Solutions to HW3 of Math 103A, Fall 2018

P.38 Q4

$\mathscr{G}_3$ is the first axiom that does not hold. Because clearly the product in $\mathbb{Q}$ is associative and has identity 1. But $0 \in \mathbb{Q}$ does not have an inverse since for any $x \in \mathbb{Q}, 0 \cdot x = 0$.

Q19

a. To show that $*$ gives a binary operation on S, we only need to show that for any $a, b \in S$, $a * b \in S$. Suppose not, then $a * b \notin S$ for some $a, b \in S$, which means $a, b \neq -1$ are real numbers but $-1 = a * b = a + b + ab$. Then

$$0 = a + b + ab + 1 = (a + 1)(b + 1).$$

Thus either $a = -1$ or $b = -1$, a contradiction. So $*$ gives a binary operation on S.
b. For $\mathscr{G}_1$, $\forall a, b, c \in S$,

$$\begin{aligned}(a * b) * c &= (a + b + ab) * c \\ &= (a + b + ab) + c + (a + b + ab)c \\ &= a + b + c + ab + ac + bc + abc.\end{aligned}$$

$$\begin{aligned}a * (b * c) &= a * (b + c + bc) \\ &= a + (b + c + bc) + a(b + c + bc) \\ &= a + b + c + ab + bc + ac + abc.\end{aligned}$$

Thus $(a * b) * c = a * (b * c)$, and $\mathscr{G}_1$ holds. For $\mathscr{G}_2$, $\forall a \in S$,

$$0 * a = 0 + a + 0 \cdot a = a.$$

As $*$ is clearly commutative, $a * 0 = 0 * a = a$, and thus $(S, *)$ has identity 0.
For $\mathscr{G}_3$, $\forall a \in S$, we try to solve $b \in S$ so that

$$0 = a * b = a + b + ab.$$

So

$$b(1+a) = -a, \quad b = -\frac{a}{1+a}.$$

Thus a has inverse $-\frac{a}{1+a}$, which makes sense as $a \neq -1$. Therefore $(S, *)$ is a group.

Q30

a. Clearly for nonzero $a, b \in \mathbb{R}$, $a * b = |a|b \neq 0$. So $*$ gives a binary operation on $\mathbb{R}^*$. For any $a, b, c \in \mathbb{R}^*$,

$$(a * b) * c = (|a|b) * c = ||a|b|c = |ab|c = |a|(|b|c) = a * (|b|c) = a * (b * c).$$

Thus $*$ is associative.

b. 1 is a left identity as for any $a \in \mathbb{R}^*$,

$$1 * a = |1|a = 1 \cdot a = a.$$

For any $a \in \mathbb{R}$, $1/|a|$ is its right inverse since

$$a * \frac{1}{|a|} = |a|\frac{1}{|a|} = 1.$$

c. $(\mathbb{R}^*, *)$ is not a group since if it is, then 1 should be a right identity. But for $a = -2$,

$$a * 1 = |a| \cdot 1 = 2 \neq a,$$

a contradiction. Thus $(\mathbb{R}^*, *)$is not a group.

d. We can prove that if $(S, *)$ is associative and has a left (resp. right) identity and for any element there is a left (resp. right) inverse, then $(S, *)$ is a group. But if we only have a left identity and right inverses for any elements, we cannot say $(S, *)$ is a group.

Q32

For any $a, b \in G$,

$$e = (a * b) * (a * b).$$

So

$$(a * b)^{-1} = a * b.$$

By Corollary 4.18,

$$(a * b)^{-1} = b^{-1} * a^{-1} = b * a.$$

Thus

$$a * b = (a * b)^{-1} = b * a.$$

Or we can still start from the equation

$$e = (a * b) * (a * b) = a * (b * a) * b.$$

And then multiply a on the left for both sides

$$a = (b * a) * b.$$

Multiplying b on the right for both sides, we have

$$a * b = b * a.$$

Q35

Suppose

$$(a * b)^2 = a^2 * b^2.$$

Then

$$a * (b * a) * a = (a * b) * (a * b) = (a * b)^2 = a^2 * b^2 = a * (a * b) * b.$$

