HW 3 Solutions

$\mathbb{Q}$ is a subgroup of $(\mathbb{R},+)$.

Pf We must check that $\mathbb{Q}$ is closed under inverses & closed under ~~multiplication.~~ addition, since $(\mathbb{R},+)$ is an additive group.

If $\frac{a}{b} \in \mathbb{Q}$, then the inverse of $\frac{a}{b}$ in $(\mathbb{R},+)$ is $\frac{-a}{b}$, which is also in $\mathbb{Q}$. (To see this, observe that the identity in $(\mathbb{R},+)$ is 0, and

$\frac{a}{b} + \frac{-a}{b} = 0$.)

If $\frac{a}{b}$ and $\frac{c}{d}$ are in $\mathbb{Q}$, then $\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd}$ is also a rational number.

Since every element of $\mathbb{Q}$ is of the form $\frac{a}{b}$, we have shown that $\mathbb{Q}$ is closed under inverses & multiplication, so $\mathbb{Q} \leq (\mathbb{R},+)$. ☒

HW 3 Solutions M31F11

$H = \{a+bi : a,b \in \mathbb{R},\ a^2+b^2=1\} \leq (\mathbb{C}^\times, \cdot)$

Proof First, we observe that the identity in the group $(\mathbb{C}^\times, \cdot)$ is $(1+0i)$: for any element $(x+iy)$ in $(\mathbb{C}^\times, \cdot)$,

$$(x+iy)(1+0i) = x + 0xi + 1iy + (0i)(iy)$$
$$= x+iy.$$

Now, observe that if $a+bi \in H$, $(a+bi)^{-1} = (a-bi)$. to see this, we compute:

$$(a+bi)(a-bi) = a^2 - abi + abi - (bi)(bi)$$
$$= a^2 - (-b^2) + 0i$$
$$= 1 + 0i.$$

If $a+bi \in H$, then $a-bi \in H$ also: $a, (-b) \in \mathbb{R}$ iff $a,b \in \mathbb{R}$, and $a^2 + (-b)^2 = a^2+b^2$, so if $a+bi \in H$, so is $(a+bi)^{-1} = a-bi$.

Now, we observe that H is closed under multiplication. If $a+bi$, $c+di \in H$, we want to show that $(a+bi)(c+di) \in H$. But

$$(a+bi)(c+di) = ac + adi + cbi + (bi)(di)$$
$$= ac - bd + i(ad+bc)$$

We want to see that if $a^2+b^2=1$, we also have $(bc+ad)^2 + (ac-bd)^2 = 1$.

But $(bc+ad)^2 + (ac-bd)^2 = b^2c^2 + 2abcd + a^2d^2 + a^2c^2$
$-2abcd + b^2d^2$
$= b^2(c^2+d^2) + a^2(c^2+d^2)$
$= b^2 + a^2 = 1.$ (over)

Since H is closed under multiplication & inverses, it's a subgroup of $(\mathbb{C}^\times, \cdot)$. $\boxtimes$

$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ has seven subgroups of order 2.

Proof Observe that $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ has 8 elements. Any element of any group generates a cyclic group. In this case, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ only has elements of order 1 & 2, so any cyclic group generated by a non-identity element will be a subgroup of order 2.

If a subgroup contains more than one non-identity element, it will have size at least 3; this tells us that the cyclic subgroups mentioned above are the only subgroups of order 2.

Explicitly, these subgroups are:

$$\langle(1,0,0)\rangle = \{(1,0,0), (0,0,0)\} = \mathbb{Z}_2 \times 0 \times 0$$

$$\langle(0,1,0)\rangle = \{(0,1,0), (0,0,0)\} = 0 \times \mathbb{Z}_2 \times 0$$

$$\langle(0,0,1)\rangle = \{(0,0,1), (0,0,0)\} = 0 \times 0 \times \mathbb{Z}_2$$

$$\langle(1,0,1)\rangle = \{(1,0,1), (0,0,0)\}$$

$$\langle(1,1,0)\rangle = \{(1,1,0), (0,0,0)\}$$

$$\langle(0,1,1)\rangle = \{(0,1,1), (0,0,0)\}$$

$$\langle(1,1,1)\rangle = \{(1,1,1), (0,0,0)\}$$

HW3 Solutions M31 F11

5.7 If $G = \langle x \rangle$ has order n, then $\langle x^m \rangle = G$ (ie, x^m generates G) iff $(m,n)=1$.

Proof If $(m,n)=1$, then by Theorem 5.5 (iii), $(m,n) = (1,n) = 1$, so x^m & x generate the same cyclic subgroup of G (which is in fact all of G).

