Examples in abstract algebra

Per Alexandersson

Introduction

Here is a collection of problems regarding rings, groups and permutations. The solutions can be found in the end. My email is `per.w.alexandersson@gmail.com`, where I happily receive comments and suggestions.

Version: 13th November 2020,14:07

GROUPS, RINGS AND FIELDS are sets with different levels of extra structure. All fields are rings, and all rings are also groups. More structure means more axioms to remember, but the additional structure makes it less abstract.

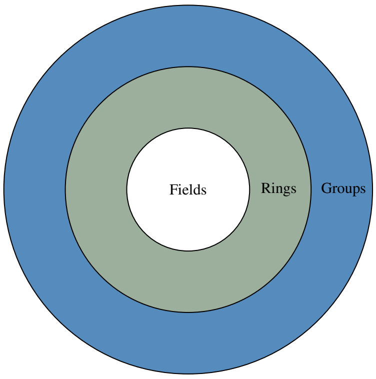


Figure 1: How to view groups, rings and fields.

If you are familiar with vector spaces, you have already seen some algebraic structures. The set is a set of vectors and the extra structure comes from the and the operators: addition of vectors, multiplication by scalar, scalar product and cross product.

It can be helpful for computer scientists to think about algebraic structures consisting of two pieces: *data* and *operators*, similar to how classes in object-oriented programming consist of data fields and methods. The data in our cases are elements in some set (numbers, matrices, polynomials), and operators which produce new members in this set.

Properties of rings

Definition 1 (Ring)**.** A *ring* $(R, +, *)$ is a set R equipped with two binary operator such that the following holds.

For the $+$ operator:

1. (CLOSEDNESS) $a + b \in R$ for all $a, b \in R$.
2. (ASSOCIATIVITY) $a + (b + c) = (a + b) + c$ for all $a, b, c \in R$.
3. (COMMUTATIVITY) $a + b = b + a$ for all $a, b \in R$.
4. (EXISTENCE OF IDENTITY) There is some $0 \in R$, such that $0 + a = a + 0 = a$ for all $a \in R$.
5. (EXISTENCE OF INVERSES) For every $a \in R$, there is a $-a \in R$ such that $a + (-a) = 0$.

For the $*$ operator:

1. (CLOSEDNESS) $a * b \in R$ for all $a, b \in R$.
2. (ASSOCIATIVITY) $a * (b * c) = (a * b) * c$ for all $a, b, c \in R$.
3. (EXISTENCE OF IDENTITY) There is some $1 \in R$, such that $1 * a = a * 1 = a$ for all $a \in R$.

Distributive law:

$$a * (b + c) = a * b + a * c \qquad (b + c) * a = b * a + c * a \qquad \text{for all } a, b, c \in R.$$

We usually refer to a ring[1] by simply specifying R when the two operators $+$ and $*$ are clear from the context. For example, if $R = \mathbb{R}$, it is understood that we use the addition and multiplication of real numbers. Moreover, we commonly write ab instead of $a * b$.

Examples of rings

Below we list some of the common rings. Here, K can be any of the sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$.

- The sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are all rings under the usual addition and multiplication.
- $M_{n,n}(K)$, the set of $n \times n$-matrices with entries in K.
- $K[x]$, the set of polynomials in one variable with coefficients in K.
- $K[x, y]$, the set of two-variable polynomials with coefficients in K.

Subrings

Definition 2. A set $R' \subseteq R$ is said to be a *subring* of $R = (R, +, *)$, if $(R', +, *)$ is a ring.

Suppose we are given a subset $R' \subseteq R$ in some ring. Then it suffices to verify that $0, 1 \in R'$, and that R' is closed under addition, multiplication and additive inverses[2].

Example 3. The set of polynomials $P \in \mathbb{Q}[x, y]$ which are symmetric is a subring of $\mathbb{Q}[x, y]$. The polynomial P is symmetric if $P(x, y) = P(y, x)$. For example,

$$x + y, \quad x^2y^2, \quad 3xy + 5x^2 + 5y^2 - 2, \quad \text{and } 43$$

are all symmetric polynomials, while $x + 7y$ is not symmetric.

Properties of fields

By adding some additional requirements to the set of properties for rings, we get the definition of a field. We now demand that multiplication is commutative, and that every non-zero element in the field has a multiplicative inverse.

Definition 4 (Field)**.** A *field* $(K, +, *)$ is a set K equipped with two binary operator such that the following holds.

