

0.10 Groups and Permutations

Several structures in this chapter have quietly behaved alike. The invertible $n \times n$ matrices, the nonzero elements of a field, and the bijections of a set can each be combined, have an element that does nothing, and can be undone. This short section gives that common structure a name, proves its basic rules once, and introduces the permutations that the determinant in Chapter 7 is built from. We keep it brief: groups are a language for us here, not a subject.

0.10.1 Groups

Look at four situations side by side. In $\text{GL}_n(F)$, the set of invertible matrices in $M_n(F)$, we multiply matrices, $\mathbf{I}_n$ does nothing, and each $\mathbf{A}$ is undone by $\mathbf{A}^{-1}$ (Theorem 0.9.7). In a field F , we multiply nonzero elements, 1 does nothing, and each a is undone by a^{-1} . The four rotations of a square about its center (by $0^\circ, 90^\circ, 180^\circ, 270^\circ$) can be performed one after another, the rotation by 0° does nothing, and each rotation is undone by rotating back. The bijections $X \rightarrow X$ of a set are composed, id_X does nothing, and each is undone by its inverse function (Theorem 0.4.7). The objects differ completely, but the rules we use are the same three. So we give the pattern a name.

A group is a set with one way of combining elements, in which combining is associative, some element does nothing, and every element can be undone.

Definition 0.10.1. Group

A **group** is a set G together with a **binary operation** $G \times G \rightarrow G$, $(a, b) \mapsto ab$, such that:

- (G1) (**Associativity**) $(ab)c = a(bc)$ for all $a, b, c \in G$;
- (G2) (**Identity**) there is an element $e \in G$ with $ea = ae = a$ for every $a \in G$;
- (G3) (**Inverses**) for every $a \in G$ there is $b \in G$ with $ab = ba = e$, where e is the element of (G2).

The group is **abelian** if moreover $ab = ba$ for all $a, b \in G$.

In words: the operation is a function on pairs, so the combination of two elements of G lies in G again; this “closure” is built into the phrase “binary operation $G \times G \rightarrow G$ ”. (G1) lets us drop brackets. (G2) asks for an element that changes nothing, from **both** sides. (G3) asks that each element can be undone, again from both sides, back to that same e . When the operation is addition we write $a + b$, 0, and $-a$ instead of ab , e , and a^{-1} ; this notation is only used for abelian groups.

Example. Groups

Check that each of the following is a group, and decide which are abelian: $(\mathbb{Z}, +)$; $(F, +)$ and $(F \setminus \{0\}, \cdot)$ for a field F ; $\text{GL}_n(F)$ under matrix multiplication; the set S_n of bijections $\{1, \dots, n\} \rightarrow \{1, \dots, n\}$ under composition; and a one-element set $\{e\}$ with $ee = e$.

Solution. $(\mathbb{Z}, +)$: the sum of integers is an integer, addition is associative, 0 is an identity, and $-a$ undoes a . It is abelian. $(F, +)$ is a group for the same reasons, by the field axioms (Definition 0.7.1); it is abelian.

$(F \setminus \{0\}, \cdot)$: the product of two nonzero elements is nonzero by Theorem 0.7.1, so the operation lands in $F \setminus \{0\}$. Associativity and the identity $1 \neq 0$ come from the field axioms, and each $a \neq 0$ has an inverse a^{-1} , which is nonzero since $aa^{-1} = 1 \neq 0$. It is abelian.

$\text{GL}_n(F)$: by Theorem 0.9.7 (part 3), a product of invertible matrices is invertible, so the operation lands in $\text{GL}_n(F)$. Associativity holds by Theorem 0.9.4, $\mathbf{I}_n$ is invertible and is an identity, and $\mathbf{A}^{-1} \in \text{GL}_n(F)$ undoes $\mathbf{A}$ by part 2. For $n \geq 2$ it is **not** abelian: for $n = 2$, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$, while the product in the other order is $\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$. (Over $\mathbb{F}_2$ read 2 as 0; the two products still differ.) For $n \geq 3$, put these blocks in the top-left corner and 1's further down the diagonal. $\text{GL}_1(F)$ is just $F \setminus \{0\}$, and is abelian.