Conversely, suppose that x^m generates G. Then Theorem 5.5 (iii) says that $(m,n) = (1,n) = 1$. $\boxtimes$

(5.8) If $G = \langle x \rangle$ has order 144, then $\langle x^{26} \rangle \leq G$ has 72 elements.

Proof We know by Theorem 4.4(iii) that $o(x^{26})$ is $144/(144,26) = 144/2 = 72$. Since $o(g) = |\langle g \rangle|$, this tells us that $|\langle x^{26} \rangle| = 72$. $\boxtimes$

(5.18) a) Show that if $H, K \leq G$ and H, K are proper subgroups, then we cannot have $H \cup K = G$.

Proof We use proof by contradiction.
Suppose $H \cup K = G$; then $H \cup K \leq G$ is a (non-proper) subgroup. Therefore, by Theorem 5.4(ii), we must have either $H \subseteq K$ or $K \subseteq H$. Without loss of generality, suppose $H \subseteq K$. Then $G = H \cup K = K$, which (by hypothesis) is strictly contained (properly contained) in G: Contradiction.
Therefore, $H \cup K \neq G$.

b) V_4 can be written as the union of 3 proper subgroups: $V_4 = \{e, a, b, c\}$ &

$V_4 = \langle a \rangle \cup \langle b \rangle \cup \langle c \rangle = \{e, a\} \cup \{e, b\} \cup \{e, c\}$.

HW 3 Solutions M31 F11

In $(\mathbb{Z}_{24}, \oplus)$, the element 6 generates $\langle 21 \rangle \cap \langle 10 \rangle$.

Proof Since $(21, 24) = 3$ and $(10, 24) = 2$, by Theorem 5.5(iii) we know that $\langle 3 \rangle = \langle 21 \rangle$ & that $\langle 2 \rangle = \langle 10 \rangle$. Since $6 = \mathrm{lcm}(2,3)$, it follows that 6 generates $\langle 2 \rangle \cap \langle 3 \rangle$, by the following problem.

(Alternatively, they could just write down the groups explicitly, observe that the intersection is $\{6, 12, 18, 24 = 0\}$, and reach the conclusion that way.)

HW 3 Solutions M31 F11

In $(\mathbb{Z}_n, \oplus)$, the subgroup $\langle m \rangle \cap \langle k \rangle$ is generated by lcm(m,k).

Proof We know that every subgroup of a cyclic group is cyclic, so $\langle m \rangle \cap \langle k \rangle = \langle l \rangle$ for some $l \in \mathbb{Z}_n$. (Students can either prove or take on faith that the intersection of two subgroups is a subgroup.)

Clearly, $\text{lcm}(m,k) \in \langle l \rangle$ (since lcm(m,k) is in both $\langle m \rangle$ & $\langle k \rangle$); we must show that $\langle \text{lcm}(m,k) \rangle = \langle l \rangle$. Since $\langle \text{lcm}(m,k) \rangle = \{ q \cdot \text{lcm}(m,k) : q \in \mathbb{Z} \}$ by definition, it's clear that every element of $\langle \text{lcm}(m,k) \rangle$ is in both $\langle m \rangle$ and $\langle k \rangle$ (any multiple of a multiple of m is still a multiple of m).

Therefore, $\langle \text{lcm}(m,k) \rangle \subseteq \langle l \rangle = \langle m \rangle \cap \langle k \rangle$. We must show that $\langle l \rangle \subseteq \langle \text{lcm}(m,k) \rangle$.

If $r \in \langle l \rangle = \langle m \rangle \cap \langle k \rangle$, then r must be a multiple of both m & k; hence $r \geq \text{lcm}(m,k)$. To see that $q := \text{lcm}(m,k)$ divides r, and hence $r \in \langle \text{lcm}(m,k) \rangle$, write $r = pq + s$ for $0 \leq s < q$ using the Division Algorithm. Since $k | r$ and $k | q$, by definition, we also have $k | s$. Similarly, we must have $m | s$. But by definition, $q = \text{lcm}(m,k)$ is the smallest positive integer that m & k both divide, so (ctd)

(Generator of $\langle m\rangle \cap \langle k\rangle$)

Terefore, $s=0$, and so $q \mid r$ as claimed. Hence any $r \in \langle \ell\rangle = \langle m\rangle \cap \langle k\rangle$ is in $\langle \mathrm{lcm}(m,k)\rangle$, so

$$\langle \ell\rangle \leq \langle \mathrm{lcm}(m,k)\rangle \quad \text{and} \quad \langle \mathrm{lcm}(m,k)\rangle \leq \langle \ell\rangle.$$

Thus, $\langle \ell\rangle := \langle m\rangle \cap \langle k\rangle = \langle \mathrm{lcm}(m,k)\rangle$ as claimed. $\boxtimes$

HW 3 Solutions M31 F11

(1) a) In $\mathbb{Z}_{18} \times \mathbb{Z}_{18}$, $o((4,9)) = 18$.