The letter K is traditional notation, and comes from the German word Körper, meaning roughly *body* in the sense of *organization*.

For the $+$ operator:

1. (Closedness) $a + b \in K$ for all $a, b \in K$.
2. (Associativity) $a + (b + c) = (a + b) + c$ for all $a, b, c \in K$.
3. (Commutativity) $a + b = b + a$ for all $a, b \in K$.
4. (Existence of identity) There is some $0 \in K$, such that $0 + a = a + 0 = a$ for all $a \in K$.

[1] That is, R stands for both the set and the ring.

[2] That is, it is closed under “minus”

5. (Existence of inverses) For every $a \in K$, there is a $-a \in K$ such that $a + (-a) = 0$.

For the $*$ operator:

1. (Closedness) $a * b \in K$ for all $a, b \in K$.

2. (Associativity) $a * (b * c) = (a * b) * c$ for all $a, b, c \in K$.

3. (Commutativity) $a * b = b * a$ for all $a, b \in K$.

4. (Existence of identity) There is some $1 \in K$, such that $1 * a = a * 1 = a$ for all $a \in K$.

5. (Existence of inverses) For every non-zero $a \in K$, there is a $a^{-1} \in K$ such that $a * a^{-1} = 1$.

Distributive law:

$$a*(b+c) = a*b+a*c \qquad (b+c)*a = b*a+c*a \qquad \text{for all } a, b, c \in K.$$

Examples of fields

The sets $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are all fields. Moreover, whenever p is a prime number, $\mathbb{Z}_p$ is a field.

Properties of groups

Definition 5 (Group)**.** A *group* $(G, *)$ is a set G equipped with a binary operator such that the following holds:

1. (Closedness)

   $a * b \in G$ for all $a, b \in G$.

2. (Associativity)

   $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$.

3. (Existence of identity)

   There is some $e \in G$, such that $e * a = a * e = a$ for all $a \in G$.

4. (Existence of inverses)

   For every $a \in G$, there is an $a' \in G$ such that $a * a' = a' * a = e$.

When it is clear from the context, we usually write just ab instead of $a * b$. The group operator is usually referred to as *group multiplication* or simply multiplication.

One can show that the identity element is unique, and that every element a has a unique inverse. The inverse of a is usually denoted a^{-1}, but it depend on the context — for example, if we use the symbol '+' as group operator, then $-a$ is used to denote the inverse of a.

Examples of groups

- $(\mathbb{Z}, +)$, the set of integers with usual addition.
- $(\mathbb{R}_{>0}, \times)$, the positive real numbers with the usual multiplication.
- $(\mathbb{Z}_n, +)$, modular arithmetic mod n under modular addition.
- $(\mathbb{Z}_n^\times, \times)$, the set of invertible elements in $\mathbb{Z}_n$ under modular multiplication.

□ $GL_n(\mathbb{R})$, the set of invertible $n \times n$-matrices under matrix multiplication.

This is called the General Linear group.

□ $SL_n(\mathbb{R})$, the set of $n \times n$-matrices with determinant 1, under matrix multiplication.

This is called the Special Linear group.

□ S_n, the set of permutations on $1, \dots, n$ under composition (seen as bijections).

□ $Aut(P)$, the set of functions[3] that send a polygon P to itself, under composition.

Definition 6 (Subgroup). If G is a group, we say that a subset $H \subseteq G$ is a *subgroup* if H is itself a group under the same multiplication as in G. It is enough to verify that H is a subset of G such that H is closed under multiplication and taking inverses.

Every group G always have G itself and $\{e\}$ as subgroups. These are called *trivial* subgroups of G.

Definition 7 (Abelian group). A group is Abelian[4] if $ab = ba$ for all a, b in G.

In other words, a group is Abelian if the order of multiplication does not matter. The second list of examples above (marked □) are non-Abelian.

Definition 8 (Cyclic group). A group G is cyclic, if there is some $g \in G$ such that

$$G = \{\dots, g^{-2}, g^{-1}, e, g, g^2, \dots\}.$$

EVERY ELEMENT IN a group *generates* a cyclic subgroup. Furthermore, every cyclic group is Abelian.

Sometimes, the notation $\langle g \rangle$ is used to denote the cyclic group generated by g.

