

Math 113 Homework 3
Solutions

- (1) **More about Direct Products.** Recall from homework # 2 that if G and H are groups, then the direct product $G \times H$ is also a group. The operation on this group was $(g_1, h_1) *_{G \times H} (g_2, h_2) = (g_1 *_G g_2, h_1 *_H h_2)$.

- (a) Show that $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic and that $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic.

In \mathbb{Z}_2 , $a^2 = e$ for all a . So in $\mathbb{Z}_2 \times \mathbb{Z}_2$, also $(a, b)^2 = (a^2, b^2) = (e, e)$. So every element has order two, and none can generate the group of size four.

For $\mathbb{Z}_2 \times \mathbb{Z}_3$, one generator is $([1]_2, [1]_3)$. If we take first six powers, we get in order: $([1]_2, [1]_3)$, $([0]_2, [2]_3)$, $([1]_2, [0]_3)$, $([0]_2, [1]_3)$, $([1]_2, [2]_3)$, and $([0]_2, [0]_3)$. So it gives all elements of the group.

- (b) Show that if A is a subgroup of G and B is a subgroup of H , then $A \times B$ is a subgroup of $G \times H$.

We will show that $A \times B$ meets the criteria of Proposition 2.9, which will show it is a subgroup of $G \times H$. First, since $e_G \in A$ and $e_H \in B$, $e_{G \times H} = (e_G, e_H) \in A \times B$.

Second, if we have $(a_1, b_1), (a_2, b_2) \in A \times B$, then $a_1, a_2 \in A$ and $b_1, b_2 \in B$. So $a_1 a_2 \in A$ and $b_1 b_2 \in B$. Then $(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2) \in A \times B$.

Finally, if $(a, b) \in A \times B$, then $a \in A$ and $b \in B$. So $a^{-1} \in A$ and $b^{-1} \in B$. This gives that $(a, b)^{-1} = (a^{-1}, b^{-1}) \in A \times B$.

So by Proposition 2.9, $A \times B$ is a subgroup of $G \times H$.

- (c) Give an example of groups G and H , and K a subgroup of $G \times H$ so that K is not the direct product of subgroups from each of G and H .

In $\mathbb{Z}_2 \times \mathbb{Z}_2$, one such subgroup is $K = \{([0], [0]), ([1], [1])\}$. If $K = A \times B$, then both A and B would have to be \mathbb{Z}_2 . But $K \neq \mathbb{Z}_2 \times \mathbb{Z}_2$. So K is not the direct product of subgroups.

- (d) If L is a subgroup of $G \times H$, Define $\pi(L)$, the projection of L to G as

$$\pi(L) \equiv \{g \in G : (g, h) \in L \text{ for some } h \in H\}$$

Prove the $\pi(L)$ is a subgroup of G .

We will prove $\pi(L)$ satisfies the criteria of Proposition 2.9. First, since L is a subgroup of $G \times H$, We must have $e_{G \times H} = (e_G, e_H) \in L$. So $e_G \in \pi(L)$.

Next, if $g_1, g_2 \in \pi(L)$, we know for some $h_1, h_2 \in H$, $(g_1, h_1), (g_2, h_2) \in L$. So $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2) \in L$. Which means $g_1 g_2 \in \pi(L)$.

Finally, if $g \in \pi(L)$, then for some $h \in H$, $(g, h) \in L$. Since L is a subgroup, $(g, h)^{-1} = (g^{-1}, h^{-1}) \in L$. So by definition $g^{-1} \in \pi(L)$.

Since all the criteria of Proposition 2.9 are satisfied about $\pi(L)$, it must be a subgroup of G .

(2) Do exercise 3.26 in Judson.

We will prove that any nontrivial subgroup of \mathbb{Z}_p must be all of \mathbb{Z}_p . If H is a nontrivial subgroup of \mathbb{Z}_p , it contains $[k]$ for some k so that $0 < k < p$. Since p is prime, we know that there are s and t so that $sp + kt = 1$. Since H contains $[k]$, it also contains $[2k], [3k], \dots$. So for any n ,

$$[n] = [(sp + kt)n] = [spn] + [ktn] = [0] + [ktn] = [(kn)t] \in G$$

I.e. every element of \mathbb{Z}_p is in G . So $G = \mathbb{Z}_p$.

(3) Prove that if G is an abelian group, $a, b \in G$, and the orders of a and b are coprime, then the order of ab is the order of a times the order of b . Show that this can fail if G is not abelian.

