A report on some exercises from Chapter 1

Groups and their representations

MATEFY Adam (Student ID: 062201898)

January 30, 2023

Since generally a map in a group is not commutative, I will denote multiplying an equation by an element c from the right by $/\cdot c$ and from the left by $/c\cdot$.

Exercise 1.1.3.

Let G be a group.

1. In this part we want to show that the identity element of a group is unique. To do this, let us assume that the group has two identities $e_1, e_2 \in G$, $e_1 \neq e_2$. From the property of the identity element, and the inverse, for a random element $a \in G$

$$\begin{aligned} e_1 &= aa^{-1} \\ e_2 &= aa^{-1} \end{aligned}$$

   from which $e_1 = e_2$, which is in contradiction with the initial assumption ($e_1 \neq e_2$), so there is only one identity element.

2. In this part, first we want to show that the inverse of the identity element is itself. By the definition of the inverse, an element multiplied by its inverse is the identity element

$$ee^{-1} = e$$

   by the definition of the identity element,

$$e^{-1} = e$$

   which means that the inverse of the identity is itself.

   Next, we want to show that $a = (a^{-1})^{-1}$ for $\forall a \in G$. From the definition of inverse

$$\begin{aligned} aa^{-1} &= e = a^{-1} \cdot (a^{-1})^{-1} \\ aa^{-1} &= (a^{-1})^{-1} \cdot a^{-1} \qquad / \cdot a \\ aa^{-1}a &= (a^{-1})^{-1} \cdot a^{-1}a \\ a &= (a^{-1})^{-1} \end{aligned}$$

so we indeed get back the initial element if we take its inverse two times (for any element of the group).

Then, we want to prove that $(ab)^{-1} = b^{-1}a^{-1}$. Using the definition of inverse again, and that the map is associative

$$\begin{aligned} (ab)^{-1} &= b^{-1}a^{-1} \qquad /ab\cdot \\ (ab)(ab)^{-1} &= ab \cdot b^{-1}a^{-1} \\ e &= aa^{-1} \\ e &= e. \end{aligned}$$

Since we got an identity by applying operations that do not change the solution of the equation, we have proven that $(ab)^{-1} = b^{-1}a^{-1}$.

Finally, we want to prove that the inverse of any element of the group is unique. To do this, let us assume that $a \in G$ has two inverse $(a^{-1})_1$ and $(a^{-1})_2$.

$$\begin{aligned} a(a^{-1})_1 &= e = a(a^{-1})_2 \qquad /(a^{-1})_1\cdot \\ (a^{-1})_1 a(a^{-1})_1 &= (a^{-1})_1 a(a^{-1})_2 \\ (a^{-1})_1 &= (a^{-1})_2 \end{aligned}$$

so the two inverse are the same, so the inverse is uniqe.

3. In this part we want to prove that if $ab = ac$ or $ba = ca$, then $b = c$. If $ab = ac$, using the inverse and associativity

$$\begin{aligned} ab &= ac \\ a^{-1}ab &= a^{-1}ac \\ b &= c. \end{aligned}$$

Similarly, if $ba = ca$, then

$$\begin{aligned} ba &= ca \\ baa^{-1} &= caa^{-1} \\ b &= c. \end{aligned}$$

Thus, if $ab = ac$ or $ba = ca$, then $b = c$.

Exercise 1.2.2.

In this exercise we want to prove that $\sim$ is an equivalence relation.
Let G be a group and $a, b \in G$. The $\sim$ is an equivalence relation if it satisfies the following three properties

1. $a \sim a$,
2. if $a \sim b$, then $b \sim a$,
3. if $a \sim b$ and $b \sim c$, then $a \sim c$.

Now let us prove that all three of these are satisfied. From the definition, $a \sim b$ if $\exists c \in G$ so that $a = cbc^{-1}$. Using this,

1. For $c = e$, $a = eae^{-1}$, thus $a \sim a$.
2. If $a \sim b$, then (using that c^{-1} is also an element of G)

$$\begin{aligned} a &= cbc^{-1} && / \cdot c \\ ac &= cb && / c^{-1} \cdot \\ c^{-1}ac &= b \\ (c^{-1})a(c^{-1})^{-1} &= b \end{aligned}$$

   thus $b \sim a$.

