Part I - Group Theory

January 7, 2026

Contents

1 Introduction to Groups

1.1

1.1.1

(a) No. $(5-4)-1 = 1-1 = 0$ but $5-(4-1) = 5-3 = 2$

(b) Yes.

$$\begin{aligned}
(a \star b) \star c &= (a+b+ab) \star c \\
&= a+b+ab+c+(a+b+ab)c \\
&= a+b+ab+c+ac+bc+abc && \text{Distributive property of } \mathbb{R} \\
&= a+b+c+bc+ab+ac+abc && \text{Commutativity of } + \text{ in } \mathbb{R} \\
&= a+b+c+bc+a(b+c+bc) \\
&= a \star (b+c+bc) \\
&= a \star (b \star c)
\end{aligned}$$

(c) No. $(1 \star 2) \star 3 = \frac{1+2}{5} \star 3 = \frac{3}{5} \star 3 = \frac{\frac{3}{5}+3}{5} = \frac{18}{5}$. But $1 \star (2 \star 3) = 1 \star \frac{2+3}{5} = 1 \star 1 = \frac{1+1}{5} = \frac{2}{5}$.

(d) Yes.

$$\begin{aligned}[(a,b)\star(c,d)]\star(e,f) &= (ad+bc,bd)\star(e,f)\\ &= ((ad+bc)f+(bd)e,(bd)f)\\ &= (adf+bcf+bde,bdf)\\ &= (a(df)+b(cf+de),b(df))\\ &= (a,b)\star(cf+de,df)\\ &= (a,b)\star[(c,d)\star(e,f)]\end{aligned}$$

(e) No. $(1\star 2)\star 3 = \frac{1}{2}\star 3 = \frac{\frac{1}{2}}{3} = \frac{1}{6}$. But $1\star(2\star 3) = 1\star\frac{2}{3} = \frac{1}{\frac{2}{3}} = \frac{3}{2}$

1.1.3

$$\begin{aligned}(\overline{a}+\overline{b})+\overline{c} &= (\overline{a+b})+\overline{c}\\ &= \overline{(a+b)+c}\\ &= \overline{a+(b+c)} && \text{associativity of } + \text{ in } \mathbb{Z}\\ &= \overline{a}+\overline{b+c}\\ &= \overline{a}+(\overline{b}+\overline{c})\end{aligned}$$

1.1.4

$$\begin{aligned}(\overline{a}\cdot\overline{b})\cdot\overline{c} &= (\overline{a\cdot b})\cdot\overline{c}\\ &= \overline{(a\cdot b)\cdot c}\\ &= \overline{a\cdot(b\cdot c)} && \text{associativity of } \cdot \text{ in } \mathbb{Z}\\ &= \overline{a}\cdot\overline{b\cdot c}\\ &= \overline{a}\cdot(\overline{b}\cdot\overline{c})\end{aligned}$$

1.1.5

$\overline{0}$ has no multiplicative inverse

1.1.9

(a)
- $(a+b\sqrt{2})+(c+d\sqrt{2}) = a+b\sqrt{2}+c+d\sqrt{2} = a+c+b\sqrt{2}+d\sqrt{2} = (a+b)+(b+d)\sqrt{2} \in G$, so the operation is closed under addition.
- Associativity follows directly from associativity in $\mathbb{R}$
- $0 = 0+\sqrt{2}$ is clearly an identity
- $-a+(-b)\sqrt{2}$

(b) To help us, we prove the following lemma

Lemma 1. *Given $a,b\in\mathbb{Q}$, $a+b\sqrt{2}\neq 0 \iff a\neq 0$ or $b\neq 0$*

Proof. For $\implies$, if we had both $a,b=0$, then we'd have $a+b\sqrt{2} = 0+0\sqrt{2} = 0$. For $\impliedby$, assume without generality that $a\neq 0$. Then $a+b\sqrt{2}=0$ would mean that $a=-b\sqrt{2}$. However, since b is rational, $-b\sqrt{2}$ is irrational. But a is rational, so they can't be equal. □

- Let $a, b \in \mathbb{Q}$ not both be zero and $c, d \in \mathbb{Q}$ not both be zero. Then $(a + b\sqrt{2})(c + d\sqrt{2}) = ac + bc\sqrt{2} + ad\sqrt{2} + 2bd = (ac + 2bd) + (ad + bc)\sqrt{2}$. The result is nonzero thanks to the zero product property in $\mathbb{R}$. Hence, the operation is closed under multiplication
- Associativity follows directly from associativity of multiplication in $\mathbb{R}$
- The identity is clearly $1 = 1 + 0\sqrt{2}$
- To find an inverse, we note that the inverse of $a + b\sqrt{2}$ in $\mathbb{R}$ is $\frac{1}{a+b\sqrt{2}}$ (note, we have $a + b\sqrt{2} \neq 0$). Now we "rationalize.":

$$
\begin{aligned}
&= \frac{1}{a + b\sqrt{2}} \\
&= \frac{1}{a + b\sqrt{2}}\left(\frac{a - b\sqrt{2}}{a - b\sqrt{2}}\right) && \text{Possible by lemma 1} \\
&= \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} \\
&= \frac{a - b\sqrt{2}}{a^2 - 2b^2} \\
&= \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}
\end{aligned}
$$

1.1.15

Clearly this holds for $n = 1$. Now suppose $(a_1 \cdots a_{n-1})^{-1} = {a_{n-1}}^{-1} \cdots {a_1}^{-1}$. Then

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

1.1.16

- First suppose that $x^2 = 1$
  - Case: $x = 1$. Then $x^1 = 1$. Hence $|x| = 1$
  - Case: $x \neq 1$. Then $x^1 \neq 1$. But $x^2 = 1$. Hence $|x| = 2$
- Now suppose $|x| = 1$ or 2
  - Case: $|x| = 1$. Then $x^1 = 1 \implies x = 1$, and $x^2 = 1^1 = 1$
  - Case: $|x| = 2$. Then $x^2 = 1$ by definition

1.1.17

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

Hence $x^{n-1} = x^{-1}$

1.1.19

(a)

$$\begin{aligned} x^a x^b &= (\underbrace{x \cdots x}_{a \text{ times}})(\underbrace{x \cdots x}_{b \text{ times}}) \\ &= \underbrace{x \cdots x}_{a+b \text{ times}} \\ &= x^{a+b} \end{aligned}$$

And

$$\begin{aligned} (x^a)^b &= \underbrace{x^a \cdots x^a}_{b \text{ times}} \\ &= \underbrace{\underbrace{x}_{a \text{ times}} \cdots \underbrace{x}_{a \text{ times}}}_{b \text{ times}} \\ &= \underbrace{x \cdots x}_{a \cdot b \text{ times}} \\ &= x^{ab} \end{aligned}$$

(b) Clearly works for $a = 1$. Now suppose that $(x^{a-1})^{-1} = x^{-(a-1)}$. Then

$$\begin{aligned} x^{-a}x^a &= (\underbrace{x^{-1} \cdots x^{-1}}_{a \text{ times}})x^a && \text{By definition} \\ &= (x^{-1}\underbrace{x^{-1} \cdots x^{-1}}_{a-1 \text{ times}})x^{a-1}x \\ &= x^{-1}x^{-(a-1)}x^{a-1}x && \text{Definition} \\ &= x^{-1}(x^{a-1})^{-1}x^{a-1}x && \text{Inductive assumption} \\ &= x^{-1}1x \\ &= x^{-1}x \\ &= 1 \end{aligned}$$

(c) Fuck my life bro. This is more annoying that it seems.

i We first show that $x^a x^b = x^{a+b}$ for all $a, b \in \mathbb{Z}$. We go by cases.

(1) Case: $a = 0$ or $b = 0$. Assume $a = 0$ without loss of generality. Then $x^a x^b = x^0 x^b = 1x^b = x^b = x^{0+b} = x^{a+b}$.

