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:

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

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

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

1.1.4

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

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

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

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

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

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 SHIIIIIIIIIIIIIIIIIIIIT

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

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 division algorithm. We can write $m = dn + r$ where r satisfies the inequalities and congruence above. Then

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

□

From this we immediately obtain two corollaries:

Corollary 1.1.1. *$x^m = 1 \implies m$ 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

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

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.

1.2 Dihedral Groups

1.2.1

Note that for any k,

$$\begin{aligned}(sr^k)^2 &= sr^k sr^k \\ &= ssr^{-k}r^k \\ &= s^2 \\ &= 1\end{aligned}$$

So $|sr^k| = 2$. On the other hand, the elements r^k form a cyclic subgroup of order n which can be identified with the group $\mathbb{Z}/n\mathbb{Z}$. Hence, to compute the order of each of the elements, we follow the same method as in exercises 1.1.11, 1.1.13. Hence...

(a) $n = 3$

$$\begin{aligned}|1| &= 1 \\ |r| &= 3 \\ |r^2| &= 3 \\ |sr^k| &= 2\end{aligned}$$

(b) $n = 4$

$$\begin{aligned}|1| &= 1 \\ |r| &= 4 \\ |r^2| &= 2 \\ |r^3| &= 4 \\ |sr^k| &= 2\end{aligned}$$

(c) $n = 5$

$$\begin{aligned}|1| &= 1 \\ |r| &= 5 \\ |r^2| &= 5 \\ |r^3| &= 5 \\ |r^4| &= 5 \\ |sr^k| &= 2\end{aligned}$$

1.2.2

$x = sr^k$. So $rx = rsr^k = sr^{-1}r^k = sr^{k-1} = sr^k r^{-1} = xr^{-1}$

1.2.3

$|sr^k| = 2$ was shown in 1.2.1. And note that
$r^k = 1r^k = 1^k r^k = (1r)^k = (s^2 r)^k = (s(sr))^k$,
and $sr^k = s(s(sr))^k$

1.2.4

Using the method of 1.1.11 again, $\text{lcm}(k, 2k) = 2k$, so $|z| = |r^k| = \frac{2k}{k} = 2$. z obviously commutes with the r^i. And

$$\begin{aligned} z(sr^i) &= r^k sr^i \\ &= sr^{-k}r^i \\ &= (sr^i)r^{-k} \\ &= (sr^i)r^{n-k} \\ &= (sr^i)r^{2k-k} \\ &= (sr^i)r^k \\ &= (sr^i)z \end{aligned}$$

Note:

$$\begin{aligned} (sr^i)(sr^j) &= sr^i sr^j \\ &= ssr^{-i}r^j \\ &= s^2 r^{j-i} \\ &= r^{j-i} \end{aligned}$$

Whereas $(sr^j)(sr^i) = r^{i-j} = r^{-(j-i)}$, which according to (b) is equal to r^{i-j} iff $i - j = k$, which is not the case for arbitrary i, j. Hence, the elements sr^i do not commute in general.
On the other hand, the r^i commute with each other. And

$$\begin{aligned} (r^i)(sr^j) &= r^i sr^j \\ &= sr^{-i}r^j \\ &= sr^{j-i} \end{aligned}$$

Whereas $(sr^j)r^i = sr^{j+i}$. And

$$\begin{aligned} sr^{j+i} &= sr^{j-i} \\ \implies r^{j+i} &= r^{j-i} \end{aligned}$$

In particular, the above equality has to apply to $j = n$. The only possible setting of $0 \leq i < n$ that fulfills this (other than $i = 0$, which gives the identity) is $i = k$

1.2.5

Follow the previous exercise and note that we can't set $i = n/2$

1.2.6

Note: $t(yx) = (xy)(yx) = x(yy)x = xx = 1$, so $t^{-1} = yx$,
and $tx = xyx = xt^{-1}$.