Multiplying a^{-1} on the left and then multiplying b^{-1} on the right, we have

$$b * a = a * b.$$

Q36

Since $a * b * c = e$, $b * c = a^{-1}$. By the definition of inverses,

$$e = a^{-1} * a = (b * c) * a = b * c * a.$$

P.55 Q2

$\mathbb{Q}^+$ is not a subgroup of $(\mathbb{C}, +)$.

Because for example $x = 1 \in \mathbb{Q}^+$, but the inverse of 1 under addition in $\mathbb{C}$ is -1 which is not in $\mathbb{Q}^+$. Thus by Theorem 5.14 (on P.52), $\mathbb{Q}^+$ is not a subgroup of $(\mathbb{C}, +)$.

Q3

$7\mathbb{Z}$ is a subgroup of $\mathbb{C}$ under addition.

First, for any $x, y \in 7\mathbb{Z}$, by definition, $x = 7k, y = 7l$ for some integers k, l. Then $x + y = 7k + 7l = 7(k + l) \in 7\mathbb{Z}$ and thus $7\mathbb{Z}$ is closed under addition.

0 is the identity of addition in $\mathbb{C}$ and is also in $7\mathbb{Z}$.

For any $x = 7k \in 7\mathbb{Z}$, the inverse of x is $-x = 7(-k)$, which is in $7\mathbb{Z}$. By Theorem 5.14, $7\mathbb{Z}$ is a subgroup of $\mathbb{C}$ under addition.

Q39

a. True

b. False

c. True

d. False (Consider the group with only one element: $G = \{e\}$.)

e. False

f. False

g. False

h. False

i. True

j. False

Q41

For every $g', h' \in \phi[H]$, by definition, $g' = \phi(g), h' = \phi(h)$ for some $g, h \in H$. Since $g * h \in H$ and ϕ is a homomorphism,

$$g' *' h' = \phi(g) *' \phi(h) = \phi(g * h) \in H.$$

So $\phi[H]$ is closed under $*'$. And we have proved that ϕ carries identity e in G to the identity e' in G', i.e., $e' = \phi(e) \in \phi[H]$. For any $h' = \phi(h) \in \phi[H]$, where $h \in H$, since

$$\phi(h^{-1}) *' h' = \phi(h^{-1} * h) = \phi(e) = e' = \phi(h * h^{-1}) = h' *' \phi(h^{-1}),$$

$\phi(h^{-1})$ is the inverse of h' in G' and $\phi(h^{-1})$ is in $\phi[H]$. Thus by theorem 5.14, $\phi[H]$ is a subgroup.

Q43

First for any $hk, h'k' \in HK$, where $h, h' \in H, k, k' \in K$,

$$(hk)(h'k') = (hh')(kk') \in HK$$

as G is abelian. Thus HK is closed under the binary operation of G. Since H, K are subgroups of G, the identity $e \in H, e \in K$ and thus $e = ee \in HK$. Finally, for any $hk \in HK$, where $h \in H, k \in K$, $h^{-1} \in H$ and $k^{-1} \in K$ as H, K are subgroups. Since

$$(h^{-1}k^{-1})hk = (h^{-1}h)(k^{-1}k) = e,$$

$(h^{-1}k^{-1})$ is the inverse of hk and is also in HK. By theorem 5.14, HK is a subgroup.

Q51

First, for any $x, y \in H_a$,

$$(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy).$$

Thus $xy \in H_a$. Since

$$ea = ae = a,$$

$e \in H_a$. For any $x \in H_a$, since

$$xa = ax,$$

we have

$$ax^{-1} = x^{-1}xax^{-1} = x^{-1}axx^{-1} = x^{-1}a.$$

Thus $x^{-1} \in H_a$. By theorem 5.14, H_a is a subgroup.