Solution for Homework 6

Xiangcan Li

March 10, 2021

Exercise 3.1.4 Prove that a nonempty set G with an associative operation $*$ is a group if and only if the equations $g * x = h$ and $x * g = h$ have solutions in G for all $g, h \in G$.

- $\Longrightarrow$: If G is a group, then for all $g, h \in G$ there exists $g^{-1} * h, h * g^{-1} \in G$ such that

  $$g * x = g * (g^{-1} * h) = (g * g^{-1}) * h = e * h = h \text{ and } y * g = (h * g^{-1}) * g = h * (g^{-1} * g) = h * e = h.$$

- $\Longleftarrow$: First we prove if $e * g = g$ for some g, then $e * h = h$ for all $h \in G$. Note that such e exists since for any $g \in G$, there exists $x, e \in G$ such that $g * x = g$ and $e * g = g$.

  For $g, h \in G$, there exists $x, y \in G$ such that $g * x = g$ and $y * g = g$.

  Hence, we have

  $$\begin{aligned} e * g = g &\implies (e * g) * x = g * x \\ &\implies e * (g * x) = g * x && \text{by associativity} \\ &\implies e * h = h. \end{aligned}$$

  We conclude there exists an element $e \in G$ so that $e * g = g$ for all $g \in G$.

  Then for any $g \in G$, since $e \in G$, there exists an element $x \in G$ so that $x * g = e$. Let $x = g^{-1}$. Hence, for all $g \in G$, there exists an element $g^{-1} \in G$ so that $g^{-1} * g = e$.

  By **Exercise 3.1.3**, G is a group.

We conclude G is a group if and only if $*$ is an associative operation such that for all $g, h \in G$ there exist $x, y \in G$ such that $g * x = h$ and $y * g = h$.

Exercise 3.2.1 Suppose $n \geq 2$ is an integer and $d, d' > 0$ are two divisors of n. Prove that $\langle [d] \rangle < \langle [d'] \rangle$ if and only if $d' \mid d$.

- $\Longrightarrow$: Since $\langle [d] \rangle < \langle [d'] \rangle$, $\langle [d] \rangle \subset \langle [d'] \rangle$. By **Proposition 3.2.3**, $\langle [d] \rangle = \{[d]^n \mid n \in \mathbb{Z}\}$. Hence, $[d] \in \langle [d] \rangle$. We have $\langle [d'] \rangle = \{[d']^a \mid a \in \mathbb{Z}\} = \{[ad'] \mid a \in \mathbb{Z}\}$. Then $[d] \in \{[ad'] \mid a \in \mathbb{Z}\}$. Hence, $[d] = [kd']$ for some $k \in \mathbb{Z}$. We have $d + np = ad' + nq$ for some $p, q \in \mathbb{Z}$. Then $ad' - d = n(p - q)$. Note that $p - q \in \mathbb{Z}$, then $n \mid ad' - d$.

  Since d' are two divisors of n, we have $d' \mid n$. Therefore, $d' \mid ad' - d$, which indicates $ad' - d = td'$ for some $t \in \mathbb{Z}$. Then $d = (a - t)d'$. Since $a - t \in \mathbb{Z}$, $d' \mid d$.

- $\Longleftarrow$: From **Theorem 3.2.10**, we know that $\langle [d] \rangle$ and $\langle [d'] \rangle$ are subgroups. Hence, both $\langle [d] \rangle$ and $\langle [d'] \rangle$ are groups. Need $\langle [d] \rangle \subset \langle [d'] \rangle$.

  Since $d' \mid d$, $d = td'$ for some $t \in \mathbb{Z}$. By **Proposition 3.2.3**, $\langle [d] \rangle = \{[nd] \mid n \in \mathbb{Z}\} = \{ntd' \mid nt \in \mathbb{Z}\}$. Also, $\langle [d'] \rangle = \{[d']^a \mid a \in \mathbb{Z}\} = \{[ad'] \mid a \in \mathbb{Z}\}$. Hence, for any $s \in \langle [d] \rangle$, we have $s \in \langle [d'] \rangle$, which implies $\langle [d] \rangle \subset \langle [d'] \rangle$.