S_n : a composition of bijections is a bijection (Theorem 0.4.3), composition is associative (Theorem 0.4.2), id is an identity, and each bijection has an inverse function (Theorem 0.4.7), which is again a bijection. We will see below that S_n is not abelian for $n \geq 3$.

$\{e\}$: all three axioms reduce to $ee = e$. This **trivial group** is the degenerate case; it reappears as the smallest subgroup of every group.

Now nonexamples, each a minimal change of an example. Replace addition on $\mathbb{Z}$ by multiplication. The operation still lands in $\mathbb{Z}$, it is associative, and 1 is an identity. But (G3) fails: there is no integer b with $2b = 1$. So $(\mathbb{Z}, \cdot)$ is **not** a group. Similarly, replace $\text{GL}_n(F)$ by all of $M_n(F)$ under multiplication: (G1) and (G2) still hold with $\mathbf{I}_n$, but the zero matrix has no inverse, so (G3) fails. Keep $\mathbb{N}$ under $+$: the identity 0 is there, but 1 has no inverse in $\mathbb{N}$.

Warning. **The operation must land in the set.** $\text{GL}_n(F)$ under matrix **addition** is not a group: $\mathbf{I}_n$ and $-\mathbf{I}_n$ are invertible, but $\mathbf{I}_n + (-\mathbf{I}_n) = \mathbf{O}$ is not, so addition is not even a binary operation on $\text{GL}_n(F)$. Before checking (G1)–(G3), check that combining two elements of the set gives an element of the set.

The rules we proved separately for fields and for matrices follow from the axioms alone. It is worth proving them once:

Theorem 0.10.1. Basic properties of groups

Let G be a group and $a, b, c \in G$.

1. The identity element of G is unique.
2. The inverse of a is unique. We denote it by a^{-1} .
3. $(a^{-1})^{-1} = a$ and $(ab)^{-1} = b^{-1}a^{-1}$.
4. **(Cancellation)** If $ab = ac$, then $b = c$. If $ba = ca$, then $b = c$.

Proof. For 1, suppose e and e' both satisfy (G2). Then $e = ee'$, using that e' is an identity, and $ee' = e'$, using that e is one. Hence $e = e'$.

For 2, suppose b and b' both satisfy $ab = ba = e$ and $ab' = b'a = e$. By (G2) and (G1),

$$b = be = b(ab') = (ba)b' = eb' = b'.$$

For 3, the equations $aa^{-1} = a^{-1}a = e$ say that a is an inverse of a^{-1} , so $(a^{-1})^{-1} = a$ by part 2. Next, by (G1),

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e,$$

and similarly $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = e$. By part 2, $(ab)^{-1} = b^{-1}a^{-1}$.

For 4, suppose $ab = ac$. Multiplying on the left by a^{-1} and using (G1), $b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}(ac) = (a^{-1}a)c = c$. The second statement follows by multiplying on the right by a^{-1} . This proves the theorem. ■

These are the arguments of Theorem 0.9.7 with matrices erased. That is the point of the definition: a proof that uses only (G1)–(G3) holds in every group at once.

0.10.2 Subgroups

After a structure comes the substructure. The even integers sit inside $(\mathbb{Z}, +)$ and form a group on their own, with the same operation.

Definition 0.10.2. Subgroup

Let G be a group. A subset $H \subseteq G$ is a **subgroup** of G if $e \in H$, and $ab \in H$ and $a^{-1} \in H$ for all $a, b \in H$.

Then the operation of G restricts to a binary operation on H , and H is a group with it: (G1) holds in H because it holds in G , and (G2), (G3) hold because e and the inverses lie in H . In practice one checks a single condition:

Theorem 0.10.2. Subgroup test

Let G be a group and $H \subseteq G$. Then H is a subgroup of G if and only if $H \neq \emptyset$ and $ab^{-1} \in H$ for all $a, b \in H$.