Theorem 9. *Every subgroup of a cyclic group is cyclic.*

Proof. Suppose G is a finite[5] cyclic group, and let H be a subgroup. Then H is of the form

$$H = \{e, g^{a_1}, g^{a_2}, \dots, g^{a_k}\}$$

for some list of integers $L = \{a_1, \dots, a_k\}$. Since H is a subgroup it is closed under group operations. This means that L is closed under addition and subtraction, which implies that it is closed under linear combinations. In particular, we must have that $d =$

[3] Some details are missing here, we need to specify what we mean by such functions.

[4] Also known as commutative

[5] One needs to adapt the proof slightly in the non-finite case

$\gcd(a_1, a_2, \dots, a_k)$ is in L, since we can produce d via Euclid's algorithm.

Therefore, $g^d \in H$ and each g^{a_i} is a power of g^d. This means that g^d generates H and H is therefore a cyclic group. □

Theorem 10 (Lagrange)**.** *Let G be a finite group and H be a subgroup of G. Then $|H|$ divides $|G|$.*

Lagrange's theorem is very powerful, as it puts lots of restrictions on the group G.

Theorem 11. *Let G be a finite group where $|G|$ is a prime number. Then G is cyclic.*

Proof. Take some $g \in G$ which is not the identity element, and consider the cyclic subgroup H it generates. In other words

$$H = \{\dots, g^{-1}, e, g, g^2, g^3, \dots\}.$$

By construction, $|H| \geq 2$ since we chose $g \neq e$. Lagrange's theorem tells us that $|H|$ divides $|G|$, but since $|G|$ is a prime number, the only possibility is if $|H| = |G|$ in which case $H = G$.

In conclusion, G is cyclic and every element in G which is not the identity element is a generator for G. □

We can construct bigger groups from smaller ones by *direct product*. Suppose G and H are groups. Define

$$G \times H := \{(g, h) : g \in G \text{ and } h \in H\}.$$

The set $G \times H$ is then a group under the group operation

What is the neutral element?

$$(g_1, h_1) * (g_2, h_h) = (g_1 * g_2, h_1 * h_2).$$

That is, we simply perform the operations in G and H respectively, element-wise. Note that if G and H are finite then $|G \times H| = |G| \times |H|$. When G and H are Abelian groups, the symbol $\oplus$ is used instead of $\times$ to denote direct product.

Notice here how we in mathematics use the same symbol, ×, to denote very different operations. We use it both as a binary operation on sets (Cartesian product), and the usual multiplication of integers.

Background on permutations

We can describe a permutation $\pi \in \mathrm{S}_n$ in several ways, the most popular ones being the *one-line notation* and the *cycle notation.*

E.g., $\pi = [4, 2, 5, 1, 3]$ is $(1, 4)(2)(3, 5)$ in cycle notation. We might be sloppy and omit the commas and just write $(14)(2)(35)$ when there is no room for confusion.

The group operation in S_n is composition of bijections. This gives us rules for how to multiply and take inverses of permutations. For example,

$$[4, 1, 5, 3, 2] \circ [3, 4, 5, 2, 1] = [5, 3, 2, 1, 4], \qquad [4, 1, 2, 3]^{-1} = [2, 3, 4, 1].$$

The *order* of a permutation π is defined in the same way as for elements in a general group: it is the smallest positive integer k, such that $\pi^k = e$. By analyzing the cycle structure, it is not hard to obtain the following result:

Theorem 12. *Let π be a permutation, where c_1, $c_2, \dots, c_\ell$, are the lengths of the cycles in the cycle form. Then*

$$\operatorname{order}(\pi) = \operatorname{lcm}(c_1, c_2, \dots, c_\ell).$$

For example, $\operatorname{order}((154)(2637)(89)) = 6$.

Given a permutation $\pi \in \mathrm{S}_n$, we define the number of inversions as

$$\operatorname{inv}(\pi) = |\{(i,j) : 1 \leq i < j \leq n \text{ such that } \pi(i) > \pi(j)\}|.$$

That is, it is the number of *pairs* of entries in π, where the first entry is greater than the second entry. The only permutation with no inversions is the identity permutation e. A permutation is said to be *even* if it has an even number of inversions, and *odd* if it has an odd number of inversions.

Transpositions are special permutations that only interchange two entries. We usually express them in cycle form as a single 2-cycle. A *simple transposition* interchanges adjacent entries. Multiplying a permutation with a simple transposition either increases or decreases the number of inversions by exactly 1.

E.g., in S_4, we have $(2,4) = [1,4,2,3]$.

