Solution for Homework 5

Xiangcan Li

March 22, 2021

Exercise 2.6.3 Prove Proposition 2.6.8: If $(G, *)$ is a group and $H \subset G$ is a subgroup, then the group operation on G restricts to an operation on H making it into a group.

Since $(G, *)$ is a group, we have

- The operation $*$ is associative.
- There is an identity $e \in G$, with the property that $e * g = g * e = g$, for all $g \in G$.
- For all $g \in G$, there exists an inverse $g^{-1} \in G$, with the property that $g * g^{-1} = g^{-1} * g = e$.

Let $*|_H$ denote the group operation on G restricts to an operation on H.

- Let $f, g, h \in H$. Since $H \subset G$, $f, g, h \in G$. Then we have

$$\begin{aligned} (f *|_H g) *|_H h &= (f * g) * h \\ &= f * (g * h) && \text{The operation } * \text{ is associative.} \\ &= f *|_H (g *|_H h) \end{aligned}$$

  We conclude the operation $*|_H$ is associative.

- Since H is a subgroup, for all $g, h \in H$, $g * h \in H$ and for all $g \in H$, $g^{-1} \in H$.
  Then for all $g, g^{-1} \in H \subset G$, we have $e = g *|_H g^{-1} = g * g^{-1} \in H$.
  Hence, there is an identity $e \in H$, with the property that $e * g = g * e = g$ for all $g \in H$.

- Since H is a subgroup, for all $g \in H$, $g^{-1} \in H$. Note that $g, g^{-1} \in G$.
  Then

$$\begin{aligned} g *|_H g^{-1} &= g * g^{-1} = e \in H \\ g^{-1} *|_H g &= g^{-1} * g = e \in H \end{aligned}$$

  Hence, for all $g \in H$, there exists an inverse $g^{-1} \in H$. with the property $g *|_H g^{-1} = g^{-1} *|_H g = e$.

We conclude the group operation on G restricts to an operation on H making it into a group.

Exercise 2.6.4 Prove that the roots of unity C_n, defined in Example 2.3.18 form a subgroup of the group S_1 from Example 2.6.12.

We have $C_n = \{e^{2\pi ki/n} \mid k \in \{0, \dots, n-1\}\}$ and $S^1 = \{e^{i\theta} \mid \theta \in \mathbb{R}\}$.
Note that $e^{i\theta} = \cos(\theta) + \sin(\theta) = \cos(\theta + 2n\pi) + \sin(\theta + 2n\pi) = e^{i(\theta+2n\pi)}$ for $n \in \mathbb{Z}$.
Suppose $g, h \in C_n$, write $g = e^{2\pi pi/n}$ and $h = e^{2\pi qi/n}$ for some $p, q \in \{0, \dots, n-1\}$.

- $g * h = e^{2\pi pi/n} \cdot e^{2\pi qi/n} = e^{2\pi(p+q)i/n}$.
  - If $(p + q) \in \{0, \dots, n-1\}$, then $e^{2\pi(p+q)i/n} \in C_n$.

– If $(p+q) \notin \{0, \ldots, n-1\}$, then $e^{2\pi(p+q)i/n} = e^{i(2\pi(p+q)/n+2m\pi)} = e^{2\pi(p+q+mn)i/n}$, where $m \in \mathbb{Z}$.
From Euclidean Algorithm, $p+q = sn+r$, where $s, r \in \mathbb{Z}$ and $0 \leq r < |n|$, or $0 \leq r < n$ since $n \geq 0$.
Then $r \in \{0, \ldots, n-1\}$. Hence, $p+q-sn \in \{0, \ldots, n-1\}$.
We set $m = -s$, then $p+q+mn \in \{0, \ldots, n-1\}$. Then $e^{2\pi(p+q)i/n} = e^{2\pi(p+q+mn)i/n} \in C_n$.

We conclude $g * h \in C_n$ in both cases.