3. Let $a, b, c, d_1, d_2 \in G$, $a = d_1 b d_1^{-1}$, and $b = d_2 c d_2^{-1}$. From this one has

$$\begin{aligned} a &= d_1 b d_1^{-1} = d_1(d_2 c d_2^{-1})d_1^{-1} \\ a &= (d_1 d_2)c(d_2^{-1} d_1^{-1}) \\ a &= (d_1 d_2)c(d_2 d_1)^{-1}. \end{aligned}$$

   If $d_1, d_2 \in G$, then $d_1 d_2 \in G$, thus $a \sim c$.

Since all three conditions are satisfied, $\sim$ is an equivalence relation.

Exercise 1.2.10.

1. In this part we want to show that G_0 is a normal subgroup if and only if for any $a \in G$ we have ${}_{G_0}[a] = [a]_{G_0}$. To prove this we need to show that ${}_{G_0}[a] = [a]_{G_0}$ if G_0 is a normal subgroup, and G_0 is a normal subgroup if ${}_{G_0}[a] = [a]_{G_0}$.

   If G_0 is a normal subgroup, then $\forall a \in G$, $aG_0a^{-1} = G_0$, so

$$\begin{aligned} aG_0a^{-1} &= G_0 && / \cdot a \\ aG_0 &= G_0 a \\ {}_{G_0}[a] &= [a]_{G_0}, \end{aligned}$$

   so ${}_{G_0}[a] = [a]_{G_0}$ if G_0 is a normal subgroup.

   If G_0 is a subgroup and for any $a \in G$ we have ${}_{G_0}[a] = [a]_{G_0}$, then

$$\begin{aligned} {}_{G_0}[a] &= [a]_{G_0} \\ aG_0 &= G_0 a && / \cdot a^{-1} \\ aG_0a^{-1} &= G_0 \end{aligned}$$

   for any $a \in G$, which means that G_0 is a normal subgroups if ${}_{G_0}[a] = [a]_{G_0}$.

   These mean that G_0 is a normal subgroup if and only if for any $a \in G$ we have ${}_{G_0}[a] = [a]_{G_0}$.

2. In this part, we first want to show that $[a]_{G_0}[b]_{G_0} := [ab]_{G_0}$ defines a product on the equivalence classes. For this, we have to show if this product is meaningful, that is, if $[a]_{G_0} = [a']_{G_0}$ and $[b]_{G_0} = [b']_{G_0}$ (for $a, a', b, b' \in G$), then $[ab]_{G_0} = [a'b']_{G_0}$, in other words, if the newly defined map ($[a]_{G_0}[b]_{G_0} := [ab]_{G_0}$) is independent of the element we choose from the equivalence class. Otherwise the product of two equivalence classes could be more than one equivalence class (depending on which element we choose from the equivalence class), which is not something we want. To prove this, first recall that $[a]_{G_0} = [a']_{G_0} \iff G_0 a = G_0 a'$ and $[b]_{G_0} = [b']_{G_0} \iff G_0 b = G_0 b'$. From these

$$[ab]_{G_0} = G_0(ab) = (G_0 a)b = (G_0 a')b$$

using the results of the previous section

$$(G_0 a')b = (a'G_0)b = a'(G_0 b) = a'(G_0 b') = (a'G_0)b' = (G_0 a')b' = G_0(a'b') = [a'b']_{G_0}$$

thus it is true that $[ab]_{G_0} = [a'b']_{G_0}$ if $[a]_{G_0} = [a']_{G_0}$ and $[b]_{G_0} = [b']_{G_0}$, so the product we defined is meaningful.

Next, we want to show that this operation defines a group. Fistly, let us check if the operation is stable on this group. Since (by definition) if $a, b \in G$, then $ab \in G$, and since every element of G is in an equivalence class, $[ab]_{G_0}$ also exists, thus the operation defined for the quotient group is stable.