Proof. ($\Rightarrow$) If H is a subgroup, then $e \in H$, so $H \neq \emptyset$. For $a, b \in H$ we have $b^{-1} \in H$, and then $ab^{-1} \in H$.

($\Leftarrow$) Suppose $H \neq \emptyset$ and $ab^{-1} \in H$ for all $a, b \in H$. Pick $h \in H$. Taking $a = b = h$ gives $e = hh^{-1} \in H$. For $b \in H$, taking $a = e$ gives $b^{-1} = eb^{-1} \in H$. For $a, b \in H$, we now know $b^{-1} \in H$, so $ab = a(b^{-1})^{-1} \in H$ by Theorem 0.10.1. Hence H is a subgroup. This proves the theorem. ■

For example, $2\mathbb{Z} = \{2k : k \in \mathbb{Z}\}$ is a subgroup of $(\mathbb{Z}, +)$. In additive notation the test reads “ $a - b \in H$ ”, and $2k - 2l = 2(k - l) \in 2\mathbb{Z}$, while $0 \in 2\mathbb{Z}$. By contrast $\mathbb{N} \subseteq \mathbb{Z}$ is nonempty and closed under $+$, but $0 - 1 = -1 \notin \mathbb{N}$: the test fails, because $\mathbb{N}$ lacks inverses. The set of odd integers fails more badly, since it does not contain 0. In $\text{GL}_n(F)$, the invertible diagonal matrices form a subgroup: $\mathbf{I}_n$ is one, and by Example (Some invertible matrices) the inverse of

$\text{diag}(d_1, \dots, d_n)$ is $\text{diag}(d_1^{-1}, \dots, d_n^{-1})$, so $\mathbf{D}\mathbf{E}^{-1}$ is again diagonal with nonzero diagonal entries. Every group G has the subgroups $\{e\}$ and G .

0.10.3 Homomorphisms

After objects come the maps between them that respect the structure.

Definition 0.10.3. Group homomorphism

Let G and H be groups. A function $\varphi: G \rightarrow H$ is a **homomorphism** if $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in G$. A **bijective** homomorphism is an **isomorphism**. The **kernel** of φ is $\ker \varphi = \{g \in G : \varphi(g) = e_H\}$, where e_H is the identity of H .

The product ab on the left is taken in G , and $\varphi(a)\varphi(b)$ on the right in H . For example, $F \setminus \{0\} \rightarrow \text{GL}_2(F)$, $a \mapsto \text{diag}(a, 1)$, is a homomorphism, since $\text{diag}(ab, 1) = \text{diag}(a, 1) \text{diag}(b, 1)$; its kernel is $\{1\}$. The map $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$, $a \mapsto [a]$, is a homomorphism of additive groups, because $[a + b] = [a] + [b]$ is exactly how addition on $\mathbb{Z}/n\mathbb{Z}$ was defined (Example (Addition modulo n is well defined)); its kernel is $n\mathbb{Z}$. On the other hand, $x \mapsto x + 1$ from $(\mathbb{R}, +)$ to itself is not a homomorphism: writing $\varphi(x) = x + 1$, we get $\varphi(0 + 0) = 1$ but $\varphi(0) + \varphi(0) = 2$.

Theorem 0.10.3. Basic properties of homomorphisms

Let $\varphi: G \rightarrow H$ be a homomorphism of groups. Then $\varphi(e_G) = e_H$, $\varphi(a^{-1}) = \varphi(a)^{-1}$ for every $a \in G$, and $\ker \varphi$ is a subgroup of G .

Proof. Since $\varphi(e_G)\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G) = \varphi(e_G)e_H$, cancellation (Theorem 0.10.1) gives $\varphi(e_G) = e_H$. Next, $\varphi(a)\varphi(a^{-1}) = \varphi(aa^{-1}) = \varphi(e_G) = e_H$, and similarly $\varphi(a^{-1})\varphi(a) = e_H$, so $\varphi(a^{-1}) = \varphi(a)^{-1}$ by uniqueness of inverses. Finally, $e_G \in \ker \varphi$, and for $a, b \in \ker \varphi$,

$$\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = e_H e_H^{-1} = e_H,$$

so $ab^{-1} \in \ker \varphi$. By Theorem 0.10.2, $\ker \varphi$ is a subgroup. This proves the theorem. ■

Two homomorphisms will matter later: the determinant $\text{GL}_n(F) \rightarrow F \setminus \{0\}$ and the sign $S_n \rightarrow \{1, -1\}$, both in Chapter 7. Linear maps in Chapter 2 are, among other things, homomorphisms of additive groups, and their kernels will be one of our main tools.