- Write $g^{-1} = e^{-2\pi pi/n}$.
  – If $p = 0$, then $e^{-2\pi pi/n} \in C_n$.
  – For $p \neq 0$, we have $e^{2\pi pi/n} = e^{i(2\pi p/n+2m\pi)} = e^{2\pi(p+mn)i/n}$, where $m \in \mathbb{Z}$.
  From Euclidean Algorithm, $p = qn+r$, where $q, r \in \mathbb{Z}$ and $0 \leq r < |n|$, or $0 \leq r < n$ since $n \geq 0$. Then $r \in \{0, \ldots, n-1\}$. Hence, $p - qn \in \{0, \ldots, n-1\}$.
  We set $m = -q$, then $p+mn \in \{0, \ldots, n-1\}$. Then $e^{2\pi pi/n} = e^{2\pi(p+mn)i/n} \in C_n$.
  We conclude $g^{-1} \in C_n$.

Hence, C_n form a subgroup of the group S_1.

Exercise 2.6.9 Suppose R is a ring and X is a nonempty set. Complete the proof that R^X forms a ring by proving (a) that pointwise addition on R^X is commutative, (b) 0 is an additive identity, (c) $-f$ is the additive inverse of any $f \in R^X$ (and so $(R^X, +)$ is an abelian group), and (d) multiplication distributes over addition. If R is a commutative ring, prove that R^X is a commutative ring. If R has 1, prove that the function $1(x) = 1$ is a 1 for R^X.

(a) We have

$$\begin{aligned}
(f+g)(x) &= f(x) + g(x) && \text{by the definition of pointwise addition} \\
&= g(x) + f(x) && (R, +) \text{ is an abelian group} \\
&= (g+f)(x) && \text{by the definition of pointwise addition}
\end{aligned}$$

We conclude pointwise addition on R^X is commutative.
(b) The zero element of R^X is the zero function $0(x) = 0$ for all $x \in X$. Then we have

$$(f+0)(x) = f(x) + 0(x) = f(x) + 0 = f(x) \quad \forall x \in X \text{ and } f \in R^X$$

We conclude 0 is an additive identity.
(c) The additive inverse $-f$ of $f \in R^X$ is given by $(-f)(x) = -f(x)$ for all $x \in X$. Then we have

$$(f + (-f))(x) = f(x) + (-f)(x) = f(x) - f(x) = 0 \quad \forall x \in X \text{ and } f \in R^X$$

We conclude $-f$ is the additive inverse of any $f \in R^X$.
(d)Let $f, g, h \in R^X$, then we have

$$\begin{aligned}
(f(g+h))(x) &= f(x)(g+h)(x) && \text{by the definition of multiplication in } R^X \\
&= f(x)(g(x) + h(x)) && \text{by the definition of pointwise addition in } R^X \\
&= f(x)g(x) + f(x)h(x) && \text{multiplication distributes over addition in } R \\
&= (fg)(x) + (fh)(x) && \text{by the definition of multiplication in } R^X \\
&= (fg + fh)(x) && \text{by the definition of pointwise addition in } R^X
\end{aligned}$$

We conclude multiplication distributes over addition in R^X.
If R is a commutative ring, then multiplication in R is commutative. Then we have

$$\begin{aligned}
(fg)(x) &= f(x)g(x) && \text{by the definition of multiplication in } R^X \\
&= g(x)f(x) && \text{multiplication in } R \text{ is commutative} \\
&= (gf)(x) && \text{by the definition of multiplication in } R^X
\end{aligned}$$

Since multiplication in R^X is commutative, R^X is a commutative ring.

If R has 1, then $1a = a1 = a$ for all $a \in R$. Let $g \in R^X$ be 1 element in R^X. Then we have

$$(gf)(x) = (fg)(x) = f(x) \implies g(x)f(x) = f(x)g(x) = f(x).$$

Note that $f(x), g(x) \in R$, then $g(x)$ is 1 element in R. Hence, $g(x) = 1$. Then g exists and $g(x) = 1$.

We conclude the function $1(x) = 1$ is a 1 for R^X.

Exercise 2.6.11 Suppose $\mathbb{F}$ is any field. Find a pair of linear transformations $S, T \in \mathcal{L}(\mathbb{F}^2, \mathbb{F}^2)$ such that $ST \neq TS$.

