphi_j(h) = (jh) \bmod n$, $h \in \mathbb{Z}_n$.

since $\varphi_j(1) = j$, $\varphi_j \neq \varphi_{j'}$, $j, j' \in U(n)$, $j \neq j'$

Hence $\Phi: U(n) \longrightarrow Aut(\mathbb{Z}_n)$ is 1-1 & onto.

Need to check (4): Φ preserves operations.

$$\Phi((j_1 j_2) \bmod n)(k) = ((j_1 j_2) \bmod n \cdot k) \bmod n$$
$$= j_1[(j_2 k) \bmod n] \bmod n$$
$$= \varphi_{j_1}(\varphi_{j_2}(k))$$
$$= (\varphi_{j_1} \circ \varphi_{j_2})(k) \quad //$$

Note: We could also define $T: Aut(\mathbb{Z}_n) \longrightarrow U(n)$

by $T(\varphi) = \varphi(1)$ $\quad \varphi \in Aut(\mathbb{Z}_n)$

How is T related to Φ?

$$\begin{array}{ccccc} \varphi & \xrightarrow{T} & \varphi(1) & \xrightarrow{\Phi} & \varphi \\ \uparrow & & \uparrow & & \uparrow \\ Aut(\mathbb{Z}_n) & & U(n) & & Aut(\mathbb{Z}_n) \end{array}$$

$\therefore T = \Phi^{-1}$

Subgroups, cosets & Lagrange's Thm

Chap. 7 in text.

Lagrange's Thm. G finite group, $H \leq G$

$\Rightarrow |H|$ divides $|G|$.

Cor 2. $a \in G \Rightarrow |a| \mid |G|$

Pf: $|a| = |\langle a \rangle|$, $\langle a \rangle \leq G$.

Apply Thm.

Cor 3. If $|G| = p$ prime, then G is cyclic & every $a \in G$, $a \neq e$, is a generator of G

Pf: $|a|$ divides p (by Cor 2).
$\therefore |a| = p$ (unless $a = e$)
$\therefore |\langle a \rangle| = |G| \Longrightarrow \langle a \rangle = G.$ //

Cor 4 If $|G| < \infty$, $a \in G$, then

$$a^{|G|} = e$$

Pf Need to show $|a|$ divides $|G|$,
since then $a^{|G|} = a^{|a|q} = (e)^q = e.$
$\therefore$ Follows from Cor 2. //

Cor 5. (Fermat's Little Thm)

$a \in \mathbb{Z}$, p prime $\Longrightarrow$ $a^p \bmod p = a \bmod p.$

Pf: $U(p) = \{1, 2, \ldots, p-1\}$, $|U(p)| = p-1$
$a \bmod p \in U(p)$ if $a \neq 0$ (which we may assume. Why?)
$\therefore (a \bmod p)^{p-1} = 1$ by Cor 4

$\therefore (a \bmod p)^{p-1} = a^{p-1} \bmod p = 1$
$\therefore a^p \bmod p = (a^{p-1} a) \bmod p = a \bmod p$ //

To prove Lagrange's Thm, we need cosets!

Def. Cosets: G group, $H \leq G$, $a \in G$

The cosets of H containing a are

$aH = \{ah : h \in H\}$ left coset

$Ha = \{ha : h \in H\}$ right coset

Note: If G is abelian, then $aH = Ha$.

In general, $aH = Ha \iff aHa^{-1} = H$.

Ex. 1. $G = S_3$, $H = \{(1), (123), (132)\} = A_3$ alternating gp.

$a = (12)$

$aH = \{(12), (12)(123), (12)(132)\}$

$= \{(12), (32), (31)\}$

$Ha = \{(12), (123)(12), (132)(12)\}$

$= \{(12), (13), (23)\}$

In this case $aH = Ha$, although S_3 not abelian.

In text, see example of subgroup K of S_3 and $a \in S_3$ for which $aK \neq Ka$.

---

what happens if $a \in H$?

Then $ah \in H \ \forall \ h \in H \implies aH = H$.