① MATH 407

4/4/18

Chap 3.3 (contd.)

$S \subseteq G$

$\langle S \rangle$ = smallest subgroup of G containing S (or strings)

Words in S: $s_1^{\pm}, s_2^{\pm}, \ldots, s_k^{\pm} \in \langle S \rangle$

$$(s_1^{\pm}, s_2^{\pm}, \ldots, s_k^{\pm}) \cdot (\tau_1^{\pm}, \tau_2^{\pm}, \ldots, \tau_\ell^{\pm})$$

$$(s_1^{\pm}, \ldots, s_k^{\pm})^{-1} = s_k^{\mp}, \ldots, s_1^{\mp}$$

Strings in S are closed under + and $\cdot$.

⊛ Isomorphism

Def. G_1, G_2 are groups
$\Phi : G_1 \to G_2$ is a homomorphism
iff for any $\{a,b\} \subseteq G_1$
$\Phi(ab) = \Phi(a)\Phi(b)$
If Φ is a bijection, then it's isomorphic

Prop. If Φ is a homomorphism,
then 1) $\Phi(e_1) = e_2$
2) $\Phi(a^{-1}) = [\Phi(a)]^{-1}$ $\forall a \in G$

$(\longrightarrow)$

Pf. e_1 only $g \in G_1$, $g^2 = g$

$$[\Phi(e_1)]^2 = \Phi(e_1)\Phi(e_1) = \Phi(e_1^2) = \Phi(e_1)$$

ii) $\Phi(a)\Phi(a^{-1})$

$= \Phi(aa^{-1})$

$= \Phi(e_1) = e_2$

$\Phi(a)^{-1} = \Phi(a^{-1})$

* Let $\Phi_1 : G_1 \to G_2$

$\Phi_2 : G_2 \to G_3$

be homomorphisms

then $\Phi_2 \circ \Phi_1 : G_1 \to G_3$ is homomorphic.

$$\Phi_2 \circ \Phi_1(ab) = \Phi_2(\Phi_1(ab))$$
$$= \Phi_2(\Phi_1(a)\Phi_1(b))$$
$$= \Phi_2(\Phi_1(a)) \cdot \Phi_2(\Phi_1(b))$$

* If $\Phi : G_1 \to G_2$ is isomorphic,

then $\Phi^{-1} : G_2 \to G_1$ is also isomorphic.

Pf Let $a, b \in G_1$ have $c = \Phi_1(a)$, $d = \Phi_1(b)$

Then, $a = \Phi_1^{-1}(c)$, $b = \Phi_1^{-1}(d)$

Look at: $\Phi_1^{-1}(cd) = \Phi_1^{-1}(\Phi_1(ab)) = ab$

$= \Phi^{-1}(c)\Phi^{-1}(d)$

3

Cor. If G is a group, then,

$$Aut(G) = \{ \Phi : G \to G \text{ isomorphism} \}$$

is a group.

($Aut(G)$:= automorphism)

* Let $G_1 \simeq G_2$ if there is isomorphism $\Phi : G_1 \to G_2$
('$\simeq$' := is isomorphic to)

Thm. '$\simeq$' is an equivalence relation on groups.

i) Reflexivity: $G \simeq G$

ii) Symmetry: $G_1 \simeq G_2$

$$\Phi : G_1 \to G_2$$

Then, $\Phi^{-1} : G_2 \to G_1$

$$G_2 \simeq G_1$$

iii) Transitivity: $G_1 \simeq G_2$, $G_2 \simeq G_3$,
then $G_1 \simeq G_3$ (by composition)

* Isomorphism Classes:

$$[G]_{\simeq} = \{ H : G \simeq H \}$$

Ex. * $[\{e\}]_{\simeq} = \{\{e\}\}$

* If p is prime, $|G| = p$ then $G \cong \mathbb{Z}_p$ $([\mathbb{Z}_p])$

* $\Phi : n \to a^n$ is isomorphism from $\mathbb{Z}_p$ to G

$$(n_1 + n_2) \to a^{n_1+n_2}$$
$$= a^{n_1} a^{n_2} \quad ([\mathbb{Z}_p]_{\simeq})$$

* If G is infinite cyclic $G = \langle a \rangle$

$$n \to a^n$$
$$\mathbb{Z} \to G \text{, isomorphism}$$

* Order 4:

$[\mathbb{Z}_4]$, [Klein Group (not cyclic)]

$\mathbb{Z}_2 \times \mathbb{Z}_2$

$\times$	(0,0)	(1,0)	(0,1)	(1,1)
(0,0)	(0,0)	(1,0)	(0,1)	(1,1)
(1,0)	(1,0)	(0,0)	(1,1)	(0,1)
(0,1)	(0,1)	(1,1)	(0,0)	(1,0)
(1,1)	(1,1)	(0,1)	(1,0)	(0,0)

$(\to)$

5

* Order 6: $[\mathbb{Z}_6]$, $[S_3]$

$\langle a,b\rangle$, $ab=ba$, $a^2b=ba$

* $G_1 \times G_2$ direct product

$(a_1,a_2)\cdot(b_1,b_2)$
$=(a_1b_1, a_2b_2)$, $o(a_1,a_2)=\operatorname{lcm}(o(a_1),o(a_2))$

* $G_1 \times G_2$ cyclic. Any subgroup is cyclic

$H_1 = G_1 \times \{e_2\} = \{(a_1,e_2) : a_1 \in G_1\}$
$H_2 = \{e_1\} \times G_2 = \{(e_1,a_2) : a_2 \in G_2\}$

$\Phi_1 : G_1 \to G_1 \times G_2$
$\Phi_1(a_1) = (a_1, e_2)$
$\Phi_2 : G_2 \to G_1 \times G_2$
$\Phi_2(a_2) = (e_1, a_2)$

* Let $\langle a_1\rangle = G_1$, $\langle a_2\rangle = G_2$

$|G_1| = o(a_1)$, $|G_2| = o(a_2)$
$|G_1 \times G_2| = o(a_1)\cdot o(a_2)$

Want $G_1 \times G_2 = \langle (a_1,a_2)\rangle$
$|G_1 \times G_2| = o(a_1,a_2)$

$$|G_1 \times G_2| = o(a_1)\, o(a_2)$$
$$= \mathrm{lcm}(o(a_1), o(a_2))$$
$$\text{iff } \gcd(o(a_1), o(a_2)) = 1$$

↳ $\mathbb{Z}_2 \times \mathbb{Z}_3$

$\mathbb{Z}_n \times \mathbb{Z}_m$ are cyclic iff $\gcd(n, m) = 1$