Let $\mathbb{F} = \mathbb{R}$. From linear algebra, we know $A \in M_{m\times n}$ defines a linear map $L_A : \mathbb{R}^n \to \mathbb{R}^m$. Furthermore, let β and γ be the standard bases for $\mathbb{R}^n, \mathbb{R}^m$, then $[L_A]^\gamma_\beta = A$.

Let $S = L_A$, $T = L_B : \mathbb{R}^2 \to \mathbb{R}^2$ and β be the standard bases for $\mathbb{R}^2$, then $[S]^\beta_\beta = A$ and $[T]^\beta_\beta = B$.

We have

$$\begin{aligned} ST \neq TS &\implies [ST]^\beta_\beta \neq [TS]^\beta_\beta \\ &\implies [S]^\beta_\beta [T]^\beta_\beta \neq [T]^\beta_\beta [S]^\beta_\beta \\ &\implies AB \neq BA. \end{aligned}$$

Let

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \text{ and } B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

then we have

$$AB = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 2 & 1 \end{pmatrix}$$

and

$$BA = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix}.$$

Hence, $AB \neq BA$.

We conclude $S : x \mapsto Ax$ and $T : x \mapsto Bx$ are a pair of linear transformations $S, T \in \mathcal{L}(\mathbb{F}^2, \mathbb{F}^2)$ such that $ST \neq TS$.

Exercise 3.1.1 Prove part (ii) of Proposition 3.1.1:
(i) If $g, h \in G$ and either $g * h = h$ or $h * g = h$, then $g = e$.
(ii) If $g, h \in G$ and $g * h = e$ then $g = h^{-1}$ and $h = g^{-1}$.

We have

$$\begin{aligned} h^{-1} &= e * h^{-1} && \text{by the definition of the identity} \\ &= (g * h) * h^{-1} && e = g * h \\ &= g * (h * h^{-1}) && \text{by associativity} \\ &= g * e && \text{by the definition of the inverse} \\ &= g && \text{by the definition of the identity} \end{aligned}$$

and

$$\begin{aligned} g^{-1} &= g^{-1} * e && \text{by the definition of the identity} \\ &= g^{-1} * (g * h) && e = g * h \\ &= (g^{-1} * g) * h && \text{by associativity} \\ &= e * h && \text{by the definition of the inverse} \\ &= h && \text{by the definition of the identity.} \end{aligned}$$

We conclude if $g, h \in G$ and $g * h = e$ then $g = h^{-1}$ and $h = g^{-1}$.

Exercise 3.1.3 Suppose that G is a nonempty set with an associative operation $*$ such that the following holds:
1. There exists an element $e \in G$ so that $e * g = g$ for all $g \in G$, and
2. for all $g \in G$, there exists an element $g^{-1} \in G$ so that $g^{-1} * g = e$.
Prove that $(G, *)$ is a group.

For some arbitrary $g \in G$, if $g * g = g$, then we have

$$\begin{aligned} e &= g^{-1} * g && \text{by 2.} \\ &= g^{-1} * (g * g) && g * g = g \\ &= (g^{-1} * g) * g && \text{by associativity} \\ &= e * g && \text{by 2.} \\ &= g && \text{by 1.} \end{aligned}$$

Hence, if $g \in G$ and $g * g = g$, then $g = e$.
We have

$$\begin{aligned} (g * g^{-1})(g * g^{-1}) &= g * (g^{-1} * g) * g^{-1} && \text{by associativity} \\ &= g * e * g^{-1} && \text{by 2.} \\ &= g * (e * g^{-1}) && \text{by associativity} \\ &= g * g^{-1} && \text{by 1.} \end{aligned}$$

then $g * g^{-1} = e$.
Finally,

$$\begin{aligned} g * e &= g * (g^{-1} * g) && \text{by 2.} \\ &= (g * g^{-1}) * g && \text{by associativity} \\ &= e * g && g * g^{-1} = e \\ &= g && \text{by 1.} \end{aligned}$$

Hence, there is an identity $e \in G$, with the property that $e * g = g * e = g$, for all $g \in G$. Also, for all $g \in G$, there exists an inverse $g^{-1} \in G$, with the property that $g^{-1} * g = g * g^{-1} = e$. We conclude $(G, *)$ is a group.