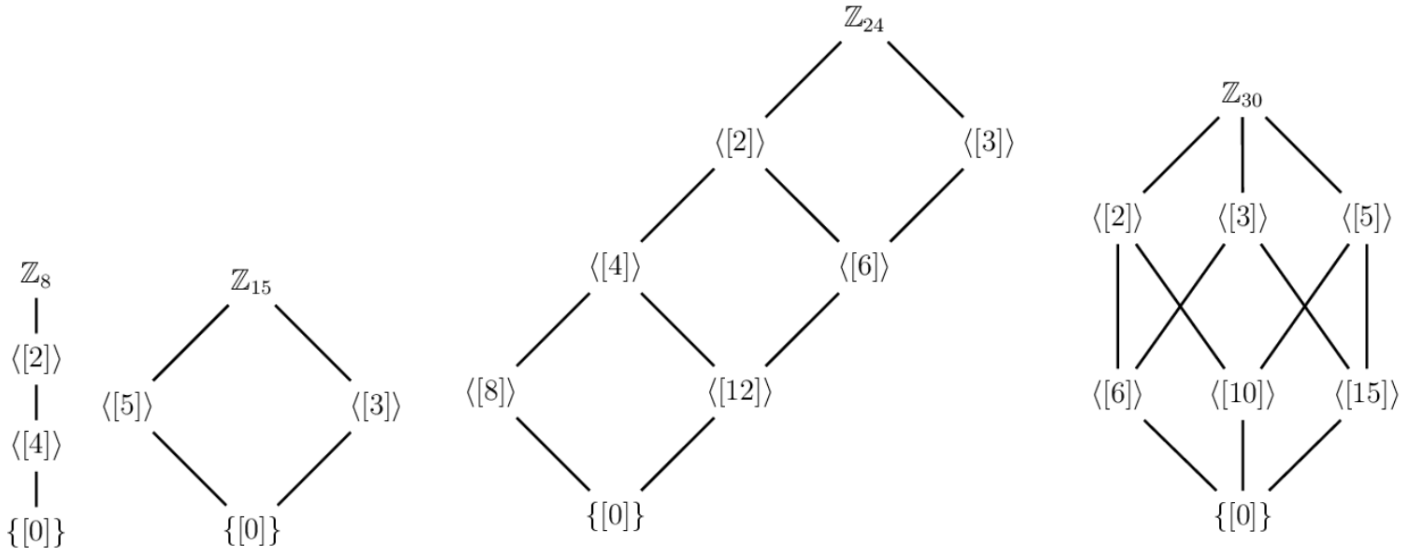
Exercise 3.2.2 Prove that the number of elements of order n in $\mathbb{Z}_n$ is exactly $\phi(n)$, the Euler phi function of n.

We first need to prove that $\gcd(a,n)=1$ if and only if $|[a]|=n$. By **Proposition 3.2.6**, since $|[a]|=n\leq\infty$, there exists a an integer $m\neq 0$ so that $[a]^m=[ma]=[0]$, the identity in $\mathbb{Z}_n$. Note that m is the smallest positive number so that $[ma]=[0]$. Hence, $m=n$. Then we have $[na]=[0]$.

- $\Longrightarrow$: Since $\gcd(a,n)=1$, $pa+qn=1$ for some $p,q\in\mathbb{Z}$. Let $0<b<n$, then $b=pab+bnq$. Since $n\nmid b$, $n\nmid pab+bnq$. Then either $n\nmid pab$ or $n\nmid bnq$. Since $bnq=(bq)n$, where $bq\in\mathbb{Z}$, $n\nmid pab$. Hence, $n\nmid pb$ for all $0<b<n$. Since $n\mid nk$, n is the smallest positive number such that $[na]=[0]$. Hence, $|[a]|=n$.
- $\Longleftarrow$: Suppose $\gcd(a,n)=t>1$, then $t\mid a$ and $t\mid n$. We also have $n/t\in\mathbb{Z}$ and $n>n/t$. Since $s=a/t\in\mathbb{Z}$, $n\mid na/t$, i.e., $n\mid(n/t)a$. Then $[(n/t)a]=[0]$. Since $n/t<n$, $|[k]|\neq n$. Hence, if $|[k]|=n$,$\gcd(a,n)=1$.

