1 Introduction to Groups

1.1 Basic Axioms and Examples, 1-18

1.1.1

(a) Yes: Subtraction in $\mathbb{Z}$ is associative

(b) Yes. Note:

$$\begin{aligned}(a \star b) \star c &= (a + b + ab) \star c &(1)\\ &= (a + b + ab) + c + (a + b + ab)c &(2)\\ &= a + b + ab + c + ac + bc + abc &(3)\end{aligned}$$

And

$$\begin{aligned}a \star (b \star c) &= a \star (b + c + bc) &(4)\\ &= a + (b + c + bc) + a(b + c + bc) &(5)\\ &= a + b + c + bc + ab + ac + abc &(6)\end{aligned}$$

Equations (3) and (6) are clearly equal from commutativity of addition in $\mathbb{R}$.

(c) No. Note:

$$\begin{aligned}a \star (b \star c) &= (\frac{a+b}{5}) \star c &(7)\\ &= \frac{\frac{a+b}{5} + c}{5} &(8)\\ &= \frac{a+b}{25} + \frac{c}{5} &(9)\\ &= \frac{a+b+5c}{25} &(10)\end{aligned}$$

But

$$\begin{aligned}a \star (b \star c) &= a \star (\frac{b+c}{5}) &(11)\\ &= \frac{a + \frac{b+c}{5}}{5} &(12)\\ &= \frac{a}{5} + \frac{b+c}{25} &(13)\\ &= \frac{5a+b+c}{25} &(14)\end{aligned}$$

Equations (10) and (14) are clearly not equal in general (e.g. set $a = 0, b = 0, c = 1$)

(d) Yes, this is associative. It is just unreduced addition in $\mathbb{Q}$

(e) No:

$$\begin{aligned}(a \star b) \star c &= (\frac{a}{b}) \star c\\ &= \frac{\frac{a}{b}}{c}\\ &= \frac{a}{bc}\end{aligned}$$

But

$$\begin{aligned}a \star (b \star c) &= a \star \frac{b}{c}\\ &= \frac{a}{\frac{b}{c}}\\ &= \frac{ac}{b}\end{aligned}$$

Set $a = 1, b = 1, c = 2$ to see they are not equal

1.1.2

(a) No. As mentioned in the text, subtraction on $\mathbb{Z}$ is not commutative

(b) Yes:

$$\begin{aligned} a \star b &= a + b + ab \\ &= b + a + ba \\ &= b \star a \end{aligned}$$

(c) Yes:

$$\begin{aligned} a \star b &= \frac{a+b}{5} \\ &= \frac{b+a}{5} \\ &= b \star a \end{aligned}$$

(d) Yes. Again, this is just unreduced addition in $\mathbb{Q}$.

(e) No. $a \star b = \frac{a}{b}$ but $b \star a = \frac{b}{a}$.

1.1.3

$$\begin{aligned} (\bar{k} + \bar{l}) + \bar{m} &= k \bar{+} l + \bar{m} \\ &= (k + \bar{l}) + m \\ &= k + (\bar{l} + m) \\ &= \bar{k} + l \bar{+} m \\ &= \bar{k} + (\bar{l} + \bar{m}) \end{aligned}$$

1.1.4

$$\begin{aligned} (\bar{k} \cdot \bar{l})\bar{m} &= \bar{kl} \cdot \bar{m} \\ &= (k\bar{l})m \\ &= k(\bar{l}m) \\ &= \bar{k} \cdot l\bar{m} \\ &= \bar{k} \cdot (\bar{l}\bar{m}) \end{aligned}$$

1.1.5

The element $\bar{0}$ doesn't have an inverse.

1.1.6

In each of these, I will denote the set in question by G

(a) Yes. The three group properties are all inherited from $\mathbb{Q}$ (the identity and the inverses are clearly in G), so we just have to verify that G is closed under addition. Given $\frac{a}{b}$, $\frac{c}{d} \in G$, we have

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

Since b, d are odd, bd is also odd. And since bd is odd, no even number divides it. Hence, reducing the fraction maintins oddness of the denominator, and the result is still in G

(b) No. This set isn't closed under addition: $\frac{1}{2} + \frac{3}{2} = \frac{4}{2} = \frac{2}{1}$

(c) No: $\frac{2}{3}+\frac{2}{3}=\frac{4}{3}$ and $|\frac{4}{3}|>1$

(d) No: $\frac{5}{3}-\frac{4}{3}=\frac{1}{3}$ and $|\frac{1}{3}|<1$

(e) Yes. This is the set

$$G=\mathbb{Z}\cup\{\frac{r}{2}|r\in\mathbb{Z}\}$$

This set is clearly closed under addition. Associativity is inherited from $\mathbb{Q}$. The identity $\frac{0}{2}$ is in G. The inverse $\frac{-r}{2}$ of $\frac{r}{2}$ is in G.

(f) No. The set isn't closed under addition. $\frac{3}{2}+\frac{2}{3}=\frac{9}{6}+\frac{4}{6}=\frac{13}{6}$ which is not under G.