1.2.7

- The old relations come from the new. Note that $b^{-1} = r^{-1}s^{-1}$, and $b^2 = 1 \implies b = b^{-1}$. So we have
  $s^2 = a^2 = 1$
  $rs = 1rs = s^2rs = ssrs = aba = ab^{-1}a = sr^{-1}s^{-1}s = sr^{-1}$
  $r^n = (1r)^n = (s^2r)^n = (s(sr))^n = (ab)^n = 1$
- The new relations come from the old. We have
  $a^2 = s^2 = 1$
  $b^2 = (sr)^2 = srsr = ssr^{-1}r = 1 \cdot 1 = 1$
  $(ab)^n = (s(sr))^n = (s^2r)^n = (1r)^n = r^n = 1$

1.2.8

n. lol

1.2.9

For these next 5 exercises, we note that the order is the amount of rotations a face can undergo, times the number of faces the face can be sent to. I.e. the formula is

$$\text{Num vertices on a face} \times \text{Num faces}$$

So for a tetrahedron, it's $3 \cdot 4 = 12$

1.2.10

$4 \cdot 6 = 24$

1.2.11

$3 \cdot 8 = 24$

1.2.12

$5 \cdot 12 = 60$

1.2.13

$3 \cdot 20 = 60$

1.2.14

$\mathbb{Z} =< 1 >$

1.2.15

$\mathbb{Z}/n\mathbb{Z} =< \overline{1} | \overline{n} = \overline{1} >$

1.2.16

$x_1^2 = y_1^2 = 1$ directly corresponds to $r^n = s^2 = 1$. And

$$\begin{aligned} & (x_1 y_1)^2 = 1 \\ \iff & x_1 y_1 x_1 y_1 = 1 \\ \iff & x_1 y_1 = {y_1}^{-1} {x_1}^{-1} \\ \iff & x_1 y_1 = y_1 {x_1}^{-1} \end{aligned}$$

1.2.17

$X_{2n} =< x, y | x^n = y^2 = 1, xy = yx^2 >$ Recall from the text that $x^3 = 1$

(a) $x^3 = 1 \implies x^2 x = 1 \implies x^{-1} = x^2$. So $xy = yx^2 \iff xy = yx^{-1}$ corresponds to $rs = sr^{-1}$. Also, $x^n = y^2 = 1$ corresponds to $r^n = s^2 = 1$, and thus in this case $X_{2n} = D_6$, so the order of course is 6.

(b) Use 1.1.2 and note that both 3 and n have to share a divisor which is the order of x. But $(3, n) = 1$ implies the order is 1.

1.2.18

$Y =< u, v | u^4 = v^3 = 1, uv = v^2u^2 >$

(a) $v^3 = 1 \implies v^{-1} = v^2$

(b)

$$\begin{aligned} v^2u^3v &= (v^2u^2)(uv) \\ &= (uv)(v^2u^2) \\ &= uv^3u^2 \\ &= u1u^2 \\ &= u^3 \end{aligned}$$

So

$$\begin{aligned} & v^2u^3v = u^3 \\ \implies & v^{-1}u^3v = u^3 \\ \implies & u^3v = vu^3 \end{aligned}$$

(c) $u^9 = u^4u^4u = 1 \cdot 1 \cdot u = u.$
$vu = vu^9 = u^9v = u^8uv = 1uv = uv$

(d)

$$\begin{aligned} & uv = v^2u^2 \\ \implies & uv = (uv)^2 && \text{Commutativity of } u, v \\ \implies & 1 = uv \end{aligned}$$

(e)

$$\begin{aligned} & u^4v^3 = 1 \\ \implies & uu^3v^3 = 1 \\ \implies & u(uv)^3 = 1 && \text{Commutativity} \\ \implies & u1 = 1 \\ \implies & u = 1 \end{aligned}$$

And thus also $uv = 1 \implies v = 1$

1.3 Symmetric Groups

In these exercises, I will use exercises 10, 13-15 throughout without explicit reference

1.3.1

- $\sigma = (1\ 3\ 5)(2\ 4)$
- $\tau = (1\ 5)(2\ 3)$
- $\sigma^2 = (1\ 5\ 3)$
- $\sigma\tau = (2\ 5\ 3\ 4)$
- $\tau\sigma = (1\ 2\ 4\ 3)$
- $\tau^2\sigma = \mathbf{1}\sigma = \sigma$

1.3.2

No thanks

1.3.3

Only doing it for exercise 1, using exercise 1.3.15.