(2) Case: Both $a, b < 0$. Then let $c = -a, d = -b$. Then

$$\begin{aligned} x^a x^b &= x^{-c}x^{-d} \\ &= (x^{-1})^c(x^{-1})^d && \text{Definition} \\ &= (x^{-1})^{c+d} && \text{By (a)} \\ &= x^{-(c+d)} && \text{Definition} \\ &= x^{-c-d} \\ &= x^{a+b} \end{aligned}$$

(3) Case: One is negative, one is positive. Assume without loss of generality that $a < 0, b > 0$. We proceed by induction on b. We can take $b = 0$ to be the base case (we've already shown it in the Case (1)) and then assume that $x^a x^{b-1} = x^{a+b-1}$. Then

$$\begin{aligned} x^a x^b &= x^a x^{b-1}x \\ &= x^{a+b-1}x \end{aligned}$$

Okay, so if $a+b-1>0$, this is just (a). If $a+b-1=0$, this is just Case (1). So we have to deal with the case $a+b-1<0$. Then

$$\begin{aligned} x^{a+b-1}x &= \underbrace{x^{-1}\cdots x^{-1}}_{-(a+b-1)\text{ times}} \\ &= \underbrace{x^{-1}\cdots x^{-1}}_{1-a-b\text{ times}}x \\ &= \underbrace{x^{-1}\cdots x^{-1}}_{1-a-b-1\text{ times}} \\ &= \underbrace{x^{-1}\cdots x^{-1}}_{-a-b\text{ times}} \\ &= \underbrace{x^{-1}\cdots x^{-1}}_{-(a+b)\text{ times}} \\ &= \underbrace{x\cdots x}_{a+b\text{ times}} \end{aligned}$$

ii Alright, now time for $(x^a)^b = x^{ab}$. We proceed by cases again

(1) Case: $a=0$. Then $(x^a)^b = (x^0)^b = 1^b = 1 = x^0 = x^{0b} = x^{ab}$

(2) Case: $b=0$. Then $(x^a)^b = (x^a)^0 = 1 = x^0 = x^{a0} = x^{ab}$

(3) Case: $a<0, b>0$. Let $c=-a$ Then

$$\begin{aligned} (x^a)^b &= (x^{-c})^b \\ &= ((x^{-1})^c)^b && \text{Definition} \\ &= (x^{-1})^{cb} && \text{By (a)} \\ &= x^{-cb} && \text{Definition} \\ &= x^{ab} \end{aligned}$$

(4) Case: $a>0, b<0$. Let $c=-b$. I REGRET DOING THIS EXERCISE. I REGRET DOING THIS EXERCISE. Then

$$\begin{aligned} (x^a)^b &= (x^a)^{-c} \\ &= ((x^a)^c)^{-1} && \text{By (b)} \\ &= ((x^{ac})^{-1} && \text{By (a)} \\ &= x^{-ac} && \text{By (b)} \\ &= x^{ab} \end{aligned}$$

(5) Case: $a, b<0$. Let $c=-a$. Then

$$\begin{aligned} (x^a)^b &= (x^{-c})^b \\ &= ((x^{-1})^c)^b && \text{Definition} \\ &= (x^{-1})^{cb} && \text{By the previous case, Case (4)} \\ &= x^{-cb} && \text{Definition} \\ &= x^{ab} \end{aligned}$$

And we're done. I regret doing this exercise.

We will use the results of this exercise without referring to it from here on.

1.1.20

- Suppose $|x| = \infty$. Then suppose $|x^{-1}| = n$ for $n \in \mathbb{Z}^+$. Then

$$\begin{aligned} (x^{-1})^{-1} &= (x^{-1})^{n-1} && \text{by 1.1.17} \\ \implies x &= x^{-n+1} \\ \implies x^{n-1}x &= x^{n-1}x^{-n+1} \\ \implies x^n &= x^{n-1-n+1} \\ &= x^0 \\ &= 1 \end{aligned}$$

  Hence $|x| \leq n$, a contradiction. So we can't have $n \in \mathbb{Z}^+$, so $n = \infty$

- Suppose $|x| = n \in \mathbb{Z}^+$. Then let $|x^{-1}| = l$. Then

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

  So $l = kn$ for some $k \in \mathbb{Z}^+$. I.e. $l \geq n$. But

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

  So $l \leq n$. So we must have $l = n$

1.1.21

Since n is odd, let $n = 2s + 1$ for $s \in \mathbb{Z}^+$ Then

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

1.1.23

Let $|x^s| = r$. Then $(x^s)^t = x^{st} = x^n = 1$, so $r \leq t$. But note that $k = r$ is the lowest positive integer for which

$$(x^s)^k = 1 \tag{1}$$

holds. However, we showed that $k = t$ also makes the equation true, so $t \geq r$. Hence $t = r$

1.1.25

Given $a, b \in G$,

$$\begin{aligned}
(ab)(ba) &= ab^2a \\
&= a1a \\
&= a^2 \\
&= 1 \\
\implies (ab)(ab)(ba) &= ab \\
\implies (ab)^2(ba) &= ab \\
\implies 1(ba) &= ab \\
\implies ba &= ab
\end{aligned}$$

1.1.26

- Closure under the operation is given by the definition
- Associativity is directly inherited from G
- Inverses exist as given by the definition
- The identity exists. Note that by definition, H is closed under the operation and inverses. We were also given that H is nonempty, so we can take some $h \in H$, and note that $h^{-1} \in H$ as well. So $hh^{-1} \in H$, i.e. $1 \in H$.

1.1.27

Let $H = \{x^n | n \in \mathbb{Z}\}$.

- H is closed under the operation. Let $x^n, x^m \in H$. then $x^n x^m = x^{n+m} \in H$.
- H is closed under inverses. Given x^n, note that $x^{-n} \in H$, which is clearly its inverse.

1.1.29

- $\impliedby$: If A, B abelian, given $(a, b), (c, d) \in A \times B$, we have $(a, b)(c, d) = (ac, bd) = (ca, db) = (c, d)(a, b)$
- $\implies$: Now assume without loss off generality that B is not abelian (e.g. space of invertible matrices), and take any $b, d \in B$ such that $bd \neq db$. Then $(a, b)(c, d) = (ac, bd)$. But $(c, d)(a, b) = (ca, db) = (ac, db)$. Note that by definition of $A \times B$, since $bd \neq db$, we have $(ac, bd) \neq (ac, db)$.

1.1.30

$(a, 1)(1, b) = (a \cdot 1, 1 \cdot b) = (1 \cdot a, b \cdot 1) = (1, b)(a, 1)$, so these elements commute. Note let $A = |a|, B = |b|, l = |(a, b)|$. Note that

$$\begin{aligned}
1 &= (a, b)^l \\
&= [(a, 1)(1, b)]^l \\
&= (a, 1)^l (1, b)^l && \text{By the commutativity we just proved} \\
&= (a^l, 1)(1, b^l) \\
\iff (1, 1) &= (a^l, b^l)
\end{aligned}$$

Which happens iff $a^l = 1, b^l = 1$. I.e. iff $l = qA = tB$, for some positive integers q, t. I.e. iff l is a multiple of both A and B, i.e. l is a common multiple of A, B. But l is the *smallest* positive integer for which this holds, i.e. l must be the *least* common multiple of A and B.

1.1.31

We follow the hint and let $t(G) = \{g \in G | g \neq g^{-1}\}$. Note that the elements of $t(G)$ come in pairs (g and g^{-1}), hence its cardinality must be even.
Now let $g \in G - t(G)$ with $g \neq 0$. Does such an element exist? Since $1 \in t(G)$, we do have $|G| > t(G)$. If $|G| = t(G) + 1$, then G would be odd, a contradiction. So we must have $|G| \geq t(G) + 2$, i.e. $G - t(G)$ has at least one nonidentity element g, and for this element we have $g = g^{-1} \implies g^2 = 1$.

1.1.32

Suppose $x^k = x^l$, with $0 \leq k \leq l \leq n-1$. Then

$$\begin{aligned} & x^k = x^l \\ \implies & 1 = x^{l-k} \\ \implies & l - k = rn \end{aligned}$$

Where $r \in Z$. Since $l \geq k$, we must have $r \geq 0$. Now suppose $r > 0$. Then $l = rn + k > n - 1$, a contradiction. Hence $r = 0$ and $l - k = 0$ i.e. $l = k$.
Now if $|x| > |G|$, then the elements $1, x, \ldots, x^{n-1}$ would comprise $n > |G|$ distinct elements in G, which is impossible.

1.1.33

A lemma will help us here.

Lemma 2. *For $i = 1, 2, \ldots, n-1$, if $x^i = x^{-i}$, then $2i = n$.*

Proof.

$$\begin{aligned} & x^i = x^{-i} \\ \implies & x^{2i} = 1 \\ \implies & 2i = rn && \text{for some } r \in \mathbb{Z} \end{aligned}$$

We must show that $r = 1$, and we're done. If $r \leq 0$, this would contradict $1 \leq i < n$.
If $r \geq 2$, then

$$\begin{aligned} 2i &= rn \\ \implies i &= \frac{r}{2}n \\ &> \frac{2}{2}n \\ &= n \end{aligned}$$

which again contradicts $1 \leq i < n$. So we must have $r = 1$ □

(a) With n odd, suppose $x^i = x^{-i}$. Then applying the lemma yields $2i = n$, making n even, a contradiction.

