1 Introduction to Groups

1.1 Basic Axioms and Examples

1.1.1

(a) No: $a - (b - c) = a - b + c \neq (a - b) - c$

(b) Yes. Note:

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

And

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

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

(c) No. Note:

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

But

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

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

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

1.1.4

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

1.1.5

The element $\overline{0}$ 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

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

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

$$\begin{aligned}
|\overline{0}| &= 1 \\
|\overline{1}| &= 12 \\
|\overline{2}| &= 6 \\
|\overline{3}| &= 4 \\
|\overline{4}| &= 3 \\
|\overline{5}| &= 12 \\
|\overline{6}| &= 2 \\
|\overline{7}| &= 12 \\
|\overline{8}| &= 3 \\
|\overline{9}| &= 4 \\
|\overline{10}| &= 6 \\
|\overline{11}| &= 12
\end{aligned}$$

1.1.12

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

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

1.1.13

Same process as in 1.1.11, yielding

$$\begin{aligned}
|\overline{1}| &= 36 \\
|\overline{2}| &= 18 \\
|\overline{6}| &= 6 \\
|\overline{9}| &= 4 \\
|\overline{10}| &= 18 \\
|\overline{12}| &= 3 \\
|\overline{-1}| &= 36 \\
|\overline{-10}| &= 18 \\
|\overline{-18}| &= 2
\end{aligned}$$

1.1.14

Note that $5^3 = 36 \cdot 4 + 1$, $13^3 = 36 \cdot 61 + 1$, $17^2 = 36 \cdot 8 + 1$, $(-13)^6 = (13^3)^2$. Then

$$\begin{aligned}
|\overline{1}| &= 1 \\
|\overline{-1}| &= 2 \\
|\overline{5}| &= 3 \\
|\overline{13}| &= 3 \\
|\overline{-13}| &= 6 \\
|\overline{17}| &= 2
\end{aligned}$$

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 SHIIIIIIIIIIIIIIIIIIIIIIT

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 llolololol

1.1.19

(a) and (b) are trivial. For (c),

- Case: $a \geq 0, b \leq 0$.
  We treat $-b$ as a nonnegative number, and $x^a x^b = x^a {(x^{-b})}^{-1} = x^a (x^{-1})^{-b} = x^{a-(-b)} = x^{a+b}$.
  Also $(x^a)^b = {((x^a)^{-b})}^{-1} = {(x^{-ab})}^{-1} = x^{ab}$.
  The case $a \leq 0, b \geq 0$ is analgous to this one.
- Case: $a, b \leq 0$
  We treat both $-a, -b$ as nonnegative numbers, and $x^a x^b = (x^{-a})^{-1} {(x^{-b})}^{-1} = {(x^{-b} x^{-a})}^{-1} = {(x^{-b+-a})}^{-1} = {(x^{-(a+b)})}^{-1} = x^{a+b}$.
  Also $(x^a)^b = {((x^{-1})^{-a})^{-b})}^{-1} = {((x^{-1})^{ab})}^{-1} = (x^{-1})^{-ab} = x^{ab}$

1.1.20

I'm going to prove a Lemma that will be useful for these exercises

Lemma 1.1. *Let $|x| = n$. If $m \in \mathbb{Z}$, then $x^m = x^r$ for $0 \leq r < n$, $r \equiv m \pmod{n}$.*

Proof. This follows directly from the Euclidean algorithm. We can write $m = dn + r$ where r satisfies the inequalities and congruence above. Then

$$\begin{aligned} x^m &= x^{dn+r} \\ &= x^{dn}x^r \\ &= (x^n)^d x^r \\ &= 1^d x^r \\ &= x^r \end{aligned}$$

$\square$

From this we immediately obtain two corollaries:

Corollary 1.1.1. *$x^m = 0 \implies m$ is a multiple of $|x|$.*

Corollary 1.1.2. *If $|x| = n$, then $1, x, x^2, \ldots, x^{n-1}$ are distinct*

Nowe we finish the exercise:
Let $|x| = n$. Then $(x^{-1})^n = x^{-n} - (x^n)^{-1} = 1^{-1} = 1$. Hence, $|x^{-1}| \leq n$.
Now suppose $|x^{-1}| = m$. Then $0 < m \leq n$. But

$$\begin{aligned} x^m &= ((x^{-1})^{-1})^m \\ &= (x^{-1})^{-m} \\ &= ((x^{-1})^m)^{-1} \\ &= 1^{-1} \\ &= 1 \end{aligned}$$

Hence, by Corollary 1.1.1, m is a multiple of n, but $0 < m \leq n$ means that $m = n$.

