Kyle Kloberdanz
5 March 2022

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.

Proof. We must show that H is a group. Recall a set G to be a group, group it must satisfy the following conditions.
(i) $*$ is associative
(ii) there is an identity $e \in G$
(iii) there exists an inverse $g^{-1} \in G$

Because were know that H is a subgroup of G, we know by the definition Of a subgroup that for all $g \in H$, $g^{-1} \in H$, and therefore we know that there exists an inverse for every g in H, satisfying (iii)

We also know from the definition of a subgroup, that for all $g, h \in H$ that $g * h \in H$. Because of this, and also from the definition that for every $h \in H$, that $h^{-1} \in H$, then if $h = g^{-1}$, then $g * h = g * g^{-1} = e$. Also, if $g = h^{-1}$ then $g*h = h^{-1}*h = e$. We can see that there exists an identity $e \in H$, satisfying (ii)

From the definition of a subgroup, we can see that for $f, g, h \in H$ that $f, g, h \in G$ and also for $x \in H$, $x = f*g*h$ that x is also in G. Because we know G is a group, and the operator on a group is associative, For $x \in G$, $x = (f*g)*h = f*(g*h)$, but because $x, f, g, h \in H$, then $x \in H$, $x = (f * g) * h = f * (g * h)$, satisfying (i), that $*$ is an associative operator for H.

Therefore, because we have satisfied i, ii, iii, we know that H is a group with the operator $*$ restricted on it.

□

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.

Proof. Recall:

$$C_n = \{e^{2\pi ki/n} | k \in \{0, ..., n-1\}\}$$

Where $k, n \in \mathbb{Z}$

$$S^1 = \{e^{i\theta} | \theta \in \mathbb{R}\}$$

Where $S^1 < \mathbb{C}^\times$ with multiplication.

We must demonstrate that $C_n < S^1$.

We must first show that for the set C_n that $C_n \subset S^1$. We notice that $2\pi k/n \in \mathbb{R}$. Hence $\{2\pi k/n | k \in \{0, ..., n-1\}\} \subset \mathbb{R}$. Hence $\{2\pi k/n | k \in \{0, ..., n-1\}\}$ is a subset of all possible values of θ. Therefore we can see that $C_n \subset S^1$.

Next, we must show that for all $x, y \in C_n$, that $xy \in C_n$. Let $k, l \in \{0, ..., n-1\}$ such that $x = e^{2\pi ik/n}$ and $y = e^{2\pi il/n}$

$$xy = e^{2\pi ik/n}e^{2\pi il/n} = e^{(2\pi ik/n)+(2\pi il/n)} = e^{(2\pi i/n)(k+l)} = e^{2\pi i(k+l)/n}$$

Rewritten using Euler's Formula:

$$e^{2\pi i(k+l)/n} = cos(2\pi(k+l)/n) + i\ sin(2\pi(k+l)/n)$$

Recall if $k \equiv l \pmod n$, then $cos(2\pi k/n) = cos(2\pi l/n)$ and $sin(2\pi k/n) = sin(2\pi l/n)$

Given this property of sin and cos with respect to multiples of 2π, we can see that k and l form an equivalency class $\pmod n$, and by equivalency class addition, $[k] + [l] = [k + l]$, hence for any $x, y \in C_n$, $xy \in C_n$.

We must now show that for all $x \in C_n$, $x^{-1} \in C_n$. Let $x = e^{2\pi ki/n}$, hence $x^{-1} = e^{-2\pi ki/n}$. We must show that $xx^{-1} = x^{-1}x = 1$.

$$xx^{-1} = e^{2\pi ki/n}e^{-2\pi ki/n} = \frac{e^{2\pi ki/n}}{e^{2\pi ki/n}} = 1$$
$$x^{-1}x = e^{-2\pi ki/n}e^{2\pi ki/n} = \frac{e^{2\pi ki/n}}{e^{2\pi ki/n}} = 1$$

Hence for all $x \in C_n$, we have shown that there exists the inverse x^{-1} such that $xx^{-1} = x^{-1}x = 1$.

Therefore, because we have shown that $C_n < S^1$, for all $x, y \in C_n$, that $xy \in C_n$, and for all $x \in C_n$, $x^{-1} \in C_n$, we conclude that $C_n < S^1$. In other words, C_n is a subgroup of 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

Proof. (a) that the pointwise addition on R^X is commutative,

Recall, pointwise addition states $(f + g)(x) = f(x) + g(x)$ where $f, g \in R^X$ Because for a ring R, $(R, +)$ forms an abelian group, and therefore addition is commutative. Because of this, we see that:

$$(f + g)(x) = f(x) + g(x) = g(x) + f(x) = (g + f)(x)$$

Therefore pointwise addition on R^X is commutative.