(b) With n even, for $\implies$, suppose $x^i = x^{-i}$. Applying the lemma again yields

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

Now for $\impliedby$, suppose $i = k$. Then

$$\begin{aligned} 1 &= x^n \\ &= x^{2k} \\ &= x^{2i} \\ \implies x^{-i} &= x^i \end{aligned}$$

1.1.34

Let $n, m \in \mathbb{Z}$. Assume $w.l.g m \geq n$. Then

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

Since $m \geq n$, we have $m-n \geq 0$ If $m-n > 0$, then $|x| \leq m-n$, contradicting $|x| = \infty$. Hence $m-n = 0$, i.e. $m = n$

1.1.35

Let $l \in \mathbb{Z}$. Then by Euclidean division, $l = kn + r$ with $0 \leq r < n$. So

$$\begin{aligned} x^l &= x^{kn+r} \\ &= x^{kn}x^r \\ &= (x^n)^k x^r \\ &= (1)^k x^r \\ &= 1x^r \\ &= x^r \end{aligned}$$

1.4 Matrix Groups

1.4.1

Since $\mathbb{F}_2 = \{0, 1\}$, it's straightforward to exhaust the elements of $GL_2(\mathbb{F}_2)$ by "turning on/off" the entries. These elements are:

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

Any other possible element's determinant is 0

1.4.2

We already listed the elements above. Simple computation gives us $|I| = 1$, $|A| = |C| = |D| = 2$, $|B| = |E| = 3$

1.4.3

We'll take the following lemma for granted moving forward:

Lemma 3. *In a field F, $0 \neq 1$*

Proof. If $0 = 1$ in F, then $F^\times = F - \{0\}$ does not contain the multiplicative identity, and therefore $F^\times$ is not an abelian group, violating the first condition in the definition of a field. □

Let $x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $y = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Then the top left entry of xy is $2 = 0$ but the top left entry of yx is 1. Since $1 \neq 0$ in a field, $xy \neq yx$.

1.4.4

Let $n = ab$ where $a, b \neq 1$. Suppose there was some $l \in \mathbb{Z}$ such that

$$\begin{aligned}
\overline{a} \cdot \overline{l} &= \overline{1} \\
\implies \overline{al} &= \overline{1} \\
\implies \overline{al} - \overline{1} &= \overline{0} \\
\implies \overline{al - 1} &= \overline{0} \\
\implies al - 1 &= qn && \text{for some integer } q \\
&= qab \\
\implies al - abq &= 1 \\
\implies a(l - bq) &= 1
\end{aligned}$$

Since $a \neq 1$ and $l - bq$ must be an integer, this is impossible. Thus $\overline{a}$ does not have a multiplicative inverse, so $\mathbb{Z}/n\mathbb{Z}$ cannot be a field.

1.4.5

- $\Longleftarrow$: If $|F| = q$ is finite, then there are at most q possibilities for each entry of an element from $GL_n(F)$, therefore $|GL_n(F)| \leq q^{n^2}$. In fact, since the 0 matrix is non-invertible, we can make this a strict inequality:

$$|GL_n(F)| < q^{n^2} \tag{2}$$

- $\Longrightarrow$: If F is infinite consider the correspondence $F^\times \to GL_n(F)$ given by

$$f \mapsto \begin{pmatrix} f & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & f \end{pmatrix} \tag{3}$$

  I.e. f on the diagonal and 0s everywhere else, in case that wasn't clear.
  This is an injective group homomorphism, or just note that it clearly embeds $F^\times$ into $GL_n(F)$ as a subgroup. Therefore, we have an infinite subgroup of $GL_n(F)$, making $GL_n(F)$ infinite.

1.4.6

Already shown in the previous exercise by by eq. (2).

1.4.7

The total number of 2×2 matrices over $\mathbb{F}_p$ is clearly p^4 (as we went over in the above 2 exercises).
Now we count all the noninvertible matrices, taking note that a 2×2 is noninvertible $\iff$ one row is a multiple of the other. Let's proceed by cases.

- Select for all the matrices whose top two entries are both nonzero: $(p-1)(p-1)$. To get the noninvertible matrices of this form, we take a multiple of the top row as the bottom row, so there are p choices for the bottom row (since there are p multiples of the top row), hence the total number of matrices in this case is $p(p-1)(p-1) = p^3 - 2p^2 + p$. The following cases proceed similarly.
- Matrices where top-left entry is 0 and top-right entry is nonzero: $p - 1$ choices for the top row, and we take multiples for the bottom row so in total $p(p-1)$ matrices
- Matrices where top-left entry is nonzero and top-right entry is 0. Analagous to the above case, yielding again $p(p-1)$ matrices
- Lastly, consider the matrices where the top entries are both 0. Then any entries for the bottom row work. there are two entries in the bottom row, so p^2 matrices

Adding these all together, we get

$$\begin{aligned}(p^3-2p^2+p)+(p^2-p)+(p^2-p)+p^2 &= p^3-2p^2+p^2+p^2+p^2+p-p-p\\ &= p^3-2p^2+3p^2-p\\ &= p^3+p^2-p\end{aligned}$$

We subtract this result (number of noninvertible matrices) to the total number of matrices to obtain the number of invertible matrices:

$$p^4-(p^3+p^2-p)=p^4-p^3-p^2+p \tag{4}$$

1.4.8

We'll also take the following lemma for granted

Lemma 4. *In a nontrivial field F, $n \neq n+1$*

Proof.

$$\begin{aligned} & n = n+1\\ \implies & 0 = 1\end{aligned}$$

which we can't have in a field □

Let p be the identity matrix except that the toprightmost entry is 1. Let q be the identity matrix except the bottomleftmost entry is 1. The topleft entry of qp is 1 but the topleft entry of pq is 2. They cannot be equal because of the lemma, and hence $qp \neq pq$

1.4.9

The following proof works for matrices over any field F

$$\begin{aligned}[\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}e & f\\ g & h\end{pmatrix}]\begin{pmatrix}i & j\\ k & l\end{pmatrix} &= \begin{pmatrix}ae+bg & af+bh\\ ce+dg & cf+dh\end{pmatrix}\begin{pmatrix}i & j\\ k & l\end{pmatrix}\\ &= \begin{pmatrix}aei+bgi+afk+bhk & aej+bgj+afl+bhl\\ cei+dgi+cfk+dhk & cej+dgj+cfl+dhl\end{pmatrix}\\ &= \begin{pmatrix}a(ei+fk)+b(gi+hk) & a(ej+fl)+b(gj+hl)\\ c(ei+fk)+d(gi+hk) & c(ej+fl)+d(gj+hl)\end{pmatrix}\\ &= \begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}ei+fk & ej+fl\\ gi+hk & gj+hl\end{pmatrix}\\ &= \begin{pmatrix}a & b\\ c & d\end{pmatrix}[\begin{pmatrix}e & f\\ g & h\end{pmatrix}\begin{pmatrix}i & j\\ k & l\end{pmatrix}]\end{aligned}$$

1.4.10

(a)

$$\begin{pmatrix}a_1 & b_1\\ 0 & c_1\end{pmatrix}\begin{pmatrix}a_2 & b_2\\ 0 & c_2\end{pmatrix}=\begin{pmatrix}a_1a_2 & a_1b_2+b_1c_2\\ 0 & c_1c_2\end{pmatrix} \tag{5}$$

Since $a_1, a_2, c_1, c_2 \neq 0$, we have $a_1a_2 \neq 0$ and $c_1c_2 \neq 0$, so the result is still in G (So G is closed under matrix multiplication)

(b) Note: $a, c \neq 0$, and we need

$$\begin{aligned} & \begin{pmatrix}a & b\\ 0 & c\end{pmatrix}\begin{pmatrix}e & f\\ 0 & g\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\\ \iff & \begin{pmatrix}ae & af+bg\\ 0 & cg\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\end{aligned}$$

Which is true iff the following system of equations hold

$$\begin{aligned} ae &= 1 \\ af + bg &= 0 \\ cg &= 1 \end{aligned}$$

Since $a, c \neq 0$, we can divide by them to obtain

$$\begin{aligned} e &= 1/a \\ f &= \frac{-bg}{a} \\ g &= 1/c \end{aligned}$$

We substitute $g = 1/c$ into the second equation to obtain $f = \frac{-b}{ca}$. Note that all the work can be connected by iffs. Hence, we have

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^{-1} = \begin{pmatrix} 1/a & \frac{-b}{ac} \\ 0 & 1/c \end{pmatrix} \tag{6}$$

(c) In exercise 1.1.26 we showed that closure under the operation and inverses means that it is a subgroup

(d)
- Closure under multiplication: Take eq. (7) and make $c_1 = a_1$ and $c_2 = a_2$, so the result becomes

$$\begin{pmatrix} a_1 & b_1 \\ 0 & a_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 c_2 \\ 0 & a_1 a_2 \end{pmatrix} \tag{7}$$

  which is clearly in G because the diagonal entries are equal.
- Closure under inverses: Take eq. (6) and make $c = a$, so we get

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}^{-1} = \begin{pmatrix} 1/a & \frac{-b}{a^2} \\ 0 & 1/a \end{pmatrix} \tag{8}$$

  Again, the inverse is clearly in G because the diagonals are equal.

