Chapter 8: External Direct Products

Given two or more groups, there is an easy way to make way to make more groups

Definition Suppose $G_1, G_2, \ldots, G_n$ are groups.
Then $G_1 \oplus G_2 \oplus \ldots \oplus G_n = \{(g_1, g_2, \ldots, g_n) \mid g_i \in G_i\}$ and the operation is component wise ie: $(g_1, g_2, \ldots, g_n) * (h_1, h_2, \ldots, h_n) = (g_1 h_1, g_2 h_2, \ldots, g_n h_n)$

It is easy to prove that this is a group. It is called the external direct product of $G_1, G_2, \ldots G_n$

Example Consider $U(4) \oplus \mathbb{Z}_4$

a) List the elements. What is $|U(4) \oplus \mathbb{Z}_4|$?

$U(4) = \{1, 3\}$ $\qquad$ $\mathbb{Z}_4 = \{0, 1, 2, 3\}$

$U(4) \oplus \mathbb{Z}_4 = \{(1,0), (1,1), (1,2), (1,3), (3,0), (3,1), (3,2), (3,3)\}$

$|U(4) \oplus \mathbb{Z}_4| = 2 \cdot 4 = 8$

b) Compute $(3,1) * (3,2) = (\overset{U(4)}{3 \cdot 3}, \overset{\mathbb{Z}_4}{1+2})$

$= (1, 3)$ $\qquad$ $(g_1, g_2) * (h_1, h_2) = (\underset{\text{in } G_1}{g_1 h_1}, \underset{\text{in } G_2}{g_2 h_2})$

c) What is the identity element?

$(1, 0) * (x, y) = (x, y) \Rightarrow e = (1, 0)$ which is in $U(4)$

d) Find the inverse of $(3, 3)$

$(3, 3)^{-1} \Rightarrow (3, 3) * (\underline{3}, \underline{1}) = (1, 0)$

3^{-1} in $U(4)$; 1 in $\mathbb{Z}_4$

Proposition 43 In $G_1 \oplus G_2 \oplus \dots \oplus G_n$

Suppose G_i is a group and e_i is the identity in G_i and $g_i \in G_i$, Then:

i) $|G_1 \oplus G_2 \oplus \dots \oplus G_n| = |G_1| \cdot |G_2| \cdot \dots \cdot |G_n|$

ii) $e = (e_1, e_2, \dots, e_n)$

iii) $(g_1, g_2, \dots, g_n)^{-1} = (g_1^{-1}, g_2^{-1}, \dots g_n^{-1})$

iv) $|(g_1, g_2, \dots, g_n)| = \text{lcm}(|g_1|, |g_2|, \dots, |g_m|)$

iv) Let $S = \text{lcm}(|g_1|, |g_2|, \dots, |g_n|)$

and $t = |(g_1, g_2, \dots, g_n)|$, WTS $s = t$

step 1 $(g_1, g_2, \dots, g_n) = (g_1^s, g_2^s, \dots, g_n^s)$

componentwise OP

$= (e_1, e_2, \dots, e_n)$ $\quad (g_1, g_2)^3 = (g_1, g_2) * (g_1, g_2) * (g_1, g_2) = (g_1^3, g_2^3)$

So $(g_1, g_2, \dots, g_n)^s = (e_1, e_2, \dots e_n)$

$\Rightarrow t \leq s$

$\Rightarrow t$ is the smallest positive integer s.t. $(g_1, g_2, \dots, g_n)^t = e$

step 2 WTS $s \leq t$

$(e_1, e_2, \dots, e_n) = (g_1, g_2, \dots, g_n)^t$

def of t

componentwise $\rightarrow = (g_1^t, g_2^t, \dots, g_n^t)$

smallest positive int $\rightarrow$ order of an element

So $\forall i \quad g_i^t = e_i$

$\Rightarrow t$ is a multiple of $|g_i|$

$\Rightarrow t \geq s \Rightarrow t = s$

Example 61 Consider $G = \mathbb{Z}_{21} \oplus \mathbb{Z}_7$

a) What is $|G|$?

