UNIVERSITY OF SOUTH CAROLINA

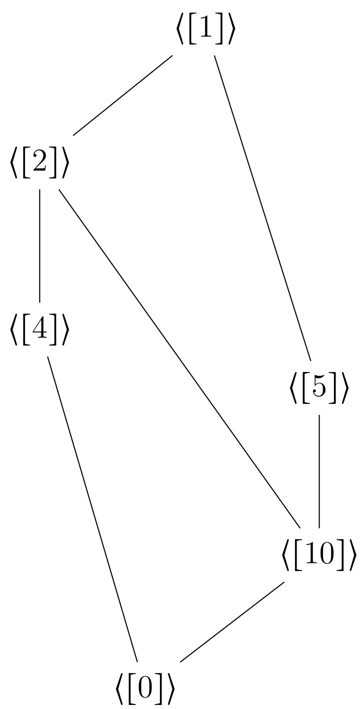
MATH-546 Algebraic Structures I Homework 5

Problems

Problem 1:

Show the subgroup diagram for the group $\mathbb{Z}_{20}$. Specify a generator for each of the subgroups in the diagram and show the inclusions between the subgroups.

Answer 1:



Note: Beware the answers ChatGPT might give you. After figuring out the lattice structure for myself, I asked ChatGPT to generate the LaTeX/TikZ code for it. ChatGPT got the layout correct but put the wrong labels in.

Problem 2:

Find all the possible orders of elements of the group $\mathbb{Z}_{10} \times \mathbb{Z}_8$. For each possible order, show two different examples of elements that have that order, or state that there is only one such element.

Answer 2:

	$[0]_8$	$[1]_8$	$[2]_8$	$[3]_8$	$[4]_8$	$[5]_8$	$[6]_8$	$[7]_8$
$[0]_{10}$	1	8	4	8	2	8	4	8
$[1]_{10}$	10	40	20	40	10	40	20	40
$[2]_{10}$	5	40	20	40	10	40	20	40
$[3]_{10}$	10	40	20	40	10	40	20	40
$[4]_{10}$	5	40	20	40	10	40	20	40
$[5]_{10}$	2	8	4	8	2	8	4	8
$[6]_{10}$	5	40	20	40	10	40	20	40
$[7]_{10}$	10	40	20	40	10	40	20	40
$[8]_{10}$	5	40	20	40	10	40	20	40
$[9]_{10}$	10	40	20	40	10	40	20	40

So there is but 1 element of order 1. 3 of order 2. 4 of order 4. 4 of order 5. 8 of order 8. 12 of order 10. 16 of order 20. 32 of order 40.

Problem 3:

Let

$$H = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} \mid a \equiv b \pmod 5\}.$$

a. Prove that H is a subgroup of $\mathbb{Z} \times \mathbb{Z}$.

b. Prove that H is generated by $(0,5)$ and $(1,1)$.

c. Prove that H is not cyclic.

Answer 3:

Note that b is not constrained.

a. - Associativity: inherited

- Identity: $0 \equiv 0 \pmod 5 \Rightarrow (0,0) \in H$
- Inverses: $a \equiv b \pmod 5$

$$\begin{aligned}
&\Rightarrow \exists n \ni a = 5n + b \\
&\Rightarrow -a = 5(-n) + (-b) \\
&\Rightarrow -a \equiv -b \pmod 5 \\
&\Rightarrow (-a,-b) \in H
\end{aligned}$$

- Closure: Let $(a,b) \in H \wedge (c,d) \in H$ then

$$\begin{aligned}
&\exists j,k \in \mathbb{Z} \ni (a = 5j + b) \wedge (c = 5k + d) \\
&\quad \Rightarrow (a,b) + (c,d) = (5j + b + 5k + d, b + d) \\
&\qquad\qquad\qquad\qquad\;\; = 5(j + l) + (b + d), b + d) \\
&\quad \Rightarrow (a + c) \equiv (b + d) \pmod 5 \\
&\quad \Rightarrow (a + c, b + d) \in H
\end{aligned}$$

Alternatively: If (a,b) and (c,d) are arbitrary elements of H then there are $j,k \in \mathbb{Z}$ such that $a = 5j + b$ and $c = 5k + d$.

$$\begin{aligned}
(a,b) + (c,d)^{-1} &= (a,b) + (-c,-d) \\
&= (5j + b - 5k - d, b - d) \\
&= (5(j - k) + (b - d), (b - d)) \\
\therefore \quad (a,b) + (c,d)^{-1} &\in H
\end{aligned}$$

and H is a subgroup of $\mathbb{Z} \times \mathbb{Z}$.

b. $(a,b) \in H \Rightarrow \exists j \in \mathbb{Z} \ni a = 5j + b \Rightarrow b = a - 5j$ so

$$\begin{aligned}(a,b) &= (a, a-5j)\\ &= (a,a) + (0,5j)\\ &= a(1,1) + j(0,5)\end{aligned}$$

and so every element of H is a linear combination of $(1,1)$ and $(0,5)$.