Theorem 13. *Let $\pi \in \mathrm{S}_n$ and let $c(\pi)$ denote the number of cycles of π. Then shortest factorization of π into*

- simple transpositions *requires* $\operatorname{inv}(\pi)$ *simple transpositions, and*
- transpositions *requires* $n - c(\pi)$ *transpositions.*

A very important theorem is the following, which relates inversions with factorizations of a permutation into transpositions:

What is the relation with inversions?

Theorem 14. *Let $\pi = \tau_1 \cdots \tau_k$ be a factorization into transpositions. Then k is even if and only if π is an even permutation.*

In other words, we might have different factorizations of a permutation, but if the permutation is even, then all of the factorizations must consist of an even number of transpositions.

Ring problems

Modular arithmetic

Problem. 1
Find the inverse of 2 in $\mathbb{Z}_{11}$.

Problem. 2
Find the inverse of 5 in $\mathbb{Z}_{13}$.

Problem. 3
Does 3 have a multiplicative inverse in $\mathbb{Z}_9$?

Problem. 4

Is it possible that $149291^2 = 22287802671$? Can you compute the remainder on both sides when dividing by some p?

Problem. 5

Calculate the remainder when 2^{1026} is divided by 17.

Problem. 6

Can we solve $2x \equiv_6 4$? What about $2x \equiv_6 5$?

Problem. 7

Solve $5x \equiv_{11} 4$, (or equivalently, solve $5x = 4$ in $\mathbb{Z}_{11}$).

Problem. 8

In $\mathbb{Z}_6$, solve the system

$$\begin{cases} x + 2y &= 3 \\ 2x + y &= 3. \end{cases}$$

Problem. 9

In $\mathbb{Z}_{11}$, solve the system

$$\begin{cases} 3x + 3y &= 1 \\ 4x - y &= 2. \end{cases}$$

Problem. 10

In $\mathbb{Z}_{19}$, solve the system

$$\begin{cases} 3x + 4y &= 1 \\ 2x - y &= 2. \end{cases}$$

Additional problems on rings

Problem. 11

Let $R \subseteq \mathbb{Q}[x]$ be the set of all polynomials which are even[6] functions. Show that R is a subring of $\mathbb{Q}[x]$.

Show that the set of polynomials which are odd[7] functions is *not* a subring.

Problem. 12

Let R' and R'' both be subrings of some ring R. Show that the intersection $R' \cap R''$ is also a subring of R.

Problem. 13

Show that $\mathbb{Z}$ does not contain a smaller set which is a subring of Z.

[6] A function f is even if $f(-x) = f(x)$.

[7] A function f is odd if $f(-x) = -f(x)$.

Problem. 14

Let R be the set of formal $\mathbb{Z}$-linear combinations of words in the alphabet $\{\mathtt{a}, \mathtt{b}\}$. We also allow the empty word to be in R. That is, elements in R look something like the four following examples:

Yes, there are several technical terms in this definition, I hope that the examples are enough to explain what is meant. The $\mathbb{Z}$ in $\mathbb{Z}$-linear simply means that the coefficients are integers.

$$2\mathtt{aab} - 5\mathtt{ba} + 7\mathtt{b} + 9, \quad \mathtt{a} + \mathtt{b}, \quad 2, \quad -4\mathtt{abab}.$$

Addition of such expressions is what you would expect. For example,

$$(2\mathtt{aab} + 4\mathtt{b}) + (6\mathtt{aa} - 8\mathtt{b}) = 2\mathtt{aab} + 6\mathtt{aa} - 4\mathtt{b}.$$

Multiplication is defined by multiplying the coefficients, and concatenating the words. Note that this is non-commutative!

$$(4\mathtt{ba}) * (6\mathtt{aabb}) = 24\mathtt{baaabb}$$
$$(6\mathtt{aabb}) * (4\mathtt{ba}) = 24\mathtt{aabbba}.$$

Moreover, we demand that the distributive law hold.

Show that this makes R into a ring.

Field problems

Problem. 15

Compute the remainder when $x^{100} + 2x + 2$ is divided by $x^2 + 2$, in $\mathbb{Z}_3$.

Additional problems on fields

Problem. 16

Show that the set

$$K = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$$

form a field under usual addition and multiplication.

Group problems

Problem. 17

Let $a \in G$ for some group. Show that a and a^{-1} have the same order.

Problem. 18

Let $a, b \in G$. Show that ab and ba have the same order.