We conclude $\gcd(a,n)=1$ if and only if $|[a]|=n$. Then all elements of order n form $\mathbb{Z}_n^\times$. Then the number of elements of order n in $\mathbb{Z}_n$ is exactly $|\mathbb{Z}_n^\times|$, which is equal to $\phi(n)$.

Exercise 3.2.3 Draw the subgroup lattice for the groups $\mathbb{Z}_8$, $\mathbb{Z}_{15}$, $\mathbb{Z}_{24}$, and $\mathbb{Z}_{30}$.



Exercise 3.2.4 Draw the subgroup lattice for S_3 (a group with respect to composition $\circ$). You will need to find all the subgroups $H<S_3$ by hand (because we don't yet have any theorems that tell us what the subgroups of S_3 are).

By the definition of S_3, we have $S_3=\{(1)(2)(3),(1\ 2),(1\ 3),(2\ 3),(1\ 2\ 3),(1\ 3\ 2)\}$. We first find all cyclic subgroups of S_3 by hands.

- $\langle(1)(2)(3)\rangle=\{(1)(2)(3)\}$
- $\langle(1\ 2)\rangle=\{(1\ 2),(1)(2)(3)\}$
- $\langle(1\ 3)\rangle=\{(1\ 3),(1)(2)(3)\}$
- $\langle(2\ 3)\rangle=\{(2\ 3),(1)(2)(3)\}$
- $\langle(1\ 2\ 3)\rangle=\{(1\ 2\ 3),(1\ 3\ 2),(1)(2)(3)\}$
- $\langle(1\ 3\ 2)\rangle=\{(1\ 3\ 2),(1\ 2\ 3),(1)(2)(3)\}$

Since $\langle(1\ 3\ 2)\rangle=\langle(1\ 2\ 3)\rangle$, the cyclic subgroups are

- $\{(1)(2)(3)\}$
- $\{(1\ 2),(1)(2)(3)\}$
- $\{(1\ 3),(1)(2)(3)\}$

- $\{(2\ 3), (1)(2)(3)\}$
- $\{(1\ 2\ 3), (1\ 3\ 2), (1)(2)(3)\}$

By Lagrange's Theorem, since S_3 is a finite group, the order of any subgroup H divides the order of S_3.

Note that $|S_3|= 6$. Then $|H|= 1, 2, 3$ or 6. Note that when $|H|= 1$, the only element in H is the identity. Hence, $H = \{(1)(2)(3)\}$. Also, when $|H|= 6$, clearly, $H = S_3$.

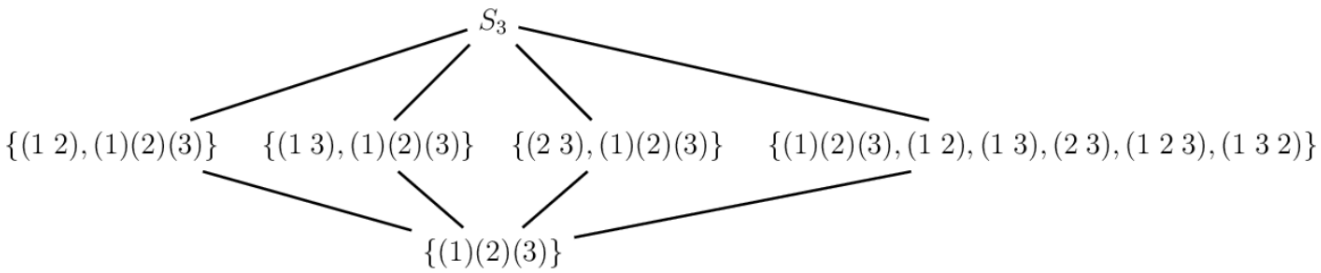
Then there are only two cases to consider: $|H|= 2$ or 3.

Since 2 and 3 are both prime integers, by **Corollary 3.5.8**, H is cyclic. Then cyclic subgroups found above with order 2 and 3 are what we want.