Let n be the order of a , b be the order of m . Then

$$(ab)^{nm} = \overbrace{abab \dots ab}^{nm \text{ times}} = a^{nm} b^{nm} = (a^n)^m (b^m)^n = e^m e^n = e$$

Now we will prove that if $(ab)^k = e$, then n and m must divide k . Since n and m are coprime, this means the least positive such k is nm . If $e = (ab)^k = abab \dots ab = a^k b^k$, then $b^{-k} = a^k$. So then $b^{(-k)n} = (b^{-k})^n = (a^k)^n = (a^n)^k = e^k = e$. By Proposition 3.5, we know m divides $(-k)n$. Since m and n are coprime, this means m divides k . Similarly, $a^{km} = b^{m(-k)} = e^{-k} = e$, so again by Proposition 3.5, n divides $-km$, and by coprimality of n and m , n divides k .

So the least positive k so that $(ab)^k = e$ is nm . I.e. the order of ab is the order of a times the order of b .

To see that abelian is necessary, look at S_3 . In S_3 , $(1\ 2\ 3)$ has order 3 and $(1\ 2)$ has order 2. But $(1\ 2\ 3)(1\ 2) = (2\ 3)$ has order 2, not $2 \cdot 3 = 6$.

(4) If n is a positive odd integer and z is a $(2n)$ -th root of unity, prove that either z or $-z$ is an n th root of unity.

Since n is odd, $(-1)^n = -1$. As z is a $2n$ th root of unity, $(z^n)^2 = z^{2n} = 1$. This tells us $z^n = \pm 1$. If $z^n = 1$, then z is an n th root of unity. If $z^n = -1$, then $(-z)^n = (-1)^n z^n = (-1)(-1) = 1$ and $-z$ is an n th root of unity.

(5) Do exercise 3.44 in Judson.

Either $|z| > 1$ or $0 < |z| < 1$. If $|z| > 1$, then for $i > 1$, $|z^i| > |z| > 1$. If $0 < |z| < 1$, then for $i > 1$, $|z^i| < |z| < 1$. Either way, $|z^i| \neq 1$, so the order of z is not i for any i . So it must be infinite.

(6) let $\omega = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14)$. For which integers i is ω^i a 14-cycle?

If $\gcd(i, 14) = n > 1$, then $(\omega^i)^{14/n} = (\omega^{14})^{i/n} = id^{i/n} = id$. Since $14/n < 14$, ω^i cannot be a 14-cycle.

Now suppose i and 14 are coprime. Fix s and t so that $is + 14t = 1$. So $is \equiv 1 \pmod{14}$. For any j , $(\omega^i)^j(1) = (1 + ij) \pmod{14}$. If $(\omega^i)^{j_1}(1) = (\omega^i)^{j_2}(1)$, then $1 + ij_1 \equiv 1 + ij_2 \pmod{14}$. But then $j_1 \equiv sjj_2 \equiv sj_2 \pmod{14}$. This means that $1 = (\omega^i)^0(1), (\omega^i)^1(1), (\omega^i)^2(1), \dots, (\omega^i)^{13}(1)$ are all distinct. Since also $(\omega^i)^{14} = id$ and ω^i only moves $1, 2, \dots, 14$, it must be that ω^i is a 14-cycle.

(7) Do exercise 4.13 in Judson.

Let ℓ_i be the length of σ_i . Since different σ_i are disjoint, they commute. So

$$\sigma^j = (\sigma_1 \dots \sigma_m)^j = \overbrace{\sigma_1 \dots \sigma_m \sigma_1 \dots \sigma_m \dots \sigma_1 \dots \sigma_m}^{j \text{ times}} = \sigma_1^j \sigma_2^j \dots \sigma_m^j$$

Since the σ_i are disjoint, so are the σ_i^j . So $\sigma^j = id$ if and only if $\sigma_i^j = id$ for each i . And $\sigma_i^j = id$ if and only if ℓ_i divides j . So $\sigma^j = id$ if and only if j is divisible by all the ℓ_i . The least positive such j is the least common multiple of the ℓ_i s by definition. And said j must be the order of σ .

(8) Do exercise 4.30 in Judson

(a) First,

$$\sigma\tau\sigma^{-1}(\sigma(a_j)) = \sigma\tau a_j = \sigma(a_{j+1 \pmod{k}})$$

So $\sigma\tau\sigma^{-1}$ cycles the $\sigma(a_j)$ s.

On the other hand, if $i \neq \sigma(a_j)$, then $\sigma^{-1}(i) \neq a_j$ for any j . So

$$\sigma\tau\sigma^{-1}(i) = \sigma(\tau(\sigma^{-1}(i))) = \sigma\sigma^{-1}(i) = i$$

Thus $\sigma\tau\sigma^{-1}$ is just the cycle $(\sigma(a_1) \sigma(a_1) \dots \sigma(a_k))$.

(b) Suppose $\mu = (b_1 b_2 \dots b_k)$. Fix σ to be any permutation so that $\sigma(a_i) = b_i$ for all i . Then by part (a), $\sigma\tau\sigma^{-1} = (\sigma(a_1) \sigma(a_2) \dots \sigma(a_k)) = (b_1 b_2 \dots b_k) = \mu$ which is what we wanted.