Problem. 19

Suppose $ab = ba$, and that $a^m = b^n = e$. Show that $(ab)^{mn} = e$.

Problem. 20

Show that all elements with finite order in an Abelian group, is a subgroup.

Problem. 21

Let a be an element in a group G, such that a has order 18. What order does a^2 have? What is the inverse of a^9?

Problem. 22

Suppose G is a finite group and let n be the number of elements in G. Show that for any $a \in G$, we have that $a^n = e$.

Problem. 23

Let G be a group with a and b in G. Show the equivalence

$$a^k = e \Longleftrightarrow \left(bab^{-1}\right)^k = e.$$

Can you draw any conclusion regarding order(a) and order(bab^{-1})?

Problem. 24

Let G be a group, and let a, b be in G. Define the set

$$H_b := \{bab^{-1} : a \in G\}.$$

Prove that H_b is a subgroup of G.

For example, if $G = \{e, a, b, c\}$, then $H_b = \{beb^{-1}, bab^{-1}, bbb^{-1}, bcb^{-1}\}$, but some of these elements might be equal.

Problem. 25

The set $H = \{0, 3, 6, 9\}$ is a subgroup of $\mathbb{Z}_{12}$. Find all cosets of H.

Problem. 26

Find the order of all elements, and all subgroups of $\mathbb{Z}_2 \otimes \mathbb{Z}_2$.

Problem. 27

Find the order of all elements and all subgroups of $\mathbb{Z}_4$.

Problem. 28

Find the order of all elements, and all subgroups of $\mathbb{Z}_3 \otimes \mathbb{Z}_2$.

Problem. 29

Give an argument why the groups $\mathbb{Z}_2 \times \mathbb{Z}_3$ and S_3 (permutations on 3 elements) are not isomorphic.

Problem. 30

Find all subgroups of $\mathbb{Z}_{24}$.

Problem. 31

Suppose $G = \{g_1, \dots, g_n\}$ is a finite Abelian group and let $c = g_1 g_2 \cdots g_n$. Prove that $g^2 = e$.

Problem. 32

How many subgroups does $\mathbb{Z}_n$ have, if $n = 2^4 \times 3^2 \times 5$?

Problem. 33

Determine which of the following statements are true.

By true, we mean *always true*.

(a) If a, b be elements in a group such that order$(a) = 4$ and order$(b) = 2$ then order$(ab) = 8$.

(b) The complex number $e^{2\pi i/n}$ generates a cyclic group of size n in $\langle \mathbb{C} \setminus \{0\}, \times \rangle$.

(c) If $|G| = m$ and $|H| = n$ then $G \times H$ has a subgroup of size m.

Multiplication tables

Problem. 34

Consider the following multiplication table for a group G and solve the following problems.

○	**e**	**a**	**b**	**c**	**d**	**f**
e	e	a	b	c	d	f
a	a	e	d	f	b	c
b	b	c	e	a	f	d
c	c	b	f	d	e	a
d	d	f	a	e	c	b
f	f	d	c	b	a	e

(1)

(a) Determine if G is commutative.

(b) Determine if G is cyclic.

(c) Find the inverse of d.

(d) Find all subgroups of size 2.

(e) Are there any subgroups of size 4?

(f) Find a subgroup of size 3.

(g) Find an element x such that $axc = f$.

Problem. 35

Consider the following multiplication table for a group G and answer the following questions.

×	**a**	**b**	**c**	**d**	**f**
a	b	f	d	a	c
b	f	c	a	b	d
c	d	a	f	c	b
d	a	b	c	d	f
f	c	d	b	f	a

(2)

(a) Which element is the identity element?

(b) Is the group commutative?

(c) Is there some $x \in G$ such that $x^3 = d$?

Permutations

Problem. 36
Let $\pi = [2,3,1,6,4,5]$, $\sigma = [1,3,6,4,2,5]$.

(a) Compute $\pi \circ \sigma$ and $\sigma \circ \pi$.

(b) Express π and σ in cycle form.

(c) Compute π^{-1} and σ^{-1}.

(d) What are the types of π and σ?

(e) Compute the order of π and σ.

(f) Compute π^{22}.

(g) Compute the number of inversions in π and σ.

(h) Express π as a product of simple transpositions.

Problem. 37
Suppose $\pi \in \mathrm{S}_n$. Show that $\mathrm{inv}(\mathrm{rev}(\pi)) = \binom{n}{2} - \mathrm{inv}(\pi)$.