- $|\sigma| = 6$
- $|\tau| = 2$
- $|\sigma^2| = 3$
- $|\sigma\tau| = 4$
- $|\tau\sigma| = 4$
- $|\tau^2\sigma| = 6$

1.3.4

(a) $S_3 = \{\mathbf{1}, (1\ 2), (2\ 3), (1\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$
The orders are, respectively, $1, 2, 2, 2, 3, 3$

(b) $S_4 = \{\mathbf{1}, (1\ 2), (2\ 3), (1\ 3), (1\ 4), (2\ 4), (3\ 4),$
$(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3),$
$(1\ 2\ 3), (1\ 3\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3), (1\ 2\ 4), (1\ 4\ 2),$
$(1\ 2\ 3\ 4), (1\ 3\ 2\ 4), (1\ 4\ 2\ 3), (1\ 2\ 4\ 3), (1\ 3\ 4\ 2), (1\ 4\ 3\ 2)\}$
The order of 1 is 1, the order of the elements with 2-cycles are 2, the order of the 3 and 4 cycles are 3 and 4 respectively.

1.3.5

Using 1.3.15, $|\sigma| = \text{lcm}(2, 3, 5) = 30$

1.3.6

Done in 1.3.4

1.3.7

Done in 1.3.4

1.3.8

$\infty! = \infty$ jk. Consider the permutation σ that shifts each element to the right by one: $1 \mapsto 2, 2 \mapsto 3$, etc. Then σ^n is distinct for all $n \geq 0$

1.3.9

We use 1.3.11.

(a) $1, 5, 7, 11$

(b) $1, 3, 5, 7$

(c) $1, 3, 5, 9, 11, 13$

1.3.10

Of course, $\sigma^0(a_k) = \mathbf{1}(a_k) = a_k = a_{k+0}$
Now suppose $\sigma^i(a_k) = a_{k+i}$.
Then $\sigma^{i+1}(a_k) = \sigma\sigma^i a_k = \sigma(a_{k+i}) = a_{k+i+1}$, where we implicitly replace the subscripts with their residues.
Hence, $\sigma^i(a_k) = a_{k+i}$ holds in general.
For $1 \leq i < m$,
$\sigma^i(a_k) = a_{k+i} \neq a_k = \mathbf{1}(a_k)$, so $\sigma^i \neq \mathbf{1}$.
But $\sigma^m(a_k) = a_{k+m} = a_k = \mathbf{1}(a_k)$, hence $\sigma^m = \mathbf{1}$ and $|\sigma| = m$

1.3.11

For convenience, relabel the elements $0, \ldots, m-1$, so

$$\sigma = (0\ 1\ 2\ \ldots\ m-1)$$

and by the previous exercise 1.3.10,

$$\sigma^i(n) = n + i \pmod{m}$$

Then

$$\begin{aligned}
& \sigma^i \text{an } m\text{-cycle} && (17)\\
\iff & m = \operatorname*{argmin}_k (\sigma^i)^k(0) = 0 && (18)\\
\iff & m = \operatorname*{argmin}_k \sigma^{ik}(0) = 0 && (19)\\
\iff & m = \operatorname*{argmin}_k 0 + ik \mod m = 0 && (20)\\
\iff & m = \operatorname*{argmin}_k 0 + ik = 0 \pmod{m} && (21)\\
\iff & m = \operatorname*{argmin}_k m|ik && (22)\\
\iff & m = \operatorname{lcm}(i,m)/i && (23)\\
\iff & mi = \operatorname{lcm}(i,m) && (24)\\
\iff & \gcd(i,m) = 1 && (25)
\end{aligned}$$

1.3.12

(a) Set $\sigma = (1\ 3\ 5\ 7\ 9\ 2\ 4\ 6\ 8\ 10)$.
Using 1.3.10, I placed each elem 5 spaces away.

(b) idk

1.3.13

The "if" is obvious, so we handle the "only if"
Consider $\sigma \in S_n$ with order 2.
given $s \in \{1, \ldots, n\}$.

- Case: $\sigma(s) = s$
  Then s is in a 1-cycle in σ
- Case: $\sigma(s) = t (t \neq s)$
  Then since $|\sigma| = 2$,

$$\begin{aligned}
& \sigma^2(s) = s\\
\implies & \sigma(\sigma(s)) = s\\
\implies & \sigma(t) = s
\end{aligned}$$

  So $(s\ t)$ makes a 2-cycle in σ

Hence, σ has only 1 and 2-cycles

1.3.14

The "if" is again obvious, so we handle the "only if"
Consider $\sigma \in S_n$ with order $p > 2$.
given $s \in \{1, \ldots, n\}$.