0.10.4 Permutations

A **permutation** of $\{1, \dots, n\}$ is a bijection $\{1, \dots, n\} \rightarrow \{1, \dots, n\}$, and S_n is the group of all of them, the **symmetric group**. It has $n!$ elements: there are n choices for $\sigma(1)$, then $n - 1$ for $\sigma(2)$, and so on.

A permutation σ can be written in **two-line notation**, with $\sigma(i)$ below i . A more compact notation lists what happens along a loop. For **distinct** $i_1, \dots, i_k \in \{1, \dots, n\}$, the **cycle** $(i_1 i_2 \cdots i_k)$ is the permutation sending

$$i_1 \mapsto i_2 \mapsto \cdots \mapsto i_k \mapsto i_1$$

and fixing every other element. A cycle of length 2 is a **transposition**: $(i j)$ swaps i and j .

The same cycle can be written starting at any of its entries: $(1\ 2\ 3) = (2\ 3\ 1) = (3\ 1\ 2)$, but $(1\ 3\ 2)$ is different.

The product $\sigma\tau$ in S_n means the composition $\sigma \circ \tau$: **first apply τ , then σ** . So products of cycles are read **from right to left**.

Example. Computing with cycles

In S_3 , compute $(1\ 3)(1\ 2)$ and $(1\ 2)(1\ 3)$. In S_5 , write $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}$ (two-line notation) as a product of cycles.

Solution. For $(1\ 3)(1\ 2)$, follow each element through $(1\ 2)$ first, then $(1\ 3)$: $1 \mapsto 2 \mapsto 2$, $2 \mapsto 1 \mapsto 3$, $3 \mapsto 3 \mapsto 1$. So $(1\ 3)(1\ 2) = (1\ 2\ 3)$. For $(1\ 2)(1\ 3)$: $1 \mapsto 3 \mapsto 3$, $3 \mapsto 1 \mapsto 2$, $2 \mapsto 2 \mapsto 1$. So $(1\ 2)(1\ 3) = (1\ 3\ 2)$. The two products differ, so S_3 is not abelian; the same two transpositions show that S_n is not abelian for every $n \geq 3$.

For σ , start at 1 and follow: $1 \mapsto 3 \mapsto 1$, a loop $(1\ 3)$. The smallest element not yet used is 2: $2 \mapsto 5 \mapsto 4 \mapsto 2$, a loop $(2\ 5\ 4)$. Every element is now used, so $\sigma = (1\ 3)(2\ 5\ 4)$. These two cycles move disjoint sets of elements, so they can be applied in either order.

Warning. Mind the order. $\sigma\tau$ applies τ first, exactly as for functions, and as for matrices: $(\mathbf{A}\mathbf{B})\mathbf{x} = \mathbf{A}(\mathbf{B}\mathbf{x})$ applies $\mathbf{B}$ first. Reading a product of cycles from left to right gives the wrong answer, as the two different products $(1\ 3)(1\ 2) \neq (1\ 2)(1\ 3)$ above show.

Quick check. Compute $(1\ 2\ 3)(1\ 2)$ in S_3 .

Solution. Apply $(1\ 2)$ first: $1 \mapsto 2 \mapsto 3$, $2 \mapsto 1 \mapsto 2$, $3 \mapsto 3 \mapsto 1$. So 1 and 3 are swapped and 2 is fixed: $(1\ 2\ 3)(1\ 2) = (1\ 3)$.

The example showed $(1\ 2\ 3) = (1\ 3)(1\ 2)$: a 3-cycle is a product of transpositions. Every permutation is, and the proof is a model induction on n .