Next, let's check if this map has the three basic properties from Definition 1.1.1.

i) Associativity:

$$([a]_{G_0}[b]_{G_0})[c]_{G_0} = [ab]_{G_0}[c]_{G_0} = [(ab)c]_{G_0}$$
$$[a]_{G_0}([b]_{G_0}[c]_{G_0}) = [a]_{G_0}[bc]_{G_0} = [a(bc)]_{G_0}$$

which are equal because of associativity of the map of G

ii) Existence of an identity element. This identity element is indeed $G_0 = G_0 e = [e]_{G_0}$, since

$$[e]_{G_0}[a]_{G_0} = [ea]_{G_0} = [a]_{G_0}.$$

iii) Existence of an inverse. If the inverse is defined as $[a]_{G_0}^{-1} := [a^{-1}]_{G_0}$, then

$$[a]_{G_0}[a^{-1}]_{G_0} = [aa^{-1}]_{G_0} = [e]_{G_0}$$

so it is indeed the inverse.

Since every condition is satisfied, the quotient group is indeed a group.

Finally, we want to show that if G is finite and if G_0 is a normal subgroup of G, then $|G/G_0| = \frac{|G|}{|G_0|}$.

Let G be a finite group with $|G| = N$ and G_0 its subgroup with $|G_0| = n$. By definition, two elements (a and b) of G are right conjugated ($b \sim^r a$) if $\exists c \in G_0$ so that $b = ca$.

Let the elements of the subset be $G_0 = \{g_1 = e, g_2, g_3, ..., g_n\}$. Based on the definition of right conjugation, the equivalence class containing a can be given as $[a]_{G_0} = \{ag_1 = a, ag_2, ag_3, ..., ag_n\}$. Since a set cannot contain duplicates, and a group is stable to its map (i.e. $\forall ag_i \in G$), every equivalence class has exactly n elements. Since every element is contained by exactly 1 equivalence class (Definition 1.2.3.), the number of equivalence classes is given by N/n. Since the elements of the factor group are the equivalence classes, the number of elements of the factor group is

$$|G/G_0| = \text{number of equivalence classes} = \frac{N}{n} = \frac{|G|}{|G_0|}$$

which is what we wanted to prove.

Exercise 1.2.12.

In this exercise we want to prove that the center $Z(G)$ of a group G is an Abelian and normal subgroup of G.

First let us check if $Z(G)$ is a group. To do this, we have to check if the inverse of any element of $Z(G)$ is also included in $Z(G)$, i.e. if $a \in Z \Rightarrow a^{-1} \in Z$. For this let's check if a^{-1} commutes with $\forall b \in G$

$$\begin{aligned} a^{-1}b &= ba^{-1} && / \cdot a \\ a^{-1}ba &= b \\ a^{-1}ab &= b \\ b &= b \end{aligned}$$

so the inverse of any element of $Z(G)$ is included in $Z(G)$.
It also has to be checked if the map of G is stable on Z. Let $a, b \in Z$, for $\forall c \in G$ one has

$$(ab)c = a(bc) = a(cb) = (ac)b = (ca)b = c(ab)$$

so the map of G is indeed stable on Z.
From these, we can see that $Z(G)$ is indeed a group.

Finally, we have to check if Z is Abelian and a normal subgroup of G. Since any element of Z commutes with any element of G and $Z \subset G$, the elements of Z commute with each other, thus Z is Abelian. This property also implies that for any $a \in Z$ and $c \in G$,

$$cac^{-1} = acc^{-1} = a \Rightarrow cZc^{-1} = Z$$

so Z is normal.

Therefore, the center $Z(G)$ of a group G is an Abelian and normal subgroup of G.

Exercise 1.2.15.

1. In this part we want to prove that if G and G' are two groups and $\phi : G \to G'$ is a homomorphism, then the identity element of G is mapped to the identity of G' and that $\phi(a^{-1}) = \phi(a)^{-1}$.

From the definition of homomorphism, for $\forall a \in G$

$$\begin{aligned} \phi(ae_G) &= \phi(a)\phi(e_G) \\ \phi(a) &= \phi(a)\phi(e_G). \end{aligned}$$

Since $\phi(a) \in G'$, $\phi(e_G)$ must be $e_{G'}$. Using this

$$\begin{aligned} e_{G'} &= \phi(e_G) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1}) \\ e_{G'} &= \phi(a)\phi(a^{-1}) \end{aligned}$$

where $\phi(a^{-1})$ must be the inverse of $\phi(a)$ to satisfy the equation for $\forall a \in G$. Thus, $\phi(e_G) = e_{G'}$ and $\phi(a^{-1}) = \phi(a)^{-1}$.