$|\mathbb{Z}_{21} \oplus \mathbb{Z}_7| = 21 \times 7 = 147$

b) What is $|x|$ if $x = (14, 5) \in G$?

$|x| = |(14, 5)| = \text{lcm}(|14|, |5|)$

$|14|$ in $\mathbb{Z}_{21}$: $14^n = 0 \pmod{21}$

$14 + 14 + \ldots + 14 = 0 \pmod{21}$

$n \cdot 14 \equiv 0 \pmod{21}$

$14 \cdot n =$ multiple of 21

$n = 3$ is the smallest one that works

$|14| = 3$ in $\mathbb{Z}_{21}$

$|5|$ in $\mathbb{Z}_7$: order of an element must divide order of group

$|5| \mid |\mathbb{Z}_7|$ so $|5| = 1$ or 7

only e has order 1 so $|5| = 7$

So $|x| = \text{lcm}(|14|, |5|) = \text{lcm}(3, 7) = 21$

Theorem 44 Suppose G and H are finite cyclic groups. Then $G \oplus H$ is cyclic iff $|G|$ and $|H|$ are relatively prime.

Corollary 45 Suppose $G_1, G_2, \ldots, G_n$ are finite cyclic groups. Then $G_1 \oplus G_2 \oplus \ldots \oplus G_n$ is cyclic iff $|G_i|$ and $|G_j|$ are relatively prime for all $i \neq j$.

Corollary 46 $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \ldots \oplus \mathbb{Z}_{n_k}$ is isomorphic to $\mathbb{Z}_m$ where $m = n_1 \cdot n_2 \cdot \ldots \cdot n_k$ iff $\gcd(n_i, n_j) = 1 \quad \forall\, i \neq j$

$\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \dots \oplus \mathbb{Z}_{n_k} \approx \mathbb{Z}_m$

$\Leftrightarrow \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \dots \oplus \mathbb{Z}_{n_k}$ is cyclic — prop 30

$\Leftrightarrow |\mathbb{Z}_{n_i}|$ and $|\mathbb{Z}_{n_j}|$ are relatively prime $\forall i \neq j$ — cor 45

$\Leftrightarrow n_i$ and n_j are relatively prime $\forall i \neq j$

Example 62

$\mathbb{Z}_3 \oplus \mathbb{Z}_7 \approx \mathbb{Z}_{21}$ $\quad \gcd(3,7) = 1$

$\mathbb{Z}_3 \oplus \mathbb{Z}_6 \not\approx \mathbb{Z}_{18}$ $\quad \gcd(3,6) = 3 \neq 1$

Proposition 48 If $m = n_1 n_2 \dots n_k$ where $\gcd(n_i, n_j) = 1$, $\forall i \neq j$.

Then $U(m) \approx U(n_1) \oplus U(n_2) \oplus \dots \oplus U(n_k)$

Theorem 49 If n is a positive integer and p a prime $p \geq 3$ then

$U(p^n) \approx \mathbb{Z}_{p^n - p^{n-1}}$ so — $p \geq 3$, $n \in \mathbb{Z}^+$

$U(p) \approx \mathbb{Z}_{p-1}$

$U(2^n) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{n-2}}$ for $n \geq 3$

$U(4) \approx \mathbb{Z}_2$

$U(2) \approx \{0\}$

Example 63 consider $U(45)$

a) Does $U(45)$ have an element of order 4?

b) Does $U(45)$ have an element of order 8?

c) Is $U(45)$ cyclic?

$U(45) = \{1, 2, 4, 7, 8, 11, 13, 14, 16, 17, 19, 22, 23, 26, 28, 29, 31,$

$32, 34, 37, 38, 41, 43, 44\}$

$|U(45)| = 24$

$U(45) \approx U(5) \oplus U(9) \approx \mathbb{Z}_4 \oplus \mathbb{Z}_6$

$U(n_1 \cdot n_2) \approx U(n_1) \oplus U(n_2)$ if $\gcd(n_1, n_2) = 1$ $\qquad U(p) \approx \mathbb{Z}_{p-1}$