Theorem 0.10.4. Transpositions generate S_n

Let $n \geq 2$. Every permutation in S_n is a product of transpositions.

Idea. Induction on n : what is the smaller object inside a permutation of $n + 1$ elements? If σ fixes $n + 1$, it is really a permutation of $\{1, \dots, n\}$. If not, one transposition repairs that: swap $\sigma(n + 1)$ back to $n + 1$. The result fixes $n + 1$, so the induction hypothesis applies, and we undo the swap.

Proof. We use induction on $n \geq 2$ (Theorem 0.2.7). For $n = 2$, $S_2 = \{\text{id}, (1\ 2)\}$, and $\text{id} = (1\ 2)(1\ 2)$.

Suppose every permutation in S_n is a product of transpositions, and let $\sigma \in S_{n+1}$.

Case 1. $\sigma(n+1) = n+1$. Since σ is injective, $\sigma(i) \neq n+1$ for $i \leq n$, so σ restricts to a function $\sigma': \{1, \dots, n\} \rightarrow \{1, \dots, n\}$. It is injective because σ is, and hence bijective by Theorem 0.4.9. By the induction hypothesis, $\sigma' = \tau_1 \cdots \tau_r$ with transpositions $\tau_j \in S_n$. Regard each τ_j as a transposition in S_{n+1} fixing $n+1$. Then $\tau_1 \cdots \tau_r$ agrees with $\sigma' = \sigma$ on $\{1, \dots, n\}$ and fixes $n+1$, as σ does. Hence $\sigma = \tau_1 \cdots \tau_r$.

Case 2. $\sigma(n+1) = k \neq n+1$. Let $\tau = (k\ n+1)$. Then $(\tau\sigma)(n+1) = \tau(k) = n+1$, so by Case 1, $\tau\sigma = \tau_1 \cdots \tau_r$ for some transpositions τ_j . Since $\tau\tau = \text{id}$, multiplying on the left by τ gives $\sigma = \tau\tau_1 \cdots \tau_r$, a product of transpositions.

This completes the induction, and proves the theorem. ■

The product is not unique: $(1\ 2\ 3) = (1\ 3)(1\ 2) = (1\ 2)(2\ 3)$, and one can always insert $(1\ 2)(1\ 2) = \text{id}$. What turns out to be unique is whether the number of transpositions is even or odd. That fact defines the **sign** of a permutation, which we do not define here; it is the subject of Chapter 7, where it builds the determinant.

0.10.5 Exercises

0.10.5.1 A. Check your understanding

Exercise. A1

- (a) State the three axioms of a group.
- (b) Is $\mathbb{Z}$ with the operation $(a, b) \mapsto a - b$ a group? Justify your answer.
- (c) Determine whether the following statement is true: “in every group, $(ab)^{-1} = a^{-1}b^{-1}$.” Justify your answer.
- (d) Compute $(1\ 3)(1\ 2\ 3)$ in S_3 .
- (e) Explain why $\{\mathbf{A} \in M_2(\mathbb{R}) : \mathbf{A} \text{ is not invertible}\}$ is **not** a subgroup of $\text{GL}_2(\mathbb{R})$.

Solution.

- (a) (G1) $(ab)c = a(bc)$ for all a, b, c ; (G2) there is e with $ea = ae = a$ for all a ; (G3) for every a there is b with $ab = ba = e$. The operation must be a binary operation $G \times G \rightarrow G$.
- (b) No. Associativity fails: $(1 - 1) - 1 = -1$, but $1 - (1 - 1) = 1$.
- (c) False. By Theorem 0.10.1, $(ab)^{-1} = b^{-1}a^{-1}$, and this can differ from $a^{-1}b^{-1}$. In S_3 take $a = (1\ 2)$ and $b = (1\ 3)$, which are their own inverses. By Example (Computing with cycles), $ab = (1\ 3\ 2)$, whose inverse is $(1\ 2\ 3)$, while $a^{-1}b^{-1} = ab = (1\ 3\ 2)$. The statement is true in abelian groups.
- (d) Apply $(1\ 2\ 3)$ first: $1 \mapsto 2 \mapsto 2$, $2 \mapsto 3 \mapsto 1$, $3 \mapsto 1 \mapsto 3$. Hence $(1\ 3)(1\ 2\ 3) = (1\ 2)$.
- (e) It is not even a subset of $\text{GL}_2(\mathbb{R})$, since its elements are not invertible; for instance it

does not contain the identity $\mathbf{I}_2$.