2. In this part we want to prove that the kernel of ϕ defined as $\ker(\phi) := \{a \in G | \phi(a) = e_{G'}\}$ is a normal subgroup of G.

   Let $a, b \in \ker(\phi)$, meaning $\phi(a) = \phi(b) = e_{G'}$. Using the property of homomorphism

$$\begin{aligned} \phi(ab) &= \phi(a)\phi(b) = e_{G'}e_{G'} = e_{G'} && \rightarrow ab \in \ker(\phi) \\ e_{G'} &= \phi(e_G) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1}) = \phi(a^{-1}) && \rightarrow a^{-1} \in \ker(\phi) \end{aligned}$$

   since this means $\ker(\phi)$ is stable to the map of G and includes the inverse of all of its elements, $\ker(\phi)$ is a subgroup.

   For any $a \in \ker(\phi)$ and $c \in G$,

$$\phi(cac^{-1}) = \phi(ca)\phi(c^{-1}) = \phi(c)\phi(a)\phi(c^{-1}) = \phi(c)\phi(c^{-1}) = \phi(c)[\phi(c)]^{-1} = e_{G'}$$

   since this means that cac^{-1} is also an element of $\ker(\phi)$, $\ker(\phi)$ is normal.

   From these, we can conclude that $\ker(\phi)$ is a normal subgroup of G.

3. In this part we want to prove that the quotient group $G/\ker(\phi)$ is isomorphic to $\phi(G)$ through the isomorphism $\widetilde{\phi}$ defined as $\widetilde{\phi}([a]_{\ker(\phi)}) := \phi(a)$ for any $a \in G$.

   Firstly, let us check that $\widetilde{\phi}$ is indeed a map, i.e. if an equivalence class is mapped to the same element regardless of which element we choose within the equivalence class. Otherwise, an equivalence class would be mapped to more than one element, which would mean that $\widetilde{\phi}$ is not a map. If a_1 and a_2 are in the same equivalence class, then theres exists $b \in \ker(\phi)$ such that $a_2 = ba_1$. From this

$$\phi(a_2) = \phi(ba_1) = \phi(b)\phi(a_1) = e_{G'}\phi(a_1) = \phi(a_1)$$

   so every equivalence class is mapped to only one element, thus $\widetilde{\phi}$ is indeed a map.

   Next, let us check if $\widetilde{\phi}$ is a homomorphism

$$\begin{aligned} \widetilde{\phi}([a]_{\ker(\phi)}[b]_{\ker(\phi)}) &= \widetilde{\phi}([ab]_{\ker(\phi)}) = \phi(ab) \\ \widetilde{\phi}([a]_{\ker(\phi)})\widetilde{\phi}([b]_{\ker(\phi)}) &= \phi(a)\phi(b) = \phi(ab) \end{aligned}$$

since ϕ is a homomorphism. This means that $\widetilde{\phi}$ is indeed a homomorphism (it indeed preserves the structure of a group).

Finally, we will prove that $\widetilde{\phi}$ is an isomorphism, that is, a bijective homomorphism.

First we will prove that it is injective, using proof by contradiction. Let us assume that $\exists a, b \in G$ such that $\phi(a) = \phi(b)$, but a is not in the same equivalence class as b (in other words, that two different equivalence classes are mapped to the same element $\iff$ $\widetilde{\phi}$ is not injective). This means that if $b = ca$ for some $c \in G$, then $c \notin \ker(\phi)$. But then we have

$$\phi(b) = \phi(ca) = \phi(c)\phi(a) = \phi(c)\phi(b)$$

from which $\phi(c) = e_{G'} \Rightarrow c \in \ker(\phi)$, but this is a contradiction, so $\widetilde{\phi}$ is injective.