1.4.11

(a)

$$XY = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} \tag{9}$$

$$= \begin{pmatrix} 1 & a+d & e+af+b \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{pmatrix} \tag{10}$$

Which is still clearly in $H(F)$, making it closed under matrix multiplication. Also note that

$$YX = \begin{pmatrix} 1 & a+d & b+cd+e \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{pmatrix} \tag{11}$$

Now note that

$$\begin{aligned} & XY = YX \\ \iff & e + af + b = b + cd + e \\ \iff & af = cd \end{aligned}$$

So no matter what field F, we're using, we can let $a, f = 0$ and $c, d = 1$ to obtain $XY \neq YX$. Explicitly, an example of two matrices that don't commute is:

$$X = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$
$$Y = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

(b) Using eq. (10), We need

$$\begin{pmatrix} 1 & a+d & b+cd+e \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{12}$$

i.e. we obtain a system of equations and solve:

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

I.e.

$$X^{-1} = \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix} \tag{13}$$

(c) Let X, Y be as given and let $Z = \begin{pmatrix} 1 & g & h \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix}$. Then, using eq. (10) again,

$$\begin{aligned} (XY)Z &= \begin{pmatrix} 1 & a+d & e+af+b \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & g & h \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & g+a+d & h+i(a+d)+e+af+b \\ 0 & 1 & i+c+f \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & a+d+g & h+ia+id+e+af+b \\ 0 & 1 & c+f+i \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & a+d+g & a(f+i)+b+h+id+e0 & 1 & c+f+i \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & d+g & h+id+e0 & 1 & f+i \\ 0 & 0 & 1 \end{pmatrix} \\ &= X[\begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & g & h \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix}] \\ &= X(YZ) \end{aligned}$$

Given an element of $H(F)$, we have 3 entries to input, and ee have $|F|$ choices for each entry, so the order is $|F|^3$ (any possible combination of the three entries yields a valid element, no noninvertible matrices or anything to cut out)

(d) We're going to do some prep work here. Let's study the powers of elements from $H(F)$. We note that, by

computation

$$X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$
$$X^2 = \begin{pmatrix} 1 & 2a & 2b+ac \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{pmatrix}$$
$$X^3 = \begin{pmatrix} 1 & 3a & 3b+3ac \\ 0 & 1 & 3c \\ 0 & 0 & 1 \end{pmatrix}$$
$$X^4 = \begin{pmatrix} 1 & 4a & 4b+6ac \\ 0 & 1 & 4c \\ 0 & 0 & 1 \end{pmatrix}$$
$$X^5 = \begin{pmatrix} 1 & 5a & 5b+10ac \\ 0 & 1 & 5c \\ 0 & 0 & 1 \end{pmatrix}$$

etc. We notice a pattern, which is fairly straightforward, except for the coefficient of ac. It follows the sequence $0, 1, 3, 6, 10, \ldots$. I.e. start at 0, add 1, then add 2, then add 3, etc. We can describe the sequence recursively:

$$a_1 = 0$$
$$a_n = a_{n-1} + n - 1$$

We would like to derive a closed form expression for a_n, and thus we expand:

$$\begin{aligned} a_n &= a_{n-1} + n - 1 \\ &= a_{n-2} + (n-2) + (n-1) \\ &= a_{n-3} + (n-3) + (n-2) + (n-1) \\ &= \cdots \\ &= a_{n-(n-1)} + (n-(n-1)) + \cdots + (n-3) + (n-2) + (n-1) \\ &= a_1 + 1 + \cdots + (n-3) + (n-2) + (n-1) \\ &= 0 + 1 + \cdots + (n-3) + (n-2) + (n-1) \\ &= 0 + 1 + 2 + 3 + \cdots + (n-3) + (n-2) + (n-1) \end{aligned}$$

This is just the standard summation of the arithmetic sequence with common difference 1, and hence

$$a_n = \frac{n(n-1)}{2} \tag{14}$$

We now can derive a formula for X^n

Lemma 5. *Given* $X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \in H(F)$ *and* n *a nonnegative integer,*

$$X^n = \begin{pmatrix} 1 & na & nb + \frac{n(n-1)}{2}ac \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{pmatrix} \tag{15}$$

Proof. Base case: If $n = 0$, then this just reduces to the identity.
Now we suppose that

$$X^{n-1} = \begin{pmatrix} 1 & (n-1)a & (n-1)b + \frac{(n-1)(n-2)}{2}ac \\ 0 & 1 & (n-1)c \\ 0 & 0 & 1 \end{pmatrix} \tag{16}$$

Then

$$\begin{aligned}
X^n &= X^{n-1}X \\
&= \begin{pmatrix} 1 & (n-1)a & (n-1)b + \frac{(n-1)(n-2)}{2}ac \\ 0 & 1 & (n-1)c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & (n-1)a + a & b + (n-1)ac + (n-1)b + \frac{(n-1)(n-2)}{2}ac \\ 0 & 1 & c + (n-1)c \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & na & b + (n-1)b + (n-1)ac + \frac{(n-1)(n-2)}{2}ac \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & na & nb + (n-1)ac + \frac{(n-1)(n-2)}{2}ac \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & na & nb + ((n-1) + \frac{(n-1)(n-2)}{2})ac \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{pmatrix}
\end{aligned}$$

Clearly, if we show that $(n-1) + \frac{(n-1)(n-2)}{2} = \frac{n(n-1)}{2}$, we're done. But

$$\begin{aligned}
(n-1) + \frac{(n-1)(n-2)}{2} &= \frac{2(n-1)}{2} + \frac{(n-1)(n-2)}{2} \\
&= \frac{2(n-1) + (n-1)(n-2)}{2} \\
&= \frac{2n - 2 + n^2 - 3n + 2}{2} \\
&= \frac{n^2 + 2n - 3n + 2 - 2}{2} \\
&= \frac{n^2 - n}{2} \\
&= \frac{n(n-1)}{2}
\end{aligned}$$

□

Now we actually find the order of each element of $H(\mathbb{F}_2)$. Note that from the previous part, $|H(\mathbb{F}_2)| = |\mathbb{F}_2|^3 =$

$2^3 = 8$, and we can exhaustively list the elements of $H(\mathbb{F}_2)$ by "turning the entries on/off":

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

Of course, $|I| = 1$. Note that in for any $x \in \mathbb{F}_2$, $2x = 0$ (in fact, nx for any even n). Now consider any element $X = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \in H(\mathbb{F}_2)$ where $ac = 0$. Then following lemma 5,

$$\begin{aligned} X^2 &= \begin{pmatrix} 1 & 2a & 2b + \frac{2(2-1)}{2}ac \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 + \frac{2(1)}{2}ac \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & ac \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{aligned}$$

Hence $X^2 = I$ for any X where $ac = 0$. Hence, $|A| = |B| = |E| = |F| = |G| = 2$

The only two elements left to check are C and D, and we can actually prove the order of these elements simultaneously, by letting b be arbitrary. Let $X = \begin{pmatrix} 1 & 1 & b \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$. Clearly $X^1 \neq I$ and $X^2 \neq I$. Also, looking at lemma 5, odd numbered exponents would make $na = n1 = n$ and $nc = n$ nonzero, so we have to check the

next even-numbered exponent, i.e.

$$\begin{aligned} X^4 &= \begin{pmatrix} 1 & 4\cdot 1 & 4b + \frac{4(4-1)}{2} 1\cdot 1 \\ 0 & 1 & 4\cdot 1 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 + \frac{4(3)}{2}\cdot 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 12\cdot 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{aligned}$$

So $|X| = 4$, and X could be either C or D, so $|C| = |D| = 4$

(e) Given nonidentity X in $H(\mathbb{R})$, we must have either $a \neq 0$, $b \neq 0$, or $c \neq 0$. Now, given $n \in \mathbb{Z}^+$ an integer, suppose X^n is the identity matrix. I.e. using lemma 5, suppose

$$\begin{pmatrix} 1 & na & nb + \frac{n(n-1)}{2} ac \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{17}$$

Which occurs iff the following system of equations holds:

$$\begin{aligned} na &= 0 \\ nb + \frac{n(n-1)}{2} ac &= 0 \\ nc &= 0 \end{aligned}$$

We proceed by cases:

- Case: $a \neq 0$. Then since $n \neq 0$, the first equation cannot hold.
- Case: $c \neq 0$. Then since $n \neq 0$, the third equation cannot hold.
- Case: $b \neq 0$. Then consider the second equation. If it holds, then since n and b are both nonzero, we must have that $\frac{n(n-1)}{2} ac \neq 0$. And in $\mathbb{R}$, this means that we must have $n \neq 0$, $n - 1 \neq 0$, $a \neq 0$, $c \neq 0$, but the latter two inequalities are covered in the first two cases.