Proof In $\mathbb{Z}_{18}$, $o(4) = \frac{18}{(18,4)}$ by Theorem 4.4(iii) (since $4 = 4 \cdot 1 = 1^4$ in multiplicative notation, and $o(1) = 18$). In other words, $o(4) = 18/2 = 9$.

Similarly, $o(9) = 18/(18,9) = 18/9 = 2$ in $\mathbb{Z}_{18}$.

Thus, by Theorem 6.1 (i), $o((4,9)) = \operatorname{lcm}(9,2) = 18$. $\boxtimes$

d) In $\mathbb{Z}_9 \times \mathbb{Z}_{17} \times \mathbb{Z}_{10}$, $o((8,6,4)) =$

Proof Since $(8,9) = 1$, the order of 8 in $\mathbb{Z}_9$ is 9.
Similarly, in $\mathbb{Z}_{17}$, $o(6) = 17$, and in $\mathbb{Z}_{10}$,
$o(4) = 10/(10,4) = 10/2 = 5$.

Thus, in $\mathbb{Z}_9 \times \mathbb{Z}_{17} \times \mathbb{Z}_{10}$, $o((8,6,4)) = \operatorname{lcm}(9,17,5)$
$= 765$.

(Observe that $\mathbb{Z}_9 \times \mathbb{Z}_{17} \times \mathbb{Z}_{10}$ is cyclic, but $\mathbb{Z}_{18} \times \mathbb{Z}_{18}$ is not; however, $(8,6,4)$ is not a generator for $\mathbb{Z}_9 \times \mathbb{Z}_{17} \times \mathbb{Z}_{10}$, because 4 is not a generator for $\mathbb{Z}_{10}$.)

(6.3) The group $\mathbb{Z}\times\mathbb{Z}$ is not cyclic.

Proof Suppose $\mathbb{Z}\times\mathbb{Z}$ were cyclic: $\mathbb{Z}\times\mathbb{Z}=\langle g\rangle$. We can write $g=(g_1,g_2)$, so since $\mathbb{Z}$ is an abelian group, we must have that

$$\mathbb{Z}\times\mathbb{Z}=\{(m,n): m,n\in\mathbb{Z}\}=\{(g_1,g_2)^k: k\in\mathbb{Z}\}$$
$$=\{(kg_1,kg_2): k\in\mathbb{Z}\}.$$

Without loss of generality, suppose $g_1\geq 0$ (if not, then replace g_1 with $-g_1$; this won't change $\langle g\rangle=\langle(g_1,g_2)\rangle$ because an element & its inverse always generate the same cyclic subgroup).

If $g_1=0$, then no pair of the form (m,n) for $m\neq 0$ can be in $\langle g\rangle=\langle(g_1,g_2)\rangle$. In this case, $\langle g\rangle=\langle(g_1,g_2)\rangle$ isn't all of $\mathbb{Z}\times\mathbb{Z}$, So we can assume $g_1>0$. But then, any pair of the form (m,n) with $0<m<g_1$ won't be in $\langle g\rangle$. The only way to avoid the existence of such pairs is to have $g_1=1$.
The same argument applied to g_2 will show that $g_2=1$. In other words, $\langle g\rangle=\langle(1,1)\rangle=\{(k,k): k\in\mathbb{Z}\}$ But then, no pair of the form (m,n) for $m\neq n$ (ctd)

can be in $\langle g \rangle$. Therefore, $\langle g \rangle \neq \mathbb{Z}\times\mathbb{Z}$.

Since no element of $\mathbb{Z}\times\mathbb{Z}$ will generate the whole group, $\mathbb{Z}\times\mathbb{Z}$ must not be cyclic. $\boxtimes$

There are 16 elements of order 15 in $\mathbb{Z}_{30} \times \mathbb{Z}_{20}$, & 2 cyclic subgroups of order 15.