Next, we proove that $\widetilde{\phi}$ is surjective. Since $\widetilde{\phi}$ maps to $\phi(G)$, and any element of an equivalence class is mapped to the same element, when the equivalence class itself is mapped to that particular element, the image did not become smaller (basically we replaced every element that was mapped to the same element with one element), so $\widetilde{\phi}$ is surjective.

Since $\widetilde{\phi}$ is both injective and surjective, it is bijective. Therefore, $G/\ker(\phi)$ is isomorphic to $\phi(G)$ through the isomorphism $\widetilde{\phi}$.

4. In this part we want to prove that if G_0 is a subgroup of G, then $\phi(G_0)$ is a subgroup of G'.

   If $a, a^{-1}, b \in G_0$, then $ab \in G_0$, so

   $$\phi(ab) = \phi(a)\phi(b) \Rightarrow \text{the product of two elements of } \phi(G_0) \text{ is in } \phi(G_0) \Rightarrow \text{the map is stable}$$
   $$e_{G'} = \phi(e_G) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1}) \Rightarrow \text{the inverse of } \phi(a) \text{ is also included in } \phi(G_0)$$

   from these if G_0 is a subgroup of G, then $\phi(G_0)$ is a subgroup of G'.

Exercise 1.3.5.

In this exercise, first we want to prove that $N \rtimes_\psi H$ is a group, and then that N is a normal subgroup of $N \rtimes_\psi H$.
To prove that $N \rtimes_\psi H$ is a group, let us check if the three basic properties of a group hold

1. Associativity:

$$\begin{aligned}
[(n_1, h_1)(n_2, h_2)](n_3, h_3) &= (n_1[\psi(h_1)](n_2), h_1h_2)(n_3, h_3) \\
&= (n_1[\psi(h_1)](n_2)[\psi(h_1h_2)](n_3), h_1h_2h_3) \\
(n_1, h_1)[(n_2, h_2)(n_3, h_3)] &= (n_1, h_1)(n_2[\psi(h_2)](n_3), h_2h_3) \\
&= (n_1[\psi(h_1)](n_2[\psi(h_2)](n_3)), h_1h_2h_3) \\
&= (n_1[\psi(h_1)](n_2) \cdot [\psi(h_1)]([\psi(h_2)](n_3)), h_1h_2h_3) \\
&= (n_1[\psi(h_1)](n_2) \cdot [\psi(h_1h_2)](n_3), h_1h_2h_3)
\end{aligned}$$

since $\psi(h_1) = \phi$ is an automorphism and since ψ is a homomorphism (which means that $\psi(h_1h_2) = \psi(h_1)\psi(h_2)$, from which $[\psi(h_1h_2)](n) = [\psi(h_1)]([\psi(h_2)](n)))$. These mean that $[(n_1,h_1)(n_2,h_2)](n_3,h_3) = (n_1,h_1)[(n_2,h_2)(n_3,h_3)]$, so the map is associative.

2. Existence of identity element

$$(n,h)(e_N,e_H) = (n[\psi(h)](e_N), he_H) = (ne_N, h) = (n,h),$$

so there exists an inverse, namely (e_N, e_H).

Note that $[\psi(h)](e_N) = e_N$, since $\psi(h)$ is an automorphism on N, which is a bijective homomorphism from N to itself, and we have seen in Exercise 1.2.15. that a homomorphism maps the identity of the domain to the identity of the codomain (and the domain and the codomain are the same in this case, so e_N is mapped to itself).

3. Existence of inverse

$$\begin{aligned}(n,h)(n,h)^{-1} &= (n,h)([\psi(h^{-1})](n^{-1}), h^{-1}) = (n[\psi(h)]([\psi(h^{-1})](n^{-1})), hh^{-1}) \\ &= (nn^{-1}, e_H) = (e_N, e_H),\end{aligned}$$

so there exists an inverse given by $(n,h)^{-1} = ([\psi(h^{-1})](n^{-1}), h^{-1})$.