1.6

Let G and H be groups

We start with some lemmas:

Lemma 6. *If $\phi : G \to H$ a homomorphism, then $\phi(1) = 1$*

Proof. Let $x \in G$. Then

$$\begin{aligned} \phi(x)\phi(1) &= \phi(x \cdot 1) && \phi \text{ a homomorphism} \\ &= \phi(x) \\ \implies \phi(1) &= 1 && \text{by left cancelation} \end{aligned}$$

□

Lemma 7. *The composition of two homomorphisms is a homomorphism*

Proof. Let $\phi : A \to B, \psi : B \to C$ be homomorphisms. Then given arbitrary $a, b \in A$,

$$\begin{aligned} \psi \circ \phi(ab) &= \psi(\phi(ab)) \\ &= \psi(\phi(a)\phi(b)) && \phi \text{ a homomorphism} \\ &= \psi(\phi(a))\psi(\phi(b)) && \psi \text{ a homomorphism} \\ &= \psi \circ \phi(a)\psi \circ \phi(b) \end{aligned}$$

□

Lemma 8. *If $\phi : G \to H$ is an isomorphism, its inverse map $\psi : H \to G$ is a homomorphism (and therefore is an isomorphism as well). We can therefore denote $\psi = \phi^{-1}$.*

Proof. From basic set theory, any bijection ϕ has a unique inverse map ψ, so that $\psi \circ \phi = \mathbf{1}$. We need to show that ψ is a homomorphism. Let $h, h' \in H$. Then there are $g, g' \in G$ such that $\phi(g) = h$ and $\phi(g') = h'$. Then

$$\begin{aligned} \psi(hh') &= \psi(\phi(g)\phi(g')) \\ &= \psi(\phi(gg')) && \phi \text{ is a homomorphism} \\ &= \psi \circ \phi(gg') \\ &= gg' && \psi \text{ is the inverse map} \\ &= \psi(h)\psi(h') \end{aligned}$$

□

1.6.1

Let $\phi : G \to H$ be a homomorphism.

(a) *Prove that $\phi(x^n) = \phi(x)^n$ for all $n \in \mathbb{Z}^+$*

- Base Case: $n = 1$. Then $\phi(x^n) = \phi(x^1) = \phi(x) = \phi(x)^1 = \phi(x)^n$.
- Induction: We assume that $\phi(x^{n-1}) = \phi(x)^{n-1}$. Then

$$\begin{aligned} \phi(x^n) &= \phi(x^{n-1}x) \\ &= \phi(x^{n-1})\phi(x) && \phi \text{ is a homomorphism} \\ &= \phi(x)^{n-1}\phi(x) && \text{Inductive hypothesis} \\ &= \phi(x)^n \end{aligned}$$

(b) *Do part (a) for $n = -1$ and deduce that $\phi(x^n) = \phi(x)^n$ for all $n \in \mathbb{Z}$.*

- We first show this for $n = -1$:

$$\begin{aligned} \phi(x)\phi(x^{-1}) &= \phi(xx^{-1}) && \phi \text{ a homomorphism} \\ &= \phi(1) \\ &= 1 && \text{By lemma 6} \end{aligned}$$

- Now suppose $n \in Z$ is a negative integer. Let $m \in -n$, so that $m \in \mathbb{Z}^+$. Then

$$\begin{aligned}
\phi(x^n) &= \phi(x^{-m}) \\
&= \phi((x^m)^{-1}) \\
&= \phi(x^m)^{-1} && \text{The } n = -1 \text{ case} \\
&= (\phi(x)^m)^{-1} && \text{By (a)} \\
&= \phi(x)^{-m} \\
&= \phi(x)^n
\end{aligned}$$

- The $n = 0$ case is obvious, via lemma 6: $\phi(x^0) = \phi(1) = 1 = \phi(x)^0$

1.6.2

If $\phi : G \to H$ is an isomorphism, prove that $|\phi(x)| = |x|$ for all $x \in G$. Deduce that any two isomorphic groups have the same number of elements of order n for each $n \in \mathbb{Z}^+$. Is the result true if ϕ is only assumed to be a homomorphism?

Let $x \in G$ and denote $|\phi(x)| = n$, $|x| = k$. Then

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

But

$$\begin{aligned}
& \phi(x)^n = 1 \\
\implies & \phi(x^n) = 1 \\
\implies & x^n = \phi^{-1}(1) && \phi \text{ is an isomorphism} \\
& = 1
\end{aligned}$$

so $k \leq n$. Hence, $k = n$.
The fact that two isomorphic groups have the same elements of order for each positive integer follows trivially. If ϕ is only a homomorphism, the result is not necessarily true: Consider the trivial homomorphism $G \to \{1\}$ where G has elements of order > 1

1.6.3

If $G \to H$ is an isomorphism, prove that G is abelian if and only if H is abelian. If $\phi : G \to H$ is a homorphism, what additional conditions on ϕ (if any) are sufficient to ensure that if G is abelian, then so is H?

- $\implies$: Let G be abelian. Then given $h, h' \in H$ there are g, g' s.t. $\phi(g) = h, \phi(g') = h'$ (since ϕ is an isomoprhism). Then

$$\begin{aligned}
hh' &= \phi(g)\phi(g') \\
&= \phi(gg') \\
&= \phi(g'g) && G \text{ abelian} \\
&= \phi(g')\phi(g) \\
&= h'h
\end{aligned}$$

  Since $h, h' \in H$ were arbitrary, H is abelian.

- $\impliedby$: Apply the same proof with ϕ^{-1} instead of ϕ

- For an arbitrary homomorphism ϕ, it suffices for ϕ to be surjective (The proof above works, because we can select $g \in \phi^{-1}(h), g' \in \phi^{-1}(h')$.

1.6.4

Prove that the multiplicative groups $\mathbb{R} - \{0\}$ *and* $\mathbb{C} - \{0\}$ *are not isomorphic.*

Note that $|e^{\frac{2\pi}{7}i}| = 7$, but $\mathbb{R} - \{0\}$ only has elements of order $1, 2, \infty$. Apply 1.6.2

1.6.5

Prove that the additive groups $\mathbb{R}$ *and* $\mathbb{Q}$ *are not isomorphic.*

$\mathbb{R}$ is uncountable and $\mathbb{Q}$ is countable. By basic theory, not even a bijection exists between them.

1.6.6

Prove that the additive groups $\mathbb{Z}$ *and* $\mathbb{Q}$ *are not isomorphic.*

Suppose $\phi : \mathbb{Z} \to \mathbb{Q}$ was an isomorphism. Then given $n \in \mathbb{Z}$, apply 1.6.1: $\phi(n) = \phi(1n) = n\phi(1) = n \cdot 1 = n$. So ϕ only maps onto the integers and therefore is not surjective onto $\mathbb{Q}$.

1.6.11

Let A *and* B *be groups. Prove that* $A \times B \cong B \times A$.

The map $(a, b) \mapsto (b, a)$ is clearly an isomorphism. Not going to bother typing out the work for this and the next problem.

1.6.12

Let $A, B,$ *and* C *be groups and let* $G = A \times B$ *and* $H = B \times C$. *Prove that* $G \times C \cong A \times H$.

Clearly the map $((a, b), c) \mapsto (a, (b, c))$ is an isomorphism.

1.6.13

Let G *and* H *be groups and let* $\phi : G \to H$ *be a homomorphism. Prove that the image of* ϕ, $\phi(G)$, *is a subgroup of* H *(cf. Exercise of Section 1). Prove that if* ϕ *is injective then* $G \cong \phi(G)$.

- Closed under the operation: If $h, h' \in \phi(G)$, then $\exists g, g' \in G$ such that $\phi(g) = h, \phi(g') = h'$. And $hh' = \phi(g)\phi(g') = \phi(gg') \in \phi(G)$.
- Closed under inverses: If $h \in \phi(G)$, then $\exists g \in G$ s.t. $\phi(g) = h$. Let $h' = \phi(g^{-1})$, and note that $h' \in \phi(G)$. And $hh' = \phi(g)\phi(g^{-1}) = \phi(gg^{-1}) = \phi(1) = 1$. So $h' = h^{-1}$ and $h^{-1} \in \phi(G)$.
- ϕ is trivially surjective onto $\phi(G)$. If it's also injective, that makes it bijective and therefore an isomorphism (onto $\phi(G)$).

1.6.14

Let G *and* H *be groups and let* $\phi : G \to H$ *be a homomorphism. Define the* kernel *of* ϕ *to be* $\{g \in G | \phi(g) = 1_H\}$ *(so the kernel is the set of elements in* G *which map to the identity of* H, *i.e., is the fiber over the identity of* G, *i.e., is the fiber over the identity of* H*). Prove that the kernel of* ϕ *is a subgroup (cf. Exercise 26 of Section 1) of* G. *Prove that* ϕ *is injective if and only if the kernel of* ϕ *is the identity subgroup of* G.

(1) We first show that $\ker \phi$ is a subgroup.