(b) 0 is an additive identity,

$$(0 + f)(x) = 0(x) + f(x) = f(x) = f(x) + 0(x) = (f + 0)(x)$$

Therefore, 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)

$$(-f + f)(x) = -f(x) + f(x) = 0 = f(x) + (-f(x)) = (f + (-f))(x)$$

Therefore, $-f$ is the additive inverse of any $f \in R^X$

(d) multiplication distributes over addition.

Recall, pointwise multiplication states $(fg)(x) = f(x)g(x)$, where $f, g \in R^X$.

Let $a, b, c \in R^X$

$$(a + b)(x) = a(x) + b(x)$$
$$c(a + b)(x) = c(x)(a(x) + b(x))$$
$$c(a + b)(x) = (c(x)a(x)) + (c(x)b(x))$$
$$c(a + b)(x) = (c(x)a(x)) + (c(x)b(x))$$
$$c(a + b)(x) = (ca)(x) + (cb)(x)$$
$$c(a + b)(x) = ((ca) + (cb))(x)$$

Therefore, multiplication distributes over addition.

If R is a commutative ring, prove that R^X is a commutative ring.

As we saw in (a), we have already shown that addition is commutative. Now we will demonstrate that multiplication is commutative.

$$(fg)(x) = f(x)g(x) = g(x)f(x) = (gf)(x)$$

If R has 1, prove that the function $1(x) = 1$ is a 1

$$(1f)(x) = 1(x)f(x) = f(x) = f(x)1(x) = (f1)(x)$$

Therefore, $1(x) = 1$ is a 1

Finally, because we have satisfied the conditions of a ring, we have shown that R^X is indeed a ring. $\square$

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 $ST \neq TS$.

Suppose $S(x, y) = (x + y, x + y)$ and $T(x, y) = (x + y, x + (-y))$ where $x, y \in \mathbb{Q}$

$$ST(4, 5) = S(T(4, 5)) = S(4 + 5, 4 - 5) = S(9, -1) = (8, 8)$$
$$TS(4, 5) = T(S(4, 5)) = T(9, 9) = (18, 0)$$

Therefore:

$$ST(4, 5) = (8, 8) \neq TS(4, 5) = (18, 0)$$
$$ST(4, 5) \neq TS(4, 5)$$

Exercise 3.1.1: Prove part (ii) of Proposition 3.1.1:

Note: for brevity, I'll omit $*$, and instead show $g * h$ as gh.
(i) If $g, h \in G$ and either $g * h = h$ or $h * g = h$, then $g = e$.

Proof.

$$gh = h$$
$$ghh^{-1} = hh^{-1}$$
$$ge = e$$
$$g = e$$

Also:

$$hg = h$$
$$h^{-1}hg = h^{-1}h$$
$$eg = e$$
$$g = e$$

□

(ii) If $g, h \in G$ and $g * h = e$ then $g = h^{-1}$ and $h = g^{-1}$

Proof.

$$gh = e$$
$$g^{-1}gh = g^{-1}e$$
$$h = g^{-1}e$$
$$h = g^{-1}$$

At the same time:

$$gh = e$$
$$ghh^{-1} = eh^{-1}$$
$$g = eh^{-1}$$
$$g = h^{-1}$$

□

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.

The difference between this and the definition of a group is that we are only assuming that e is a "left identity", and that elements have a "left inverse". Of course, we could have replaced "left" with "right" and there is an analogous definition of a group. Hint: Start by proving that if $g \in G$ and $g * g = g$, then $g = e$. Then prove that $g * g^{-1} = e$ (that is, the left inverse is also a right inverse for the left identity). Finally, prove that the left identity is also a right identity.

Proof. First, we will show that for $g \in G$, if $g * g = g$, then $g = e$. For brevity, I will omit the $*$.

$$gg = g$$
$$g^{-1}gg = g^{-1}g$$
$$eg = e$$
$$g = e$$

Second, we will show that $e = g^{-1}g = gg^{-1}$

$$e = g^{-1}g = eg^{-1}g = ((g^{-1})^{-1}g^{-1})(g^{-1}g) = ((g^{-1})^{-1}g)e = gg^{-1}e$$

Because $e = gg^{-1}e$, and we know that e is a left identity, then the only way for $e = gg^{-1}e$, is if $gg^{-1} = e$, which yields $e = ee$ (left identity for e), hence $gg^{-1} = g^{-1}g$, a right inverse.

Third, we will find the right identity. Because $g^{-1}g = gg^{-1}$,

$$g = eg = (gg^{-1})g = g(g^{-1}g) = ge = g$$

Finally, because we know that $*$ is associative (given by the problem statement), and there exists an identity $e \in G$ such that $e * g = g * e = g$ for all $g \in G$, and for all $g \in G$, there exists an inverse $g^{-1} \in G$, such that $g * g^{-1} = g^{-1} * g = e$, we know that G is indeed a group. $\square$