- Case: $\sigma(s) = s$
  Then s is in a 1-cycle in σ
- Case: $\sigma(s) = t (t \neq s)$
  Then we know at least that $\sigma^p(s) = s$.
  Suppose s is in an m-cycle with $1 < m < p$.
  Then $\sigma^m(s) = s$.
  Let $p = mq + r$ by Euclidean division. Note $0 < r < m$ (if $r = 0$, then $m|p$, contradicting primeness of p). Then

$$\begin{aligned} s &= \sigma^p(s) \\ &= \sigma^{mq+r}(s) \\ &= \sigma^r \sigma^{mq}(s) \\ &= \sigma^r (\sigma^m)^q(s) \\ &= \sigma^r (\mathbf{1})^q(s) \\ &= \sigma^r \mathbf{1}(s) \\ &= \sigma^r(s) \\ \implies \sigma^r(s) &= s \end{aligned}$$

  So s is actually in an r-cycle, a contradiction.

A counterexample is any product of cycles of different length

1.3.15

Exercise 1.3.10 immediately implies that a m-cycle has an order of m, while a combination of Corollary 1.1.1 and exercise 1.1.24 show that it's the lcm when we have a product of cycles

1.3.16

"Count the number of ways of forming an m-cycle and divide by the number of representations of a particular m-cycle" is the solution lol.

1.3.17

Analgous to above, we count the number of ways of ordering 4 elements, then divide by 2 since we don't care about the order of the cycles, then divide by 2 again since we don't care about the order of the elements in the first cycle, then 2 again for the second cycle.

1.3.18

How many ways are there to add up to 5?

- $\text{lcm}(1, 1, 1, 1, 1) = 1$
- $\text{lcm}(2, 1, 1, 1) = 2$
- $\text{lcm}(2, 2, 1) = 2$
- $\text{lcm}(2, 3) = 6$
- $\text{lcm}(3, 1, 1) = 3$
- $\text{lcm}(4, 1) = 4$
- $\text{lcm}(5) = 5$

1.3.19

How many ways are there to add up to 7?

- $\text{lcm}(1,1,1,1,1,1,1) = 1$
- $\text{lcm}(2,1,1,1,1,1) = 2$
- $\text{lcm}(2,2,1,1,1) = 2$
- $\text{lcm}(2,2,2,1) = 2$
- $\text{lcm}(3,2,2) = 6$
- $\text{lcm}(3,1,1,1,1) = 3$
- $\text{lcm}(3,2,1,1) = 6$
- $\text{lcm}(4,2,1) = 4$
- $\text{lcm}(4,1,1,1) = 4$
- $\text{lcm}(4,3) = 12$
- $\text{lcm}(5,1,1) = 5$
- $\text{lcm}(5,2) = 10$
- $\text{lcm}(6,1) = 6$
- $\text{lcm}(7) = 7$

1.3.20

$S_3 =< (1\ 2\ 3), (1\ 2) >$.
Verify:
$(1\ 2\ 3)^2 = (1\ 3\ 2)$
$(1\ 2\ 3)(1\ 3\ 2) = \mathbf{1}$
$(1\ 2\ 3)(1\ 2) = (1\ 3)$
$(1\ 2\ 3)(1\ 3) = (2\ 3)$

1.4

1.4.1

$|F_2| = |\mathbb{Z}/2\mathbb{Z}| = 2$, so
$|GL_2(F_2)| = (2^2 - 2^0)(2^1 - 2^1) = 3 \cdot 2 = 6$

1.4.2

Denote:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
$$B = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$
$$C = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$
$$D = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$
$$E = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Manual computation yields

$$|I| = 1$$
$$|A| = 2$$
$$|B| = 3$$
$$|C| = 3$$
$$|D| = 2$$
$$|E| = 3$$

1.4.3

$CD = E$, but $DC = A$

1.4.4

If n is not prime, decompose $n = ab$ with $1 < a, b < n$.
In $\mathbb{Z}/n\mathbb{Z}$, $ab = 0$, so $\mathbb{Z}/n\mathbb{Z} - \{0\}$ is not a group under multiplication (because it fails closure)

1.4.5

For the "only if", suppose $GL_n(F)$ is finite. Let D be the subgroup of $GL_n(F)$ of diagonal matrices where each entry of the diagonal is the same. Then we can identify F with D. So $GL_n(F)$ finite means that D is finte, and hence so is F.
For the "if", the following exercise provides an upper bound

1.4.6

For each entry of a matrix, we have at most q choices, and there are n^2 entries, so in total we have $\prod_{i=1}^{n^2} q = q^{n^2}$ choices.