And, conversely, every linear combination of $(1,1)$ and $(0,5)$ can be reduced to the form $(a, a-5j)$ satisfying the requirements of H.

c. If H is cyclic then $\langle (a,b) \rangle = H$ for some $(a,b) \in H$.

$$\begin{aligned}(1,1) \in H &\Rightarrow \exists j \in \mathbb{Z} \ni j(a,b) = (1,1)\\ &\Rightarrow a = b\\ (0,5) \in H &\Rightarrow \exists k \in \mathbb{Z} \ni k(a,a) = (0,5)\\ &\Rightarrow ka = 0 \wedge ka = 5 \qquad \Rightarrow\Leftarrow\end{aligned}$$

So H cannot be cyclic.

Problem 4:

a. Prove that $G = \mathbb{Z}_4 \times \mathbb{Z}_8$ does not have any elements of order 16.

b. Give two different examples of subgroups of $\mathbb{Z}_4 \times \mathbb{Z}_8$ that have order equal to 16. For each of the two subgroups, list the elements of that subgroup.

Answer 4:

a. Let $([a]_4, [b]_8) \in G$ then $o([a]_4) \mid |\mathbb{Z}_4|$ and $o([b]_8) \mid |\mathbb{Z}_8|$. Therefore $8([a]_4, [b]_8) = ([0]_4, [0]_8)$. And so no element of $\mathbb{Z}_4 \times \mathbb{Z}_8$ has an order greater than 8.

b. Consider $\langle([1]_4, [2]_8)\rangle$ and $\langle([2]_4, [1]_8)\rangle$ and expand.

Theoretical Questions

Problem 5:

For every element $[a]_n \in \mathbb{Z}_n$, prove that

$$o([a]_n) = \frac{n}{\gcd(a,n)}$$

Answer 5:

By definition, $o([a]_n)$ is the smallest positive integer such that $o([a]_n)a$ is a multiple of n. Therefore, using duality of lcm and gcd:

$$\begin{aligned} o([a]_n)a &= \operatorname{lcm}(a,n) \\ &= \frac{an}{\gcd(a,n)} \\ o([a]_n) &= \frac{n}{\gcd(a,n)} \end{aligned}$$

Problem 6:

Let G_1 and G_2 be groups. Prove that $G_1 \times G_2$ is abelian if and only if both G_1 and G_2 are abelian.

Answer 6:

$\Leftarrow$ Let a_1, b_1 be arbitrary elements of G_1 and a_2, b_2 be arbitrary elements of G_2, then

$$\begin{aligned}(a_1, a_2)(b_1, b_2) &= (a_1 b_1, a_2 b_2)\\ &= (b_1 a_1, b_2 a_2)\\ &= (b_1, b_2)(a_1, a_2)\end{aligned}$$

$\Rightarrow$ Let (a_1, a_2) and (b_1, b_2) be arbitrary elements of $G_1 \times G_2$, then

$$\begin{aligned}(a_1 b_1, a_2 b_2) &= (a_1, a_2)(b_1, b_2)\\ &= (b_1, b_2)(a_1, a_2)\\ &= (b_1 a_1, b_2 a_2)\end{aligned}$$

Problem 7:

Let G_1 and G_2 be groups.

a. Prove that if $G_1 \times G_2$ is cyclic, then both G_1 and G_2 are cyclic.

b. Give an example to show that the converse of the statement in part (a) is not true.

Answer 7:

a. Let (g_1, g_2) be a generator of $G_1 \times G_2$ and consider $a_1 \in G_1$ an arbitraty element of G_1. Then $(a_1, e_2) \in G_1 \times G_2$ implies that $(a_1, e_2) = (g_1, g_2)^n = (g_1^n, g_2^n)$ and therefore $a_1 = g_1^n$ for some integer n. Since a_1 is arbitrary, $\langle g_1 \rangle = G_1$ and g_1 is a generator of G_1.

   We can use the same argument for g_2 and G_2.

b. $\mathbb{Z}_4 \times \mathbb{Z}_8$ from problem 4: both $\mathbb{Z}_4$ and $\mathbb{Z}_8$ are individually cyclic but the direct product has order 32 but can't be cyclic since no element has an order greater than 8.