0.10.5.2 B. Practice

Exercise. B1: The table of S_3

List the six elements of S_3 in cycle notation and write out the table whose entry in row x and column y is xy . Hence find all elements $x \in S_3$ with $x^2 = \text{id}$, and all x that commute with every element of S_3 .

Solution. The elements are $\text{id}, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)$. Computing each product right to left, as in [Example \(Computing with cycles\)](#), the entry in row x , column y is xy :

xy	id	$(1\ 2)$	$(1\ 3)$	$(2\ 3)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$
id	id	$(1\ 2)$	$(1\ 3)$	$(2\ 3)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$
$(1\ 2)$	$(1\ 2)$	id	$(1\ 3\ 2)$	$(1\ 2\ 3)$	$(2\ 3)$	$(1\ 3)$
$(1\ 3)$	$(1\ 3)$	$(1\ 2\ 3)$	id	$(1\ 3\ 2)$	$(1\ 2)$	$(2\ 3)$
$(2\ 3)$	$(2\ 3)$	$(1\ 3\ 2)$	$(1\ 2\ 3)$	id	$(1\ 3)$	$(1\ 2)$
$(1\ 2\ 3)$	$(1\ 2\ 3)$	$(1\ 3)$	$(2\ 3)$	$(1\ 2)$	$(1\ 3\ 2)$	id
$(1\ 3\ 2)$	$(1\ 3\ 2)$	$(2\ 3)$	$(1\ 2)$	$(1\ 3)$	id	$(1\ 2\ 3)$

For example, the entry in row $(1\ 2)$, column $(2\ 3)$ is $(1\ 2)(2\ 3)$: $1 \mapsto 1 \mapsto 2$, $2 \mapsto 3 \mapsto 3$, $3 \mapsto 2 \mapsto 1$, which is $(1\ 2\ 3)$.

Reading the diagonal, $x^2 = \text{id}$ exactly for $x = \text{id}, (1\ 2), (1\ 3), (2\ 3)$. An element x commutes with every element exactly when row x equals column x . This holds for id . It fails for every other element: $(1\ 2)(1\ 3) = (1\ 3\ 2) \neq (1\ 2\ 3) = (1\ 3)(1\ 2)$ handles $(1\ 2)$ and $(1\ 3)$; $(2\ 3)(1\ 2) = (1\ 3\ 2) \neq (1\ 2\ 3) = (1\ 2)(2\ 3)$ handles $(2\ 3)$; and $(1\ 2\ 3)(1\ 2) = (1\ 3) \neq (2\ 3) = (1\ 2)(1\ 2\ 3)$ handles $(1\ 2\ 3)$ and, since $(1\ 3\ 2)(1\ 2) = (2\ 3) \neq (1\ 3) = (1\ 2)(1\ 3\ 2)$, also $(1\ 3\ 2)$. Hence only id commutes with everything.

Exercise. B2: Invertible upper triangular matrices

Let F be a field and $T = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in F, a \neq 0, d \neq 0 \right\}$.

- Prove that T is a subgroup of $\text{GL}_2(F)$.
- For which fields F is T abelian? Justify your answer.

Solution.

- Let $\mathbf{X} = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in T$. Since $a, d \neq 0$, $ad - b \cdot 0 = ad \neq 0$ by Theorem 0.7.1, so $\mathbf{X}$ is invertible by Theorem 0.9.8. Hence $T \subseteq \text{GL}_2(F)$, and $T \neq \emptyset$ since $\mathbf{I}_2 \in T$. Now let $\mathbf{Y} = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} \in T$. By Theorem 0.9.8, $\mathbf{Y}^{-1} = (a'd')^{-1} \begin{pmatrix} d' & -b' \\ 0 & a' \end{pmatrix} = \begin{pmatrix} a'^{-1} & -b'(a'd')^{-1} \\ 0 & d'^{-1} \end{pmatrix}$.

