

# Part I - Group Theory

December 22, 2025

## Contents

### 1 Introduction to Groups

#### 1.1 Basic Axioms and Examples

##### 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.  $(1 \star 2) \star 3 = \frac{1}{2} \star 3 = \frac{\frac{1}{2}+3}{3} = \frac{7}{6}$ . But  $1 \star (2 \star 3) = 1 \star \frac{2}{3} = \frac{1+\frac{2}{3}}{\frac{2}{3}} = \frac{5}{2}$

##### 1.1.3

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

### 1.1.4

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

### 1.1.5

$\bar{0}$  has no multiplicative inverse

### 1.1.9

- (a)
- $(a + b\sqrt{2}) + (c + d\sqrt{2}) = a + b\sqrt{2} + c + d\sqrt{2} = a + c + b\sqrt{2} + d\sqrt{2} = (a + c) + (b + d)\sqrt{2} \in G$ , 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.  $\square$

- 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.":

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

### 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

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

### 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

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

(c) Fuck my life bro. This is more annoying than 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

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

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

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

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

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

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

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

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

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

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

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

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

- $\Leftarrow$  : If  $A, B$  abelian, given  $(a, b), (c, d) \in A \times B$ , we have  $(a, b)(c, d) = (ac, bd) = (ca, db) = (c, d)(a, b)$
- $\Rightarrow$  : Now assume without loss of 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

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

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  $g = g^{-1} \Rightarrow g^2 = 1$ .

### 1.1.32

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

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

Where  $r \in \mathbb{Z}$ . 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  $1, x, \dots, x^{n-1}$  would comprise  $n > |G|$  distinct elements in  $G$ , which is impossible.

### 1.1.33

A lemma will help us here.

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

*Proof.*

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

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  $\Leftarrow$ , 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:

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

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.  $\square$

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

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

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

#### 1.4.5

- $\Leftarrow$  : 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:

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

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

$$f \mapsto \begin{pmatrix} f & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & f \end{pmatrix} \quad (3)$$

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 ??.

#### 1.4.7

The total number of  $2 \times 2$  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  $2 \times 2$  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. Analogous 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:

$$p^4 - (p^3 + p^2 - p) = p^4 - p^3 - p^2 + p \quad (4)$$

#### 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 top-rightmost entry is 1. Let  $q$  be the identity matrix except the bottom-leftmost entry is 1. The top-left entry of  $qp$  is 1 but the top-left 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  $F$

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

#### 1.4.10

(a)

$$\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 c_2 \\ 0 & c_1 c_2 \end{pmatrix} \quad (5)$$

Since  $a_1, a_2, c_1, c_2 \neq 0$ , we have  $a_1 a_2 \neq 0$  and  $c_1 c_2 \neq 0$ , 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

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

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

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

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

which is clearly in  $G$  because the diagonal entries are equal.

- Closure under inverses: Take ?? and make  $c = a$ , so we get

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

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

#### 1.4.11

(a)

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

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

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

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

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 ??, We need

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

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.

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

(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 ?? again,

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

Given an element of  $H(F)$ , we have 3 entries to input, and we 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

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

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

$$\begin{aligned}
a_1 &= 0 \\
a_n &= a_{n-1} + n - 1
\end{aligned}$$

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

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

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

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

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,

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

*Proof.* Base case: If  $n = 0$ , then this just reduces to the identity.

Now we suppose that

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

Then

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

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 ??,

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

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 ??, 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 ??, suppose

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

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.