If $o(x) = o(x_1, x_2) = 15$ in $\mathbb{Z}_{30} \times \mathbb{Z}_{20}$, then by Theorem 6.1(i), we know $\operatorname{lcm}(o(x_1), o(x_2)) = 15$.

By Theorems 4.4 & 4.6, the only possible orders of elements of $\mathbb{Z}_{30}$ are the divisors of 30:

Since $o(1) = 30$ and every element in $\mathbb{Z}_{30}$ is a power (multiple) of 1, $o(k) = \frac{30}{(30,k)}$ is a divisor of 30.

As the same is true for $\mathbb{Z}_{20}$, we have the following:

Possible orders of x_1	Possible orders of x_2
1	1
2	2
3	4
5	5
6	10
10	20
15	
30	

We must pick one number from each column so that their lcm is 15. The possibilities are:
$(3,5)$ & $(15,1)$.

There are two elements of order 3 in $\mathbb{Z}_{30}$: 10 & 20.
These are the only elements k with $(k,30) = 10$, so that $o(k) = 30/(k,30) = 30/10 = 3$.

Similarly, if $o(k)=5$ in $\mathbb{Z}_{20}$, we must have that $(20,k)=4$, so that $o(k) = 20/(20,k) = 20/4 = 5$.

The possibilities for this element k are 4, 8, 12, 16.

Therefore, $(10,4)$, $(20,4)$, $(10,8)$, $(20,8)$, $(10,12)$, $(20,12)$, $(10,16)$, $(20,16)$ are 8 elements of order 15.

If $o(k)=15$ in $\mathbb{Z}_{30}$, we must have $(k,30)=2$: these elements are 2, 4, 8, 14, 16, 22, 26, 28. (!!)

Since there is only one element of order 1 in $\mathbb{Z}_{20}$ (the identity), it follows that there are a total of $\boxed{16}$ elements of order 15 in $\mathbb{Z}_{30} \times \mathbb{Z}_{20}$.

Each element of order 15 will generate a cyclic subgroup of order 15 in $\mathbb{Z}_{30} \times \mathbb{Z}_{20}$. The subgroups $\langle(2,0)\rangle$, $\langle(4,0)\rangle$, $\langle(8,0)\rangle$, etc (coming from the elements of (!!)) all generate the same subgroup, because the elements of (!!) all generate the same subgroup of $\mathbb{Z}_{30}$, by Theorem 5.5(iii).

We also observe that $(10,4)$ & $(20,8)$ & $(10,16)$ & $(20,12)$ are all in the same cyclic subgroup (generated by $\langle(10,4)\rangle$, for example). Similarly, $\langle(10,8)\rangle$ contains $(20,16)$, $(10,12)$ & $(20,4)$. But in fact, $\langle(10,8)\rangle = \langle(10,4)\rangle$ because $(10,8) = (10,4)^7 = (70,28) = (10,8)$. (continued)

So, there are two cyclic subgroups of order 15.

Alternatively, you can call on Theorem 5.5 to see that if $\langle x\rangle$ has 15 elements, then x^r generates $\langle x\rangle$ iff $(15, r)=1$. Since there are 8 integers r, less than 15, such that $(15, r)=1$, we know that the 16 elements of order 15 must ~~belong~~ generate ~~to~~ precisely ~~to~~ two cyclic subgroups of order 15. $\boxtimes$

We cannot write D_4 as a direct product of some of its proper subgroups.

<u>Proof</u> The proper, nontrivial subgroups of D_4 are $\langle H \rangle, \langle V \rangle, \langle D \rangle, \langle OD \rangle, \langle 90 \rangle, \langle 180 \rangle, \{0, 180, H, V\}$ & $\{0, 180, D, OD\}$.

The cyclic groups are abelian, and we can check that the other groups are abelian as well, by direct computation (students should do this!). Observe further that the direct product of abelian groups is abelian: If $G_1, \ldots, G_n$ are abelian, then if $(g_1, \ldots, g_n)$ & $(h_1, \ldots, h_n) \in G_1 \times \cdots \times G_n$, we have

$$(g_1, \ldots, g_n)(h_1, \ldots, h_n) = (g_1h_1, \ldots, g_nh_n) = (h_1g_1, \ldots, h_ng_n)$$
$$= (h_1, \ldots, h_n)(g_1, \ldots, g_n).$$

Thus $G_1 \times \cdots \times G_n$ is abelian.

Therefore, since D_4 is not abelian but all its subgroups are abelian, we cannot write D_4 as a direct product of some of its subgroups. ☒