Therefore

$$\mathbf{XY}^{-1} = \begin{pmatrix} aa'^{-1} & -ab'(a'd')^{-1} + bd'^{-1} \\ 0 & dd'^{-1} \end{pmatrix},$$

whose $(2, 1)$ -entry is 0 and whose diagonal entries aa'^{-1} , dd'^{-1} are nonzero by Theorem 0.7.1. So $\mathbf{XY}^{-1} \in T$, and T is a subgroup by Theorem 0.10.2.

- (b) It depends on the field. *Case 1:* F has an element c with $c \neq 0$ and $c \neq 1$ (for example $c = 2$ in $\mathbb{R}$ or $\mathbb{F}_3$). Let $\mathbf{X} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\mathbf{Y} = \text{diag}(1, c)$, both in T . Then $\mathbf{XY} = \begin{pmatrix} 1 & c \\ 0 & c \end{pmatrix}$ and $\mathbf{YX} = \begin{pmatrix} 1 & 1 \\ 0 & c \end{pmatrix}$, which differ in the $(1, 2)$ -entry since $c \neq 1$. So T is **not** abelian. *Case 2:* $F = \{0, 1\}$, that is, $F = \mathbb{F}_2$. Then $a = d = 1$ is forced, so $T = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{F}_2 \right\}$, and $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b + b' \\ 0 & 1 \end{pmatrix}$ is symmetric in b, b' . So T is abelian over $\mathbb{F}_2$, and over every other field it is not.

Exercise. B3: The exponential is an isomorphism

Let $\mathbb{R}_{>0} = \{x \in \mathbb{R} : x > 0\}$. Show that $(\mathbb{R}_{>0}, \cdot)$ is a group, and that $\exp: (\mathbb{R}, +) \rightarrow (\mathbb{R}_{>0}, \cdot)$, $x \mapsto e^x$, is an isomorphism. What is its kernel? You may use the familiar facts $e^{x+y} = e^x e^y$, $e^x > 0$, and that $\ln: \mathbb{R}_{>0} \rightarrow \mathbb{R}$ satisfies $\ln(e^x) = x$ and $e^{\ln y} = y$.

Solution. A product of positive reals is positive, so multiplication is a binary operation on $\mathbb{R}_{>0}$. It is associative, $1 \in \mathbb{R}_{>0}$ is an identity, and for $y > 0$ the inverse $1/y$ is positive. Hence $(\mathbb{R}_{>0}, \cdot)$ is a group.

Since $e^x > 0$, $\exp$ maps $\mathbb{R}$ into $\mathbb{R}_{>0}$, and $e^{x+y} = e^x e^y$ says exactly that it is a homomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}_{>0}, \cdot)$. The function $\ln$ satisfies $\ln \circ \exp = \text{id}_{\mathbb{R}}$ and $\exp \circ \ln = \text{id}_{\mathbb{R}_{>0}}$, so $\exp$ is bijective by Theorem 0.4.7. Hence $\exp$ is an isomorphism. Its kernel is $\{x \in \mathbb{R} : e^x = 1\} = \{0\}$, since $\exp$ is injective and $e^0 = 1$.

0.10.5.3 C. Going deeper

Exercise. C1: Every element its own inverse

- (a) Let G be a group in which $g^2 = gg = e$ for every $g \in G$. Prove that G is abelian.
 (b) Show that $(M_2(\mathbb{F}_2), +)$ is an example of such a group, written additively.

Solution.

- (a) Let $a, b \in G$. The hypothesis $gg = e$ says that every g is its own inverse, by uniqueness of inverses (Theorem 0.10.1). Applying this to ab , a , and b , and using Theorem 0.10.1,

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba.$$

Hence G is abelian.

