Chapter 08

Mostafa Touny

November 3, 2023

Contents

Problems

4

Clearly, For arbitrary $a, c \in G$ and $b, d \in H$

$$\begin{aligned} &ac = ca \wedge bd = db \\ \leftrightarrow &(ac, bd) = (ca, db) \\ \leftrightarrow &(a, b)(c, d) = (c, d)(a, b) \end{aligned}$$

I guess the general case is any group-theoretic property on both G and H is also on $G \oplus H$, and vice verca.

5

Assume for the sake of contradiction $Z \oplus G$ is cyclic. Then by definition there is a generator (a, b). Then necessarily $\langle a \rangle = Z$ and $\langle b \rangle = G$ as by definition we have $(a, b)^k = (a^k, b^k)$. Observe $\langle a \rangle$ is of infinite order. Fix $c \in Z$, Then we know $a^k = c$ for some k. Compute $(a, b)^k = (a^k, b^k) = (c, d)$. Let h be the element other than d in G. Now we can't generate (c, h). By *theorem 4.1* (page 76) if $a^i = a^k$ then $i = k$. In other words, k is the only integer that yields $a^k = c$.

6

Clearly $(1, 1) \in Z_8 \oplus Z_2$ is of order 8. We claim no element of $Z_4 \oplus Z_4$ is of order 8, Which suffices to solve the problem.

From *Theorem 4.3* (page 81) we know any element of Z_4 is of order, which divides 4. In other words, For any element a, there is $k \leq 4$ such that $k|a| = 4$. Similarly for another element b we have $k'|b| = 4$.

So for any $(a, b) \in Z_4 \oplus Z_4$, Observe $(a, b)^4 = (a^4, b^4) = (a^{k|a|}, b^{k'|b|}) = ((a^{|a|})^k, (b^{|b|})^{k'}) = (0^k, 0^{k'}) = (0, 0)$. So order of (a, b) is at most 4.

15

Let $\phi : C \to R \oplus R$ where $\phi(a + bi) = (a, b)$.

- Injective. $\phi(a+bi) = \phi(c+di)$ implies $(a, b) = (c, d)$, and in turn $a = c$ and $b = d$.
- Surjective. For any (a, b) we have $\phi(a + bi) = (a, b)$.
- Preserves Operation. $\phi(a + bi)\phi(c + di) = (a, b)(c, d) = (a + c, b + d) = \phi((a + c) + (b + d)i) = \phi((a + bi) + (c + di))$.

17

Since $G \oplus H$ is cyclic, it has a generator (a, b). It follows $\langle a \rangle = G$ and $\langle b \rangle = H$. If that is not the case, Then we can select an element from G or H whereby $(a, b)^k = (a^k, b^k)$ won't cover it, on it corresponding index.

21

Denote the equivalence $\langle (g, h) \rangle = \langle g \rangle \oplus \langle h \rangle$ by (1).

Recall theorem 8.1 (page 158).

By definition we know $(g, h)^k = (g^k, h^k)$ where $g^k \in \langle g \rangle$ and $h^k \in \langle h \rangle$.

The condition is $|g|$ and $|h|$ are coprime. Observe it is equivalent to $lcm(|g|, |h|) = |g||h|$.

(Necessity) We show given (1), The condition holds. Since sets are equal, and cardinality of L.H.S is $|g| \cdot |h|$, Then $|(g, h)| = |g| \cdot |h|$. By *thm 8.1*, The condition is satisfied.

(Sufficent) We show given the condition, (1) holds. By *thm 8.1*, $|(g, h)| = |g| \cdot |h|$. So its cardinality is the same as R.H.S, and it is a subset of it. It follows (1) holds.

23

Any element in $\mathcal{Z}_3$ is of order 3, except the identity 0. Consider an arbitrary non-identity element $(x_1, x_2, \ldots, x_k) \neq e = \underbrace{(0, \ldots, 0)}_{k \text{ times}}$ in $\underbrace{\mathcal{Z}_3 \oplus \cdots \oplus \mathcal{Z}_3}_{k \text{ times}}$. We claim $|(x_1, \ldots, x_k)| = 3$.

Following the fact all non-identity elements are of order 3, and we have some $x_i \neq 0$,

$$
\begin{aligned}
(x_1, x_2, \ldots, x_k)^1 &= (x_1^1, x_2^1, \ldots, x_k^1) \neq e \\
(x_1, x_2, \ldots, x_k)^2 &= (x_1^2, x_2^2, \ldots, x_k^2) \neq e \\
(x_1, x_2, \ldots, x_k)^3 &= (0, 0, \ldots, 0) = e
\end{aligned}
$$

Therefore we have $3^k - 1$ elements of order 3 in $\underbrace{\mathcal{Z}_3 \oplus \cdots \oplus \mathcal{Z}_3}_{k \text{ times}}$.

35

Recall the square root of any complex number z exists. Observe C^* is closed under the square root operation.

Assume for the sake of contradiction, there is an isomorphism $\phi : C^* \to R^* \oplus R^*$. Then by surjectivity there is some complex z where $\phi(z) = (-1, -1)$. It follows

$$\begin{aligned} \phi(\sqrt{z} \cdot \sqrt{z}) &= (-1, -1) \\ \phi(\sqrt{z}) \cdot \phi(\sqrt{z}) &= \\ (\phi(\sqrt{z}))^2 &= \\ (a, b)^2 &= \\ (a^2, b^2) &= \end{aligned}$$

In other words $a^2 = -1$ and $b^2 = -1$, but either of these leads to a contradiction, as no square of a real number is negative.

46

The infinite group is $\mathcal{Z} \oplus D_4 \oplus A_4$. Clearly $\{(e_Z, x, e_{A_4}) \mid x \in D_4\}$ and $\{(e_Z, e_{D_4}, x) \mid x \in A_4\}$ are both subgroups.

48

Claim. It is all permutations on $\mathcal{Z}_2 \oplus \mathcal{Z}_2$ which maps $(0, 0)$ to itself.

Note. Our characterization is consistent with the fact the identity is always mapped to itself, and that isomorphism is a bijection.

Fact. In any group, fixing element a_0, then for any elements $b_0 \neq b_1$, we have $a_0 b_0 \neq a_0 b_1$.

Lemma. For any $(a, b) \in \mathcal{Z}_2 \oplus \mathcal{Z}_2$, $(a, b)^2 = (a^2, b^2) = (0, 0) = e$, As $0^2 = 0$ and $1^2 = 0$.

Lemma. Any two elements of $X = \{(0, 1), (1, 0), (1, 1)\}$ multiplies to the third.

For distinct $a, b, c \in X$, $ab \neq (0, 0)$ since $aa = (0, 0)$. Also $ab \neq a$ since $a(0, 0) = a$. Similarly $ab \neq b$. Therefore the only remaining choice is $ab = c$.

Theorem. Our permutations preserve the operation.

We know for distinct elements $a, b, c \in X$, we have $ab = c$. As ϕ is a permutation on these, We have $X = \{\phi(a), \phi(b), \phi(c)\}$. It follows $\phi(a)\phi(b) = \phi(c)$. That concludes $\phi(c) = \phi(ab) = \phi(a)\phi(b)$.