$U(3^2) \approx \mathbb{Z}_{3^2 - 3^1} = \mathbb{Z}_6$

a) $(\underline{1}, \underline{0})$ has order 4 since $\text{lcm}(4, 1) = 4$

$|(x, y)| = \text{lcm}(|x|, |y|)$ know $|x|$ divides 4, $|y|$ divides 6

b) $\text{lcm}(a, b)$ is never 8, where $a|4$ and $b|6$

c) $U(45) \approx \mathbb{Z}_4 \oplus \mathbb{Z}_6 \overset{?}{\approx} \mathbb{Z}_{24}$

No, because it is only isomorphic if the gcd is 1, so it is not cyclic

Example 64 Write $U(2079)$ as an external direct product of cyclic groups of minimal order

$U(2079) \approx U(11) \oplus U(3^3) \oplus U(7)$ $\qquad 2079 = 11 \cdot 3^3 \cdot 7$

$\approx \mathbb{Z}_{10} \oplus \mathbb{Z}_{18} \oplus \mathbb{Z}_6$

$\approx \mathbb{Z}_5 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$ $\qquad$ cor 46

Example 65 Is $U(8045)$ cyclic?

$U(8044) \approx U(4) \oplus U(2011)$

$\approx \mathbb{Z}_2 \oplus \mathbb{Z}_{2010}$ $\qquad U(2011) = \mathbb{Z}_{2010}$ cuz prime

$\gcd(2, 2010) \neq 1$ so its not cyclic

Example 66 Find the isomorphism classes:

$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6$ 24 $\quad$ $\mathbb{Z}_{12} \oplus \mathbb{Z}_2$ 24 $\quad$ S_4 24

$\mathbb{Z}_4 \oplus \mathbb{Z}_6$ 24 $\quad$ $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2$ 24

$U(45)$ 24 $\quad$ $A_4 \oplus \mathbb{Z}_3$ 36 $\quad$ $\mathbb{Z}_{24}$ 24

$G = \langle (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8)(9\ 10\ 11) \rangle$ $\quad$ $D_4 \oplus \mathbb{Z}$ 24

$\text{lcm}(8,3) = 24$

① orders $A_4 \oplus \mathbb{Z}_3$ not isom to the others

② Abelian $\quad$ Non Abelian

$U(45) \approx \mathbb{Z}_4 \oplus \mathbb{Z}_6$ $\quad$ $D_4 \oplus \mathbb{Z}_3$

$\approx \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2$ $\quad$ S_4

$\approx \mathbb{Z}_{12} \oplus \mathbb{Z}_2$

$G \approx \mathbb{Z}_{24}$

$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_6$

③ orders of elements or $Z(G)$ centres

$D_4 \oplus \mathbb{Z}_3$ largest order of element is 12

$> \text{lcm}(|R_{90}|, |1|) = \text{lcm}(4, 3) = 12$

In S_4: $\text{lcm}((\_\_\_),(\_\_\_)) = 12$? not possible

Chapter 9: Normal subgroups and factor groups

Consider $K = \{R_0, R_{180}\}$ a subgroup of D_4. There are 4 left cosets since

$|D_4 : K| = \frac{|D_4|}{|K|} = \frac{8}{2} = 4$

They are:

K

$R_{90}K = \{R_{90}, R_{270}\}$

$HK = \{H, V\}$

$DK = \{D, D'\}$

We can define an operation $*$ on those 4 cosets

$$aK * bK = abK$$

eg $R_{90}K * DK = HK$

$$R_{90} \circ D = H$$

$R_{90}K * HK = D'K$

$R_{90} \circ H = D'$ lemma 33

It turns out that using $*$ the cosets form a group!

This happens if the subgroup is a normal subgroup.

Definition A subgroup H of a group G is called a normal subgroup of G if $aH = Ha$ for all $a \in G$. Then we write it as $\trianglelefteq G$

Proposition 49 Suppose H is a subgroup of G. Then H is normal in G iff $xHx^{-1} \subseteq H$

Warning $aH = Ha \ \forall a \in G$ does not mean $ah = ha \ \forall a \in G$

$ah = \{ah \mid h \in H\}$ $h \in G$

$Ha = \{ha \mid h \in H\}$

$$\{ah_1, ah_2, ah_3\} = \{h_1a, ah_2, ah_2\}$$