- (b) $(M_2(\mathbb{F}_2), +)$ is a group by Theorem 0.9.1: addition is associative, $\mathbf{0}$ is an identity,

and $-\mathbf{A}$ is an inverse. In additive notation, “ $g^2 = e$ ” reads $\mathbf{A} + \mathbf{A} = \mathbf{O}$, and indeed $(\mathbf{A} + \mathbf{A})_{ij} = a_{ij} + a_{ij} = (1 + 1)a_{ij} = 0$ in $\mathbb{F}_2$. (This group is abelian anyway, consistent with (a).)

Exercise. C2: The order of a product of disjoint cycles

The **order** of $\sigma \in S_n$ is the smallest integer $m \geq 1$ with $\sigma^m = \text{id}$, where σ^m is the product of m copies of σ . Two cycles are **disjoint** if no element appears in both.

- (a) Let $\sigma = (i_1 \cdots i_k)$ be a k -cycle. Prove that $\sigma^m = \text{id}$ if and only if k divides m . Deduce that σ has order k .
- (b) Prove that disjoint cycles σ and τ commute, and deduce $(\sigma\tau)^m = \sigma^m\tau^m$ for all $m \geq 1$.
- (c) Let σ be a k -cycle and τ an l -cycle, disjoint. Prove that $\sigma\tau$ has order $\text{lcm}(k, l)$.
- (d) Find the order of $(1\ 2)(3\ 4\ 5) \in S_5$.

Hint for (c): σ^m moves only elements that appear in σ .

Solution.

- (a) Index the entries of the cycle modulo k , so $\sigma(i_j) = i_{j+1}$ with $i_{k+1} = i_1$. By induction on m , $\sigma^m(i_j) = i_{j+m}$, indices taken modulo k , and σ^m fixes every element not in the cycle. Hence $\sigma^m = \text{id}$ if and only if $i_{j+m} = i_j$ for all j . Since $i_1, \dots, i_k$ are distinct, this holds if and only if $j + m \equiv j \pmod{k}$, that is, $k \mid m$. The smallest $m \geq 1$ with $k \mid m$ is k , so σ has order k .
- (b) Let A and B be the disjoint sets of elements appearing in σ and τ . Note that σ maps A to A and fixes everything outside A , and τ does the same with B . Let $i \in \{1, \dots, n\}$. If $i \in A$, then $i \notin B$ and $\sigma(i) \in A$, so $\sigma(i) \notin B$; hence $\sigma\tau(i) = \sigma(i) = \tau\sigma(i)$. The case $i \in B$ is the same with the roles swapped. If $i \notin A \cup B$, both sides give i . Hence $\sigma\tau = \tau\sigma$. Then $(\sigma\tau)^m = \sigma^m\tau^m$ follows by induction on m : $(\sigma\tau)^{m+1} = \sigma^m\tau^m\sigma\tau = \sigma^m\sigma\tau^m\tau = \sigma^{m+1}\tau^{m+1}$, moving σ past τ one factor at a time, which is allowed because they commute.
- (c) By (b), $(\sigma\tau)^m = \sigma^m\tau^m$. We claim this is id if and only if $\sigma^m = \text{id}$ and $\tau^m = \text{id}$. One direction is clear. Conversely, suppose $\sigma^m\tau^m = \text{id}$, and let $i \in A$. Then $i \notin B$, so $\tau^m(i) = i$ by the hint, and $\sigma^m(i) = \sigma^m\tau^m(i) = i$. Since σ^m also fixes every $i \notin A$, $\sigma^m = \text{id}$, and then $\tau^m = \sigma^m\tau^m = \text{id}$ as well. By (a), $(\sigma\tau)^m = \text{id}$ if and only if $k \mid m$ and $l \mid m$. The smallest such $m \geq 1$ is $\text{lcm}(k, l)$, which is therefore the order of $\sigma\tau$.
- (d) $(1\ 2)$ and $(3\ 4\ 5)$ are disjoint cycles of lengths 2 and 3, so by (c) the order is $\text{lcm}(2, 3) = 6$.