Since all three basic properties of a group are satisfied, $N \rtimes_\psi H$ is indeed a group.
Next, let us see if N is a normal subgroup of $N \rtimes_\psi H$. First let us identify N with $\{(n,e_H)|n \in N\}$. If $(n_0,e_H) \in \{(n,e_H)|n \in N\}$ (which is the group we identified N with) and $(n,h) \in N \rtimes_\psi H$,

$$\begin{aligned}(n,h)(n_0,e_H)(n,h)^{-1} &= (n[\psi(h)](n_0), h)([\psi(h^{-1})](n^{-1}), h^{-1}) \\ &= (n[\psi(h)](n_0)[\psi(h)]([\psi(h^{-1})](n^{-1})), hh^{-1}) = (n[\psi(h)](n_0)n^{-1}, e_H).\end{aligned}$$

Since ψ is an automorphism, $[\psi(h)](n_0) \in N$, and thus $n[\psi(h)](n_0)n^{-1} \in N$ too. Therefore, $(n[\psi(h)](n_0)n^{-1}, e_H) \in \{(n,e_H)|n \in N\}$, which means that N is a normal subgroup of $N \rtimes_\psi H$.

Exercise 1.5.2.

In this exercise we want to prove that $(T(n),1)$ is a normal subgroup of $E(n)$, and that $E(n)$ is isomorphic to the semi-direct product of $T(n) \rtimes R(n)$.
First let us check if $(T(n),1)$ is a normal subgroup of $E(n)$. Let $a \in T(n)$, $(b,B) \in E(n)$. For $(a,1) \in (T(n),1)$ we have

$$\begin{aligned}(b,B)(a,1)(b,B)^{-1} &= (b+Ba, B)(-B^{-1}b, B^{-1}) = (b+Ba+B(-B^{-1}b), BB^{-1}) \\ &= (b+Ba-b, 1) = (Ba, 1) \in (T(n),1)\end{aligned}$$

thus $(T(n),1)$ is indeed a normal subgroup of $E(n)$.
Next let us see if $E(n)$ is isomorphic to the semi-direct product of $T(n) \rtimes R(n)$.
Let $N(n) = (T(n),1)$ and $H(n) = (0,R(n))$. Observe that

- $N(n) \lhd E(n)$ (from the previous part of this exercise)

- $N(n) \cap H(n) = \{(0,1)\} = e_E$
- if $b \in T(n)$, $B \in R(n)$, then

$$(b,1)(0,B) = (b + 1 \cdot 0, 1B) = (b,B)$$

  so any element of $E(n)$ can be obtained as a product of one-one element from $N(n)$ and $H(n)$.

These properties imply that $E(n)$ is the inner semi-direct product of $N(n)$ and $H(n)$.

Exercise 1.5.6.

In this exercise we want to prove that $(T(4),1)$ is a normal subgroup of $\mathcal{P}$, and that $\mathcal{P}$ is isomorphic to the semi-direct product of $T(4) \rtimes \mathcal{L}$.
First let us check if $(T(4),1)$ is a normal subgroup of $\mathcal{P}$. Let $a \in T(4)$, $(b,\Lambda) \in \mathcal{P}$. For $(a,1) \in (T(a),1)$ we have

$$\begin{aligned}(b,\Lambda)(a,1)(b,\Lambda)^{-1} &= (b + \Lambda a, \Lambda)(-\Lambda^{-1}b, \Lambda^{-1}) = (b + \Lambda a + \Lambda(-\Lambda^{-1}b), \Lambda\Lambda^{-1}) \\ &= (b + \Lambda a - b, 1) = (\Lambda a, 1) \in (T(4),1)\end{aligned}$$

thus $(T(4),1)$ is indeed a normal subgroup of $\mathcal{P}$.
Next let us see if $\mathcal{P}$ is isomorphic to the semi-direct product of $T(4) \rtimes \mathcal{L}$. Let $N = (T(4),1)$ and $H = (0,\mathcal{L})$. Observe that

- $N \lhd \mathcal{P}$ (from the previous part of this exercise)
- $N \cap H = \{(0,1)\} = e_{\mathcal{P}}$
- if $b \in T(4)$, $\Lambda \in \mathcal{L}$, then

$$(b,1)(0,\Lambda) = (b + 1 \cdot 0, \Lambda) = (b,\Lambda)$$

  so any element of $\mathcal{P}$ can be obtained as a product of one-one element from N and H.

These properties imply that $\mathcal{P}$ is the inner semi-direct product of N and H.