1.4.7

idk

1.4.8

Let A be an upper triangular matrix of 1s. And let B be a lower triangular matrix of 1s. Then
$(AB)_{1,1} = \sum_{i=1}^{n} A_{i,1}B1, i = \sum_{i=1}^{n} 1 = n$
$(BA)_{1,1} = \sum_{i=1}^{n} A_{1,i}Bi, 1 = A_{1,1}B_{1,1} + \sum_{i=2}^{n} 0 = 1$
So $AB \neq BA$

1.4.9

No shit. Waste of time.

1.4.10

Denote

$$A = \begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}$$
$$B = \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix}$$

(a)

$$AB = \begin{pmatrix} a_1a_2 & a_1b_2 + b_1c_2 \\ 0 & c_1c_2 \end{pmatrix}$$

(b) If $B = A^{-1}$, we must set

$$\begin{aligned} a_2 &= \frac{1}{a_1} \\ c_2 &= \frac{1}{c_2} \\ a_1 b_2 + b_1 c_2 &= 0 \\ \implies b_2 &= \frac{-b_1 c_2}{a_1} \end{aligned}$$

All of which is doable in $\mathbb{R}$

(c) Immediate

(d) In (a), $c_1 = a_1$, and $c_2 = a_2$, so

$$AB = \begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 c_2 \\ 0 & a_1 a_2 \end{pmatrix}$$

And using (b), the inverse is

$$A^{-1} = \begin{pmatrix} \frac{1}{a_1} & \frac{-b_1 a_2}{a_1} \\ 0 & \frac{1}{a_1} \end{pmatrix}$$

which is clearly also in the group

1.4.11

(a)

$$XY = \begin{pmatrix} 1 & a+d & e+af+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix}$$
$$YX = \begin{pmatrix} 1 & a+d & e+cd+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix}$$

So all the entries in XY and YX are the same except the top-right entry. Setting $a, f = 1$, and $c, d = 2$ immediately yields equality

(b) If $Y = X^{-1}$, we must have

$$\begin{aligned} a + d &= 0 \\ e + af + b &= 0 \\ f + c &= 0 \end{aligned}$$

which yield

$$\begin{aligned} d &= -a \\ e &= ca - b \\ f &= -c \end{aligned}$$

(c) I'M ASSUMIN MATRIX MULT IS ASSOCIATIVE. It's $|F|^3$ because we have $|F|$ choices for each entry a, b, c

(d)

(e) It's easy to see that the top middle element of X^n is na. And $na \neq 0$ for any $a \in \mathbb{R}$ and $n \in \mathbb{Z}^+$

1.5

1.5.1

$|1| = 1, |-1| = 2$ of course. The orders of the rest are 4.

1.5.2

no

1.5.3

idk

1.6

1.6.1

(a) $\phi(x^1) = \phi(x) = \phi(x)^1$ is the base case. Now supposing things hold for $k = 1, \ldots, n$, note that

$$\begin{aligned} \phi(x^{n+1}) &= \phi(x^n x) \\ &= \phi(x^n)\phi(x) && \text{(homomorphism)} \\ &= \phi(x)^n \phi(x) && \text{(induction)} \\ &= \phi(x)^{n+1} \end{aligned}$$

(b) We will prove that homomorphisms preserve identity (and use this fact for granted moving forward):

$$\begin{aligned} \phi(x)\phi(1) &= \phi(x \cdot 1) \\ &= \phi(x) \\ \implies \phi(1) &= 1 && \text{(cancellation property)} \end{aligned}$$

Note that this also proves the case $n = 0$.
Hence we have $\phi(x^{-1})\phi(x) = \phi(x^{-1}x) = \phi(1) = 1$
So $\phi(x^{-1})$ is the inverse of $\phi(x)$, i.e.
$\phi(x^{-1}) = \phi(x)^{-1}$.
Now suppose

$$\phi(x^{-k}) = \phi(x)^{-k}$$

for $k = 1, \ldots, n$ (note we've shown the base case).
Then

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

1.6.2

Let $|x| = n$. Then
$\phi(x)^n = \phi(x^n) = \phi(1) = 1$
So $|\phi(x)| \leq n$.
Suppose $\phi(x)^k = 1$ for $k \leq n$.
Then

$$\begin{aligned} \phi(x^k) &= 1 \\ \implies x^k &= 1 \end{aligned}$$

The second equality follows from injectivity of the isomorphism ϕ. Since $k \leq n = |x|$, we have $k = n$. Hence, $|\phi(x)| = n$ as needed.
ϕ and ϕ^{-1} glue together elements from G and H in pairs of the same order. It doesn't work for general homomorphisms. See Example 1 from the text, with $k < n$, and compare the orders of r and its image r_1