1.1.21

Let $n = 2l + 1$. Then

$$\begin{aligned} x^n &= 1 \\ \implies x^{2l+1} &= 1 \\ \implies x^{2l}x &= 1 \\ \implies x^{2l} &= x^{-1} \\ \implies (x^2)^l &= x^{-1} \\ \implies (x^2)^l x^2 &= x^{-1}x^2 \\ \implies (x^2)^{l+1} &= x \end{aligned}$$

Why did we need G to be finite? Lol

1.1.22

Let $|x| = n$. Then $(g^{-1}xg)^n = g^{-n}x^n g^n = g^{-n}g^n = 1$, so $|g^{-1}xg| \leq n$. Suppose $|g^{-1}xg| = m$, with $0 < m \leq n$. Then

$$\begin{aligned} (g^{-1}xg)^m &= 1 \\ \implies g^{-m}x^m g^m &= 1 \\ \implies x^m g^m &= g^m \\ \implies x^m &= 1 \end{aligned}$$

So m must be a multiple of $|x| = n$, but $0 < m \leq n$ so $m = n$.
Now let $|ab| = n$. Then

$$\begin{aligned} (ab)^n &= 1 \\ \iff a^n b^n &= 1 \\ \iff a^n &= b^{-n} \\ \iff 1 &= a^{-n} b^{-n} \\ \iff 1 &= (a^n)^{-1} (b^n)^{-1} \\ \iff 1 &= b^n a^{n-1} \\ \iff 1 &= (ba)^{n-1} \end{aligned}$$

So $|(ba)^{-1}| \leq n$. But if we follow the proof above backwards with arbitrary n, we see that since $|ab| = n$, $|(ba)^{-1}| = n$. But by 1.1.20, we get that in fact $|ba| = n$.

1.1.23

$$\begin{aligned} x^n &= 1 \\ \iff x^{st} &= 1 \\ \iff (x^s)^t &= 1 \end{aligned}$$

So $|x^s| \leq t$. Follow the proof backwards to establish that $|x^s| = t$.

1.1.24

Clearly $(ab)^1 = a^1 b^1$.
Now suppose for $n > 0$, $(ab)^n = a^n b^n$. Then

$$\begin{aligned} (ab)^{n+1} &= (ab)^n ab \\ &= a^n b^n ab \\ &= a^n a b^n b \\ &= a^{n+1} b^{n+1} \end{aligned}$$

so $(ab)^n = a^n b^n$ for $n \geq 1$. The case $n = 0$ is obvious. And also if $n \geq 0$, we have

$$\begin{aligned} (ab)^{-n} &= ((ab)^n)^{-1} \\ &= (a^n b^n)^{-1} \\ &= (b^n)^{-1} (a^n)^{-1} \\ &= b^{-n} a^{-n} \\ &= a^{-n} b^{-n} \end{aligned}$$

So $(ab)^n = a^n b^n$ for negative n as well.

1.1.25

Given $x, y \in G$,

$$\begin{aligned} xy &= xy1 \\ &= xy(yx)^2 \\ &= xyyxyx \\ &= xy^2xyx \\ &= x1xyx \\ &= xxyx \\ &= x^2yx \\ &= 1yx \\ &= yx \end{aligned}$$

1.1.26

Trivial. Associativity and identity are inherited from G. Closure and inverses are given in the definition.

1.1.27

Let $H = \{x^n | n \in \mathbb{Z}\}$. Then $x^n x^m = x^{n+m} \in H$, satisfying closure. And given $x^n \in H$, x^{-n} is also clearly in H.

1.1.28

(a)

$$\begin{aligned} (a,b)((c,d),(e,f)) &= (a,b)(ce,df) \\ &= (a(ce),b(df)) \\ &= ((ac)e,(bd)f) \\ &= (ac,bd)(e,f) \\ &= ((a,b),(c,d))(e,f) \end{aligned}$$

(b) Le $(a,b)(1,1) = (a \cdot 1, b \cdot 1) = (a,b) = (1 \cdot a, 1 \cdot b) = (1,1)(a,b)$

(c) Le $(a,b)(a^{-1},b^{-1}) = (aa^{-1},bb^{-1}) = (1,1) = (a^{-1}a,b^{-1}b) = (a^{-1},b^{-1})(a,b)$

1.1.29

- $\implies$:
  Suppose A, B are abelian. Then given $(a,b),(c,d) \in A \times B$, we have $(a,b)(c,d) = (ac,bd) = (ca,db) = (c,d)(a,b)$. Hence $A \times B$ is abelian.

- $\impliedby$:
  Suppose $A \times B$ is abelian. Then given $a, c \in A$,

$$\begin{aligned} (a,1)(c,1) &= (c,1)(a,1) \\ \implies (ac,1) &= (ca,1) \\ \implies ac &= ca \end{aligned}$$

  Hence, A is abelian. An analagous proof shows that B is also abelian.