1.1.7

- The set G is clearly closed under the operation, since we always cut off the ones place and use nonnegative numbers.
- The operation is associative. Adding two real numbers and cutting off the ones place, then adding another one and cutting off the ones place, is the same as adding them all and THEN cutting off the ones place
- The identity is 0
- The inverse of x is $1-x$

1.1.8

(a) If $z,c\in\mathbb{C}$, then $\exists n,m\in\mathbb{Z}^+$ s.t. $z^n,c^m=1$. And

$$\begin{aligned}(zc)^{nm}&=z^{nm}c^{nm}\\&=(z^n)^m(c^m)^n\\&=1^m1^n\\&=1\end{aligned}$$

Hence, $zc\in\mathbb{C}$, so G is closed under complex multiplication. Associativity is inherited from associativity of complex multiplication. The identity 1^1 i in G. And given $z\in G$ with $z^n=1$, $n\in\mathbb{Z}^+$, we have $(\frac{1}{z})^n=\frac{1^n}{z^n}=\frac{1}{1}=1$, so the inverse of z is in G.

(b) No identity element. $0\notin G$

1.1.9

(a) Note $(a+b\sqrt{2})+(c+d\sqrt{2})=(a+c)+(b+d)\sqrt{2}\in G$. So G is closed under the operation. Associativity follows from associativity of addition in $\mathbb{R}$. The identity is $0=0+0\sqrt{2}$. And the inverse of $a+b\sqrt{2}$ is $-a-b\sqrt{2}$.

(b) Set $G'=G-\{0\}$. Note that

$$\begin{aligned}(a+b\sqrt{2})(c+d\sqrt{2})&=ac+(ad+bc)\sqrt{2}+2bd\\&=(ac+2bd)+(ad+bc)\sqrt{2}\\&\in G\end{aligned}$$

And since in $\mathbb{R}$, $xy=0\implies x=0$ or $y=0$, the result is in fact in $G-\{0\}=G'$. Hence, G' is closed under multiplication. Associativity is inherited from the reals, the identity is $1+0\sqrt{2}=1$, and the following demonstrates that the inverse is in G':

$$\begin{aligned}\frac{1}{a+b\sqrt{2}}&=\frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})}\\&=\frac{a-b\sqrt{2}}{a^2-2b^2}\\&=\frac{a}{a^2-2b^2}+\frac{-b}{a^2-2b^2}\sqrt{2}\end{aligned}$$

1.1.10

NO SHIT. Transposing the matrix is equivalent to reversing the order of operations, and the upper triangle remains the same since the matrix is symmetric.

1.1.11

Process: $|\bar{r}| = \frac{l}{r}$ where $l = \text{lcm}(r, 12)$. l itself can be calculated by $gl = 12r$, where $g = \gcd(r, 12)$. Given that, we have,

$$
\begin{aligned}
|\bar{0}| &= 0 \\
|\bar{1}| &= 12 \\
|\bar{2}| &= 6 \\
|\bar{3}| &= 4 \\
|\bar{4}| &= 3 \\
|\bar{5}| &= 12 \\
|\bar{6}| &= 2 \\
|\bar{7}| &= 12 \\
|\bar{8}| &= 3 \\
|\bar{9}| &= 4 \\
|\bar{1}0| &= 6 \\
|\bar{1}1| &= 12
\end{aligned}
$$

1.1.12

Noting that $5^2 = 12 \cdot 2 + 1$, $7^2 = 12 \cdot 4 + 1$, $13 = 12 + 1$, we have

$$
\begin{aligned}
|\bar{1}| &= 1 \\
|\bar{-}1| &= 2 \\
|\bar{5}| &= 2 \\
|\bar{7}| &= 2 \\
|\bar{-}7| &= 2 \\
|\bar{1}3| &= 1
\end{aligned}
$$

1.1.13

Same process as in 1.1.11, yielding

$$
\begin{aligned}
|\bar{1}| &= 36 \\
|\bar{2}| &= 18 \\
|\bar{6}| &= 6 \\
|\bar{9}| &= 4 \\
|\bar{1}0| &= 18 \\
|\bar{1}2| &= 3 \\
|\bar{-}1| &= 36 \\
|\bar{-}10| &= 18 \\
|\bar{-}18| &= 2
\end{aligned}
$$

1.1.14

Note that $5^3 = 36 \cdot 4 + 1$, $13^3 = 36 \cdot 61 + 1$, $17^2 = 36 \cdot 8 + 1$. Then

$$\begin{aligned} |\bar{1}| &= 1 \\ |\bar{-}1| &= 2 \\ |\bar{5}| &= 3 \\ |\bar{1}3| &= 3 \\ |\bar{-}13| &= 3 \\ |\bar{1}7| &= 2 \end{aligned}$$

1.1.15

Using generalized associativity,

$$\begin{aligned} (a_1 a_2 \cdots a_{n-1} a_n)({a_n}^{-1} {a_{n-1}}^{-1} \cdots {a_1}^{-1}) &= a_1 a_2 \cdots a_{n-1}(a_n {a_n}^{-1}) {a_{n-1}}^{-1} \cdots {a_1}^{-1} \\ &= a_1 a_2 \cdots a_{n-1}(1) {a_{n-1}}^{-1} \cdots {a_1}^{-1} \\ &= a_1 a_2 \cdots a_{n-1} {a_{n-1}}^{-1} \cdots {a_1}^{-1} \end{aligned}$$

Et cetera. You could make this an "inductive" proof but it's not necessary.

1.1.16

NOOOOOOOOOOO SHIIIIIIIIIIIIIIIIIIIIIT

1.1.17

$$\begin{aligned} |x| &= n \\ \implies x^n &= 1 \\ \implies x^n x^{-1} &= 1 \cdot x^{-1} \\ \implies x^{n-1} x x^{-1} &= x^{-1} \\ \implies x^{n-1} \cdot 1 &= x^{-1} \\ \implies x^{n-1} &= x^{-1} \end{aligned}$$

1.1.18

The proof is in the very formulation of the exercise llololololol