- Closure under the operation: Let $g, g' \in \phi^{-1}(1)$. Then

$$\begin{aligned} \phi(gg') &= \phi(g)\phi(g') \\ &= 1 \cdot 1 \\ &= 1 \\ \implies gg' &\in \phi^{-1}(1) \end{aligned}$$

- Closure under inverse. Given $g \in \phi^{-1}(1)$. we note that

$$\begin{aligned} \phi(g^{-1}) &= \phi(g)^{-1} \\ &= 1^{-1} \\ &= 1 \\ \implies g^{-1} &\in \phi^{-1}(1) \end{aligned}$$

(2) Now we show that ϕ is injective $\iff \phi^{-1}(1) = \{1\}$. Let's prove a lemma

Lemma 9. *$\phi : G \to H$ is injective if and only if $\forall g \in G : \phi(g) = 1 \implies g = 1$*

Proof. The definition of an injective map is $\phi(g) = \phi(h) \implies g = h$.

- $\implies$: Suppose ϕ is injective. Note that since ϕ is a homomorphism, $\phi(1) = 1$ by lemma 6. But $\phi(g) = 1$. So we must have have $g = 1$ because ϕ is injective.
- $\impliedby$: Let $g, h \in G$. Then

$$\begin{aligned} \phi(g) &= \phi(h) \\ \implies 1 &= \phi(h)\phi(g)^{-1} \\ &= \phi(h)\phi(g^{-1}) \\ &= \phi(hg^{-1}) \\ \implies 1 &= hg^{-1} \\ \implies g &= h \end{aligned}$$

Since g, h were arbitrary, ϕ is injective

□

Now we proceed with the exercise

- $\implies$: Suppose ϕ injective. Then given $g \in G$,

$$\begin{aligned} \phi(g) &= 1 \\ &= \phi(1) && \text{by lemma 6} \\ \implies g &= 1 && \text{by lemma 9} \end{aligned}$$

Since g was arbitrary, we have $\phi^{-1}(1) = \{1\}$.

- $\impliedby$: Suppose $\phi^{-1}(1) = \{1\}$. Then given $g \in G$,

$$\begin{aligned} \phi(g) &= 1 \\ \implies g &\in \phi^{-1}(1) \\ \implies g &= 1 && \text{by the condition} \end{aligned}$$

Hence lemma 9 gives us injectivity.

1.6.15

Define a map $\pi : \mathbb{R}^2 \to \mathbb{R}$ by $\phi((x, y)) = x$. Prove that π is a homomorphism and find the kernel of π (cf. Exercises 1.6.14).

- Let $(x, y), (a, b) \in \mathbb{R}^2$. Then $\pi((x, y)(a, b)) = \pi(xa, yb) = xa = \pi(x, a)\pi(y, b)$. Thus, π is a homomorphism.
- If we have $\pi(x, y) = 1$, then we must have $x \in 1$. Hence $\ker \pi = \{(1, y)|y \in \mathbb{R}\}$.

1.6.16

Let A and B be groups and let G be their direct product, $A \times B$. Prove that the maps $\pi_1 : G \to A$ and $\pi_2 : G \to B$ defined by $\pi_1((a, b)) = a$ and $\pi_2((a, b)) = b$ are homomorphisms and find their kernels.

The demonstration that they are homomorphisms is analagous to the previous exercise. The kernels are also analagous

1.6.17

Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^{-1}$ is a homomorphism if and only if G is abelian.

Denote the map as ϕ

- $\implies$: Suppose ϕ a homomorphism. Then

$$\begin{aligned} gh &= \phi(g^{-1})\phi(h^{-1}) \\ &= \phi(g^{-1}h^{-1}) \\ &= \phi((hg)^{-1}) \\ &= hg && \text{Definition of } \phi \end{aligned}$$

  Hence G is abelian

- $\impliedby$: Suppose G is abelian. Then

$$\begin{aligned} \phi(gh) &= (gh)^{-1} \\ &= h^{-1}g^{-1} \\ &= g^{-1}h^{-1} && G \text{ abelian} \\ &= \phi(g)\phi(h) \end{aligned}$$

  Hence, ϕ is a homomorphism.

1.6.18

Let G be any group. Prove that the map from G to itself defined by $g \mapsto g^2$ is a homomorphism if and only if G is abelian.

Denote the map as ϕ

- $\implies$: Suppose ϕ is a homomorphism. Let $g, h \in G$. Then

$$\begin{aligned} gh &= 1gh1 \\ &= g^{-1}gghhh^{-1} \\ &= g^{-1}g^2h^2h^{-1} \\ &= g^{-1}\phi(g)\phi(h)h^{-1} \\ &= g^{-1}\phi(gh)h^{-1} && \phi \text{ homomorphism} \\ &= g^{-1}(gh)^2h^{-1} \\ &= g^{-1}ghghh^{-1} \\ &= 1hg1 \\ &= hg \end{aligned}$$

  Hence, G is abelian.

- $\impliedby$: Suppose G is abelian. Then given $g, h \in G$,

$$\begin{aligned} \phi(gh) &= (gh)^2 \\ &= ghgh \\ &= gghh && G \text{ abelian} \\ &= g^2h^2 \\ &= \phi(g)\phi(h) \end{aligned}$$

  So ϕ is a homomorphism.

1.6.19

Let $G = \{z \in \mathbb{C} | z^n = 1$ for some $n \in \mathbb{Z}^+\}$. Prove that for any fixed integer $k > 1$ the map from G to itself defined by $z \mapsto z^k$ is a surjective homomorphism but is not an isomorphism

Fix $k > 1$ an integer and denote the homomorphism by ϕ. Let $z \in G$. Then $\exists n \in \mathbb{Z}^+$ such that $z^n = 1$. We write $z = re^{xi}$, and assume *w.l.g*that $r \geq 0$. Then

$$\begin{aligned} z^n &= 1 \\ \implies (re^{xi})^n &= 1 \\ \implies r^n e^{xni} &= 1e^{0i} \end{aligned}$$

So we must have $r = 1$ and, for some $m \in \mathbb{Z}$, we have $xn = 2\pi m$. Dividing by n on both sides yields

$$x = \frac{2\pi m}{n} \tag{18}$$

We want l such that

$$\begin{aligned} \phi(l) &= z \\ \implies (re^{yi})^k &= e^{\frac{2\pi m}{n}i} \\ \implies r^k e^{yki} &= 1e^{\frac{2\pi m}{n}i} \end{aligned}$$

So we must have $r = 1$ and also

$$\begin{aligned} yk &= \frac{2\pi m}{n} \\ \implies y &= \frac{2\pi m}{nk} \end{aligned}$$

Hence, $l = e^{\frac{2\pi m}{nk}} \mapsto z$ under ϕ (Note that $l^{nk} = 1$ as well, so $l \in G$). Since $z \in G$ was arbitrary, ϕ is surjective. Also note that $e^{\frac{2\pi}{k}i}, e^{\frac{4\pi}{k}i} \in G$ are not equal, but they both map to 1 under ϕ.

1.6.20

Let G be a group and let $\mathrm{Aut}(G)$ *be the set of all isomorphisms from G onto G. Prove that* $\mathrm{Aut}(G)$ *is a group under function composition (called the* automorphism group *of G and the elements of* $\mathrm{Aut}(G)$ *are called* automorphisms *of G*

- $\mathrm{Aut}\, G$ has an identity since the identity map is an isomorphism.
- If ϕ is an isomorphism, it has an inverse isomorphism by lemma 8.
- $\mathrm{Aut}\, G$ is closed under composition by lemma 7
- Associativity: Let $\phi, \psi, \delta \in \mathrm{Aut}\, G$, and let $g \in G$. Then

$$\begin{aligned}\phi \circ (\psi \circ \delta)(g) &= \phi(\psi \circ \delta(g)) \\ &= \phi(\psi(\delta(g))) \\ &= \phi \circ \psi(\delta(g)) \\ &= (\phi \circ \psi) \circ \delta(g)\end{aligned}$$

  Since $g \in G$ was arbitrary, we have $\phi \circ (\psi \circ \delta) = (\phi \circ \psi) \circ \delta$

1.6.21

Prove that for each fixed nonzero $k \in \mathbb{Q}$ the map from $\mathbb{Q}$ to itself defined by $q \mapsto kq$ is an automorphism of $\mathbb{Q}$ (cf. Exercise 1.6.20).

Fix nonzero $k \in \mathbb{Q}$. Denote the homomorphism by ϕ. Let $q, p \in Q$. Then $\phi(q+p) = k(q+p) = kq+kp = \phi(q)+\phi(p)$, so ϕ is a homomorphism. Note that we must have $k \neq 0$ and $1/k \in \mathbb{Q}$, and the inverse map $q \mapsto \frac{1}{k}q$ makes ϕ a bijection, and therefore an automorphism.

1.6.22

Let A be an abelian group and fix some $k \in \mathbb{Z}$. Prove that the map $a \mapsto a^k$ is a homomorphism from A to itself. If $k = -1$ prove that this homomorphism is an isomorphism (i.e., is an automorphism of A).