1.6.3

For the "only if", suppose G is abelian. Then let $y, z \in H$, with $\phi(a) = y, \phi(b) = z$ (such a, b existsince ϕ is surjective).
Then $yz = \phi(a)\phi(b) = \phi(b)\phi(a) = zy$,
so H is abelian.
For the "if", repeat the above with ϕ^{-1}
In the case that ϕ is a general homomorphism, note that in the proof of the "only if", we only used surjectivity.

1.6.4

i has order 4 in $\mathbb{C} - \{0\}$, but the only finite order elements in $\mathbb{R} - \{0\}$ are $|1| = 1, |-1| = 2$

1.6.5

Cantor's diagonalization argument

1.6.6

$\mathbb{Z}$ is generated by a single element 1, but no single element can generate $\mathbb{Q}$.

1.6.7

Q_8 has a single elem of order 2, which is -1,
but in D_{2n}, both s and r^2 have order 2

1.6.8

$$\begin{aligned} & S_n \equiv S_m \\ \implies & |S_n| = |S_m| \\ \implies & n! = m! \\ \implies & n = m \end{aligned}$$

Take the contrapositive

1.6.9

In D_{24}, $|r| = 12$. But looking back at 1.3.4, we see no elements of order 12 in S_4.

1.6.10

(a) A composition of bijections is a bijection

(b) Define $\psi : S_\Omega \to S_{Delta}$ by
$\delta \mapsto \theta^{-1} \circ \delta \circ \theta$.
So then

$$\begin{aligned} \psi(\phi(\sigma)) &= \psi(\theta \circ \sigma \circ \theta^{-1}) \\ &= \theta^{-1} \circ \theta \circ \sigma \circ \theta^{-1} \circ \theta \\ &= \sigma \end{aligned}$$

and analagously

$$\begin{aligned} \phi(\psi(\delta)) &= \psi(\theta^{-1} \circ \delta \circ \theta) \\ &= \theta \circ \theta^{-1} \circ \delta \circ \theta \circ \theta^{-1} \\ &= \delta \end{aligned}$$

So ψ is a 2 sided inverse for ϕ, and hence ϕ is a bijection i.e. an isomorphism

(c)

$$\begin{aligned}\phi(\sigma \circ \tau) &= \theta \circ \sigma \circ \tau \circ \theta^{-1} \\ &= \theta \circ \sigma \circ \mathbf{1} \circ \tau \circ \theta^{-1} \\ &= \theta \circ \sigma \circ \theta^{-1} \circ \theta \circ \tau \circ \theta^{-1} \\ &= \phi(\sigma) \circ \phi(\tau)\end{aligned}$$

1.6.11

Define

$$\begin{aligned}\phi : A \times B &\to B \times A \\ (a, b) &\mapsto (b, a)\end{aligned}$$

So

$$\begin{aligned}\phi((a, b)(c, d)) &= \phi(ac, bd) \\ &= (bd, ac) \\ &= (b, a)(d, c) \\ &= \phi(a, b)\phi(c, d)\end{aligned}$$

So ϕ is a homomorphism. And it is clearly a bijection with inverse $(b, a) \mapsto (a, b)$

1.6.12

waste of time

1.6.13

Let $y, z \in \phi(G)$. Then we must have $\phi(a) = y, \phi(b) = z$ for some $a, b \in G$.
And

$$\begin{aligned}yz &= \phi(a)\phi(b) \\ &= \phi(ab) \\ &\in \phi(G)\end{aligned}$$

So closure is satisfied.
Now, given $y \in \phi(G)$, we have $y = \phi(a)$ for some $a \in G$. Now let $z = \phi(a^{-1})$, so $z \in \phi(G)$. Then from 1.6.1, we have in fact that $z = \phi(a)^{-1}$, i.e. $z = y^{-1}$. So inverses are in $\phi(G)$