1.1.30

$(a, 1)(1, b) = (a1, 1b) = (a, b) = (1a, b1) = (1, b)(a, 1)$.
Then

$$\begin{aligned} & (a,b)^n = (1,1) \\ \iff & ((a,1)(1,b))^n = (1,1) \\ \iff & ((a,1)^n(1,b^n) = (1,1) && \text{(Since they commute)} \\ \iff & (a^n,1)(1,b^n) = (1,1) \\ \iff & (a^n,b^n) = (1,1) \\ \iff & a^n = 1, b^n = 1 \end{aligned}$$

Suppose n satisfies both these equations. Then n must be a multiple of both $|a|$ and $|b|$, by Corollary 1.1.1. But n is an order, so it in fact must be the LEAST common multiple of $|a|$ and $|b|$.

1.1.31

$g \in t(G) \implies g^{-1} \in t(G)$, where these elements are distinct. Hence, the elements of $t(G)$ appear in pairs, and $|t(G)|$ is even.
Suppose $x \in G - t(G)$. Then $x = x^{-1} \implies x^2 = 1$. So $|x| \leq 2$. But $|x| = 1 \implies x = 1$, so if $x \neq 1$ and $x \in G - t(G)$, then $|x| = 2$. But since $|t(G)|$ is even and $1 \in G - t(G)$, then $G - t(G)$ must have at least one other element for $|G|$ to be even, and this element has order 2.

1.1.32

This is Corollary 1.1.2

1.1.33

Assume $i > 0$ wlg. Note

$$x^i = x^{-i} \tag{15}$$

$$\implies x^{2i} = 1 \tag{16}$$

Since the order of x is n, we must have by Corollary 1.1.1 that $2i$ is a multiple of n. There is some positive d such that

$$nd = 2i$$

(a) If $d = 1$, then n is not odd, a contradiction. If $d \geq 2$, then

$$\begin{aligned} 2i &= nd \\ &\geq 2n \\ \implies i &\geq n \end{aligned}$$

contradicting the assumption that $i = 1, 2, \ldots, n-1$. Hence, (15) is impossible.

(b) Let $n = 2k$. Then

$$\begin{aligned} & nd = 2i \\ \implies & 2kd = 2i \\ \implies & i = kd \end{aligned}$$

- Case: $d = 2l + 1$ is odd. Then
$$\begin{aligned} nd &= 2i \\ \implies nd - n &= 2i - n \\ \implies n(d-1) &= 2i - 2k \\ \implies n(2l+1-1) &= 2(i-k) \\ \implies 2nl &= 2(i-k) \\ \implies nl &= i - k \\ \implies i \equiv k \pmod{n} \end{aligned}$$

- Case: $d = 2l$ is even. Then
$$\begin{aligned} nd &= 2i \\ \implies n2l &= 2i \\ \implies nl &= i \\ \implies i \equiv 0 \pmod{n} \end{aligned}$$

Hence, this exercise is WRONG, because we can't have $k = 0$. For a trivial counterexample, take $i = n$ (or any multiple of n). Then the exercise would tell us that $n \equiv k \pmod{n}$. But $n = 2k$, so $0 < k < n$, so this is ridiculous.

1.1.34

Let $n, m \in \mathbb{Z}$, with $n \neq m$. Then
$$\begin{aligned} x^n &= x^m \\ \implies x^{n-m} &= 1 \end{aligned}$$

- Case: $n - m > 0$
Then $|x| \leq n - m < \infty$, a contradiction
- Case: $n - m < 0$
Then $(x^{n-m})^{-1} = 1 \implies x^{m-n} = 1$, and $|x| \leq m - n \leq \infty$, a contradiction.

1.1.35

This is Corollary 1.1.2.

1.1.36

We cannot have $|x| = 1$ for $x \neq 1$. So let's consider the case $|a| = 3$. We can't have $a^2 = 1$, since this contradicts that. We can't have $a^2 = a$, or else cancellation gives $a = 1$. So assume wlg $a^2 = b$. Then $b^2 = a^2a^2 = a^3a = a$. So $|b| \neq 2$, i.e. $|b| = 3$. If $b^2 = a$. Then $a^2 = b \implies a^3 = ab \implies 1 = ab$, and right multiplication instead gives $1 = ba$. I.e. $b = a^{-1}$. Then
$$\begin{aligned} c &= 1 \cdot c \\ &= abc \\ \implies ac &= a^2bc \\ \implies ac &= bbc \\ \implies ac &= b^2c \\ \implies a &= ac \\ \implies c &= 1 \end{aligned}$$

But this reduces the order of the group. So this is a contradiction, and we cannot have $|a| = 3$. Setting $|b| = 3$, $|c| = 3$ of course also yields contradicions
In which case, we must have $|a| = 2$, so $a^2 = 1$. We can't have $ab = a$ or $ab = b$, else we'd get $b = 1$ or $a = 1$. We can't have $ab = 1$ or $ba = 1$, else we'd get $b = a^{-1}$. But $a^2 = 1 \implies a^{-1} = a \implies b = a$, reducing the order of the group. So we must have $ab = c$ and $ba = c$. Similarly, we are forced to set $|b| = 2, |c| = 2$, which forces $bc = cb = a$ and $ca = ac = b$, respectively.