- Denote the homomorphism ϕ. Then

$$\begin{aligned}\phi(ab) &= (ab)^k \\ &= a^k b^k && A \text{ abelian} \\ &= \phi(a)\phi(b)\end{aligned}$$

  so ϕ is a homomorphism
- Suppose $k = -1$. Then clearly ϕ is an inverse homomorphism for itself.

1.7

1.7.1

Let F be a field. Show that the multiplicative group of nonzero elements of F (denoted by $F^\times$) acts on the set F by $g \cdot a = ga$, where $g \in F^\times, a \in F$ and ga is the usual product in F of the two field elements (state clearly which axioms in the definition of a field are used).

What a long problem statement for a simple exercise

- Let $x, y \in F^\times$, and let $z \in F$. Then

$$\begin{aligned} x \cdot (y \cdot z) &= x \cdot (yz) && yz \text{ is multiplication in } F \\ &= x(yz) && yz \in F, \text{ and } x(yz) \text{ is multiplication in } F \\ &= (xy)z && \text{Associativity in } F \\ &= (x \cdot y) \cdot z && \text{Rewrapping in the definition} \end{aligned}$$

  IS THAT EXPLICIT ENOUGH DUMMY AND FOOTE?

- Let $x \in F$. Then $1 \cdot x = 1x = x$.

1.7.2

Show that the additive group $\mathbb{Z}$ acts on itself by $z \cdot a = z + a$ for all $z, a \in \mathbb{Z}$

- Let $x, y \in \mathbb{Z}$, and $z \in \mathbb{Z}$. Then

$$\begin{aligned} x \cdot (y \cdot z) &= x \cdot (y + z) \\ &= x + (y + z) \\ &= (x + y) + z && \text{Associativity in } \mathbb{Z} \\ &= (x + y) \cdot z \\ &= (x \cdot y) \cdot z \end{aligned}$$

- Let $z \in \mathbb{Z}$. Then $0 \cdot x = 0 + x = x$

1.7.3

Show that the additive groups $\mathbb{R}$ acts on the x, y plane $\mathbb{R} \times \mathbb{R}$ by $\cdot(x, y) = (x + ry, y)$.

- Let $r, z \in \mathbb{R}$ and $(x, y) \in \mathbb{R}^2$. Then $r \cdot (s \cdot (x, y)) = r \cdot (x + sy, y) = ((x + sy) + ry, y) = (x + (sy + ry), y) = (x + (s + r)y, y) = (x + (r + s)y, y) = (r + s) \cdot (x, y) = (r \cdot s) \cdot (x, y)$.
- Let $(x, y) \in \mathbb{R}^2$. Then $0 \cdot (x, y) = (x + 0y, y) = (x, y)$.

1.7.4

Let G be a groups acting on a set A and fix some $a \in A$. Show that the following sets are subgroups of G (cf. Exercise 1.1.26 of Section 1):

(a) *the kernel of the action,*

By the NEXT exercise (1.7.5), the kernel is equal to the kernel of a homorphism $G \to S_A$, so by Exercise 1.6.14, it is a subgroup of G.

(b) $\{g \in G | ga = a\}$ - *this subgroup is called the* stabilizer *of a in G.*

- Closure under the operation. Let $g, h \in G$. Let $g, h \in G$, and $a \in A$.

$$\begin{aligned} (gh)a &= g(ha) && \text{Property 1 of an action} \\ &= ga && h \in \operatorname{Stab} a \\ &= a && g \in \operatorname{Stab} a \end{aligned}$$

  Hence, $gh \in \operatorname{Stab} a$.

- Closure under inverses. Let $g \in G$. Then

$$\begin{aligned} a &= 1a \\ &= (g^{-1}g)a \\ &= g^{-1}(ga) \\ &= g^{-1}a && \text{Since } g \in \operatorname{Stab} a \end{aligned}$$

Hence, $g^{-1} \in \operatorname{Stab} a$.

1.7.5

*Prove that the kernel of an action of the group G on the set A is the same as the kernel of the corresponding permutation representation $G \to S_A$ (cf. Exercise 1.6.14 in Section **??**).*

Denote the action $\sigma : G \times A \to A$, so that, by definition,

$$\ker \sigma = \{g \in G | \forall a \in A : \sigma_g(a) = a\} \tag{19}$$

Denote the permutation representation $G \to S_A$ by ϕ. Then

$$\begin{aligned} \ker \phi &= \{g \in G | \phi(g) = \mathbf{1}\} \\ &= \{g \in G | \forall a \in A : \phi(g)(a) = \mathbf{1}(a)\} \\ &= \{g \in G | \forall a \in A : \phi(g)(a) = a\} \\ &= \{g \in G | \forall a \in A : \sigma_g(a) = a\} && \text{Definition of permutation representation} \end{aligned}$$

But this is exactly the same as eq. (19).

1.7.6

Prove that a group G acts faithfully on a set A if and only if the kernel of the action is the set consisting only of the identity.

As the book states, "A faithful action is therefore one in which the associated permutation representation is injective," and we apply 1.6.14.

1.7.7

Prove that in Example 2 in this section the action is faithful.

The Example is the action $\mathbb{R}^\times \times \mathbb{R}^n \to \mathbb{R}^n$ given by $\alpha(r_1, \ldots, r_n) = (\alpha r_1, \ldots, \alpha r_n)$. Then given $x \in \mathbb{R}^\times$, x is in the kernel of the action if and only if...

$$\begin{aligned} &\forall (r_1, \ldots, r_n) \in \mathbb{R}^n : x \cdot (r_1, \ldots, r_n) = (r_1, \ldots, r_n) \\ \iff &\forall r_1, \ldots, r_n \in \mathbb{R} : x \cdot (r_1, \ldots, r_n) = (r_1, \ldots, r_n) \\ \iff &\forall r_1, \ldots, r_n \in \mathbb{R} : (xr_1, \ldots, xr_n) = (r_1, \ldots, r_n) \end{aligned}$$

i.e. for $i = 1, \ldots, n$, we have $xr_i = r_i \iff x = 1$ (by right cancelation in $\mathbb{R}$). Since the r_i were arbitrary, the kernel is trivial (only includes 1).

1.7.8

Let A be a nonempty set and let k be a positive integer with $k \leq |A|$. The symmetric group S_A acts on the set B consisting of all subsets of A of cardinality k by $\sigma \cdot \{a_1, \ldots, a_k\} = \{\sigma(a_1), \ldots, \sigma(a_k)\}$.

(a) *Prove that this is a group action.*

- Let $\sigma, \delta \in S_A$, and $\{a_1, \ldots, a_k\} \in B$. Then

$$\begin{aligned} \sigma \cdot (\delta \cdot \{a_1, \ldots, a_k\}) &= \sigma \cdot (\{\delta(a_1), \ldots, \delta(a_k)\}) \\ &= \{\sigma(\delta(a_1)), \ldots, \sigma(\delta(a_k))\} \\ &= \{\sigma \circ \delta(a_1), \ldots, \sigma \circ \delta(a_k)\} \\ &= \sigma \circ \delta\{a_1, \ldots, a_k\} \qquad\qquad = \sigma \cdot \delta\{a_1, \ldots, a_k\} \end{aligned}$$

- Now let $\{a_1, \ldots, a_k\} \in B$. Then $\mathbf{1}\{a_1, \ldots, a_k\} = \{\mathbf{1}(a_1), \ldots, \mathbf{1}(a_k)\} = \{a_1, \ldots, a_k\}$

(b) *Describe explicitly how the elements* $(1\,2)$ *and* $(1\,2\,3)$ *act on the six* 2*-element subsets of* $\{1, 2, 3, 4\}$

$$\begin{aligned} (1\,2)\{1,2\} &= \{1,2\} \\ (1\,2)\{1,3\} &= \{2,3\} \\ (1\,2)\{1,4\} &= \{2,4\} \\ (1\,2)\{2,3\} &= \{1,3\} \\ (1\,2)\{2,4\} &= \{1,4\} \\ (1\,2)\{3,4\} &= \{3,4\} \end{aligned}$$

And

$$\begin{aligned} (1\,2\,3)\{1,2\} &= \{2,3\} \\ (1\,2\,3)\{1,3\} &= \{1,2\} \\ (1\,2\,3)\{1,4\} &= \{2,4\} \\ (1\,2\,3)\{2,3\} &= \{1,3\} \\ (1\,2\,3)\{2,4\} &= \{3,4\} \\ (1\,2\,3)\{3,4\} &= \{1,4\} \end{aligned}$$

1.7.9

Do both parts of the preceding exercise with "ordered k-tuples" in place of "k-element subsets," where the action on k-tuples is defined as above but with set braces replaced by parentheses.

Basically the same shit.