Hence, all the subgroups of S_3 are

- $\{(1)(2)(3)\}$
- $\{(1\ 2), (1)(2)(3)\}$
- $\{(1\ 3), (1)(2)(3)\}$
- $\{(2\ 3), (1)(2)(3)\}$
- $\{(1\ 2\ 3), (1\ 3\ 2), (1)(2)(3)\}$
- $\{(1)(2)(3), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$

The subgroup lattice is



Exercise 3.2.5 Prove that if G and H are groups and $K < G, J < H$ are subgroups, then $K \times J \subset G \times H$ is a subgroup. Construct an example of a subgroup of $\mathbb{Z}_2 \times \mathbb{Z}_2$ which is **not** of the form $K \times J$ for some $K < \mathbb{Z}_2$ and $J < \mathbb{Z}_2$.

Let m, n and p, q be arbitrary elements in K and J, respectively. Then (m, p) and (n, q) are arbitrary elements in $K \times J$.

We have $(m, p)(n, q) = (mn, pq)$. Since K, J are subgroups, $m, n \in K$ and $p, q \in J$, $mn \in K$ and $pq \in J$. Hence, $(mn, pq) \in K \times J$.

Since K, J are subgroups, $m \in K$ and $p \in J$, there exists some $m^{-1} \in K$ and $p^{-1} \in J$ such that $mm^{-1} = m^{-1}m = e_1$ and $pp^{-1} = p^{-1}p = e_2$, where e_1 and e_2 are identities in K and J, respectively.

Then $(m^{-1}, p^{-1}) \in K \times J$ and we have

$$(m^{-1}, p^{-1})(m, p) = (m^{-1}m, p^{-1}p) = (e_1, e_2)$$
$$(m, p)(m^{-1}, p^{-1}) = (mm^{-1}, pp^{-1}) = (e_1, e_2)$$

Hence, there exists an inverse $(m^{-1}, p^{-1}) \in K \times J$ such that $(m^{-1}, p^{-1})(m, p) = (m, p)(m^{-1}, p^{-1}) = (e_1, e_2)$.

Since (m, n) and (p, q) are arbitrary, for all $(g_1, g_2), (h_1, h_2) \in K \times J$, $(g_1, g_2)(h_1, h_2) \in K \times J$ and for all $(g_1, g_2) \in K \times J$, $(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1}) \in K \times J$.

We conclude $K \times J$ is a subgroup.

$\{([0], [0]), ([1], [1])\}$ is a subgroup of $\mathbb{Z}_2 \times \mathbb{Z}_2$ and is not of the form $K \times J$ for some $K < \mathbb{Z}_2$ and $J < \mathbb{Z}_2$.

Note that $\mathbb{Z}_2 = \{[0], [1]\}$ and $\{[0]\}, \{[0], [1]\}$ is a subgroup of $\mathbb{Z}_2$.

Then the following sets is of the form $K \times J$:

$$\{[0],[1]\} \times \{[0],[1]\} = \{([0],[0]),([0],[1]),([1],[0]),([1],[1])\}$$
$$\{[0],[1]\} \times \{[0]\} = \{([0],[0]),([1],[0])\}$$
$$\{[0]\} \times \{[0],[1]\} = \{([0],[0]),([0],[1])\}$$
$$\{[0]\} \times \{[0]\} = \{([0],[0])\}$$

Hence, $\{([0],[0]),([1],[1])\}$ is not of the form $K \times J$.
Let $S = \{([0],[0]),([1],[1])\} \subset \mathbb{Z}_2$.
We have

$$([0],[0]) + ([0],[0]) = ([0],[0]) \in S$$
$$([0],[0]) + ([1],[1]) = ([1],[1]) \in S$$
$$([1],[1]) + ([0],[0]) = ([1],[1]) \in S$$
$$([1],[1]) + ([1],[1]) = ([0],[0]) \in S$$

Then for any $g, h \in S$, $gh \in S$.
We also have

$$([0],[0]) + ([0],[0]) = ([0],[0]) \in S$$
$$([1],[1]) + ([1],[1]) = ([0],[0]) \in S$$

Then for any $g \in S$, $g^{-1} \in S$.
Hence, S is a subgroup of $\mathbb{Z}_2 \times \mathbb{Z}_2$.
We conclude $\{([0],[0]),([1],[1])\}$ is a subgroup of $\mathbb{Z}_2 \times \mathbb{Z}_2$ and is not of the form $K \times J$ for some $K < \mathbb{Z}_2$ and $J < \mathbb{Z}_2$.