1.7.10

With reference to the preceding two exercises determine:

(a) *for which values of* k *the action of* S_n *on* k*-element subsets is faithful, and*

- Case: $k < |A|$. Then Let $\sigma \in S_A$, with $\sigma \neq \mathbf{1}$. Let $a \in A$ such that $\sigma(a) = b$ where $a \neq b$. (This is possible since $\sigma \neq \mathbf{1}$).
  Now let's take distinct $a_1, \ldots, a_{k-1} \in A$, such that $a, b \notin \{a_1, \ldots, a_{k-1}\}$. Is this possible? Yes, because

$$\begin{aligned} & k < |A| \\ \implies & k \leq |A| - 1 \\ \implies & k - 1 \leq |A| - 2 \\ & = |A - \{a, b\}| \end{aligned}$$

(By the way, if A is a singleton, then $k < |A|$ forces k to be 0. But k has to be a positive integer. So this can't happen in this case). Now we note that

$$\sigma\{a_1, \ldots, a_{k-1}, a\} = \{\sigma(a_1), \ldots, \sigma(a_{k-1}), b\} \tag{20}$$

Suppose we had

$$\{a_1, \ldots, a_{k-1}, a\} = \{\sigma(a_1), \ldots, \sigma(a_{k-1}), b\} \tag{21}$$

But $b \notin$LHS while $b \in$RHS. So they are not equal. Hence σ is not in the kernel. Since σ was an arbitrary nontrivial permutation, the kernel of the action is trivial, and the action is therefore faithful.

- Now let $k = |A|$. Then the only k-element subset of A is A itself. So $B = \{A\}$. And for any $\sigma \in S_A$, we have $\sigma A = A$, so σ is in the kernel of the action. i.e. the kernel in this case is all of S_A itself, and the action is therefore not faithful.

(b) *for which values of k the action of S_n on ordered k-tuples is faithful.*

Let $\sigma \in S_A$ with $\sigma \neq \mathbf{1}$. Let $a \in A$ such that $\sigma(a) = b$ with $a \neq b$. Let $a_1, \ldots, a_{k-1}$ distinct with $a \neq a_i$ for $i = 1, \ldots, k-1$ (This is possible since $k \leq |A|$ i.e. $k \leq |A| - 1$). Then

$$\sigma(a_1, \ldots, a_{k-1}, a) = (\sigma(a_1), \ldots, \sigma(a_{k-1}), b) \tag{22}$$

Since $a \neq b$, it is definitely the case that as tuples

$$(a_1, \ldots, a_{k-1}, a) \neq (\sigma(a_1), \ldots, \sigma(a_{k-1}), b) \tag{23}$$

So σ is not in the kernel of the action. Since it was arbitrary nontrivial, the kernel is trivial and the action is faithful.

1.7.13

Find the kernel of the left regular action.

$g \in G$ is in the kernel of the action if and only if

$$\begin{aligned} & \forall a \in A : ga = a \\ \iff & \forall a \in A : g = 1 && \text{Left cancellation} \\ \iff & g = 1 \end{aligned}$$

Hence, the kernel is trivial. (The action is faithful)

1.7.14

Let G be a group and let $A = G$. Show if G is non-abelian then the maps defined by $g \cdot a = ag$ for all $g, a \in G$ do not *satisfy the axioms of a (left) group action of G on itself.*

Let $g, h \in G$ and let $a \in G$. Then

$$\begin{aligned} (gh)a &= a(gh) \\ &= agh \end{aligned}$$

But

$$\begin{aligned} g(ha) &= g(ah) \\ &= (ah)g \\ &= ahg \end{aligned}$$

For this action to satisfy the first axiom in the definition, we would at least need $agh = ahg$. But if we let $a = 1$, then this is $gh = hg$. But this is not true for all $g, h \in G$ if G is non-abelian.

1.7.15

Let G be any group and let $A = G$. Show that the maps defined by $g \cdot a = ag^{-1}$ for all $g, a \in G$ do *satisfy the axioms of a (left) groups action of G on itself.*

- Let $g, h \in G$, and $a \in A = G$. Then

$$\begin{aligned}(gh) \cdot a &= a(gh)^{-1} \\ &= a(h^{-1}g^{-1}) \\ &= (ah^{-1})g^{-1} \\ &= g \cdot (ah^{-1}) \\ &= g \cdot (h \cdot a)\end{aligned}$$

- Let $a \in A$. Then $1 \cdot a = a1^{-1} = a1 = a$.

1.7.16

Let G be any group and let $A = G$. Show that the maps defined by $g \cdot a = gag^{-1}$ for all $g, a \in G$ do *satisfy the axioms of a (left) group action (this action of G on itself is called* conjugation*).*

- Let $g, h \in G$ and $a \in A = G$. Then

$$\begin{aligned}(gh) \cdot a &= (gh)a(gh)^{-1} \\ &= ghah^{-1}g^{-1} \\ &= g \cdot (hah^{-1}) \\ &= g \cdot (h \cdot a)\end{aligned}$$

- Let $a \in A$. Then $1 \cdot a = 1a1^{-1} = 1a1 = a$

1.7.17

Let G be a group and let G act on itself by left conjugation, so each $g \in G$ maps G to G by $x \mapsto gxg^{-1}$. For fixed $g \in G$, prove that conjugation by g is an isomorphism from G onto itself (i.e., is an automorgphism of G - cf Exercise 1.6.20, Section **??***). Deduce that x and gxg^{-1} have the same order for all x in G and that for any subset of A of G, $|A| = |gAg^{-1}|$ (here $gAg^{-1} = \{gag^{-1}\} = \{gag^{-1} | a \in A\}$).*

(note that each map is the permutation associated with g under the permutation representation). Let's denote the map $\delta_g : G \to G$.

- δ_g is a homomorphism, since given $x, y \in G$, we have $\delta_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \delta_g(x)\delta_g(y)$.
- δ_g is a bijection. I'll do a fancy proof. Consider the permutation representation of the bijection $\phi : G \to S_G$ (Recall that this is a group homomorphism). Then $\delta_g \circ \delta_{g^{-1}} = \phi(g)\phi(g^{-1}) = \phi(gg^{-1}) = \phi(1) = \delta_1 = \mathbf{1}$. Now swap g and g^{-1} in this proof and you have a two-sided inverse. THEREFORE, δ_g is an automorphism.
- The deductions regarding orders follow from 1.6.2.

1.7.18

Let H be a group acting on a set A. Prove that the relation $\sim$ on A defined by $a \sim b$ if and only if $a = hb$ for some $h \in H$ is an equivalence relation. (For each $x \in A$ the equivalence class of x under $\sim$ is called the orbit *of x under the action H. The orbits under the action of H partition the set A.)*

- Reflexive. $a = 1a$, so $a \sim a$ since $1 \in H$.
- Symmetric. Suppose $a \sim b$. Then $a = hb$ for some $h \in H$. But

$$\begin{aligned} & a = hb \\ \implies & b = h^{-1}a \\ \implies & b \sim a \text{Since } h^{-1} \in H \end{aligned}$$

- Transitive. Suppose $a \sim b$ and $b \sim c$. Then $\exists g, h \in H$ such that $a = hb$ and $b = gc$. But then $a = hb = h(gc) = (hg)c$. So $a \sim c$ since $hg \in G$

1.7.19

Let H be a subgroup (cf. Exercise 1.1.26 of section **??** *of the finite group G and let H act on G (here $A = G$) by left multiplication. Let $x \in G$ and let $\mathcal{O}$ be the orbit of x under the action of H. Prove that the map $H \to \mathcal{O}$ defined by $h \mapsto hx$ is a bijection (hence all orbits have cardinality $|H|$). From this and the preceding exercise deduce* Lagrange's Theorem:

Theorem 1 (Lagrange's Theorem)**.** *if G is a finite group and G is a subgroup of G then $|H|$ divides $|G|$.*

Denote the map by ϕ. Then

- Injectivity. Let $g, h \in H$. Then

$$\begin{aligned} & \phi(g) = \phi(h) \\ \implies & gx = hx \\ \implies & g = h && \text{Right cancellation in } G \end{aligned}$$

- Surjectivity. Let $y \in \mathcal{O}$. Then $y \sim x$. I.e. $y = hx$ for some $h \in H$. i.e. $y = \phi(h)$ for some $h \in H$. So ϕ is surjective

Hence, ϕ is a bijection. Let us prove Lagrange's Theorem.

Proof. Let $x \in G$. Denote the orbit of x under the action of H by $\mathcal{O}_x$. Since the orbits *partition* G, we must have $x_1, \ldots, x_n \in G$ such that

$$\sum_{i=1}^{n} |\mathcal{O}_{x_i}| = |G| \tag{24}$$

But There is a bijection from each $\mathcal{O}_{x_i}$ to H, therefore $|\mathcal{O}_{x_i}| = |H|$ for $i = 1, \ldots, n$. Hence, the equation above can be written as

$$\begin{aligned} & \sum_{i=1}^{n} |H| = |G| \\ \implies & n|H| = |G| \\ \implies & |H| \big| |G| \end{aligned}$$

□