The *reverse*, rev, of a permutation is the permutation obtained by reversing the one-line notation. For example, $\mathrm{rev}([5,2,4,3,1]) = [1,3,4,2,5]$.

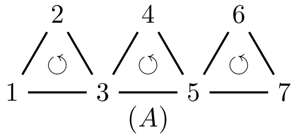
Problem. 38
Recall that a permutation is even (odd) if it is a product of an even (odd) number of transpositions. Prove that the following rules hold for composition of permutations:

- Even∘Even=Even,
- Even∘Odd=Odd,
- Odd∘Odd=Even.

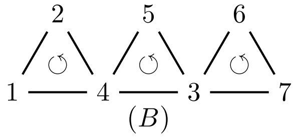
Problem. 39
Prove that a permutation is even if and only if its inverse is even.

Problem. 40
Let π be a permutation such that $\mathrm{order}(\pi)$ is odd. Prove that π must be even.

Problem. 41
Consider the puzzle below, where one can rotate each of the three triangles. For example, rotating the middle triangle in (A) once gives the configuration in (B).

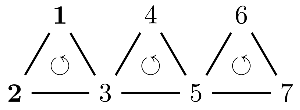


(A)



(B)

Prove that it there is no sequence of rotations that produce the following configuration, starting from (A).



Hint: Use the sign property of permutations.

Problem. 42

How many permutations in S_{10} are there of type $(2,2,2,2,1,1)$?

Problem. 43

How many permutations in S_{12} are there of type $(3,3,3,3)$?

Problem. 44

Let S_8 be the group of permutations on 8 elements. Describe an Abelian subgroup of S_8 with 10 elements.

Problem. 45

Consider the group of permutations S_n and let s_i denote the simple transposition $(i, i+1)$ for $1 \leq i < n$. Prove that

$$s_i s_j = s_i s_j \text{ whenever } |i-j| \geq 2$$

and

$$s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1} \text{ whenever } 1 \leq i < n.$$

These relations are extremely important when studying S_n, and they show up countless times in mathematics. These relations are called *braid relations*, and as the name suggests, describes how braiding works.

Solutions

Solution. 1

We wish to solve $2x \equiv_{11} 1$. This can be turned into the Diophantine equation

$$2x + 11y = 1.$$

Euclid's algorithm gives a possible solution $x = 6$, $y = -1$. The multiplicative inverse is therefore $x = 6$.

Solution. 2

We wish to solve $5x \equiv_{13} 1$. This can be turned into the Diophantine equation

$$5x + 13y = 1.$$

Euclid's algorithm gives

$$\begin{aligned} 13 &= 2 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \end{aligned}$$

Thus,

$$1 = 3 - 2 = 2 \cdot 3 - 5 = 2(13 - 2 \cdot 5) - 5 = 2 \cdot 13 - 5 \cdot 5$$

Euclid's algorithm gives the solution $x = -5$, $y = 2$. Thus, the multiplicative inverse is $-5 \equiv 13 - 5 = 8$.

Solution. 3

We turn the problem into a Diophantine equation and get $3x + 9y = 1$. Since $\gcd(3, 9) = 3$, the left hand side is always divisible by 3. However, the right hand side is never divisible by 3, so there cannot be any solutions. The number 3 does not have a multiplicative inverse.

Solution. 4

We have that $149291 \equiv_3 2$, so the left hand side has remainder 1 modulo 3. On the other hand, the right hand side is divisible by 3, so we can be sure that it is not an equality.

Solution. 5

We have that

$$\begin{aligned} 2^{1026} &= 2^2 \cdot 2^{1024} \\ &= 4 \cdot (2^4)^{256} \\ &\equiv_{17} 4 \cdot (-1)^{256} \\ &\equiv_{17} 4 \end{aligned}$$

so the remainder is 4.

Solution. 6

Yes, $2 \cdot 2 \equiv_6 4$, but we cannot solve $2x \equiv_6 5$. This we can see from the multiplication table.

Solution. 7

We need to find the multiplicative inverse of 5. This is possible since 11 is a prime number. There are several approaches, but we first note that

$$2 \cdot 5 = 10 \equiv_{11} -1.$$

Hence, $(2 \cdot 5)^2 \equiv_{11} 1$, so $5 \cdot (2 \cdot 2 \cdot 5) \equiv_{11} 1$. In other words, $2 \cdot 2 \cdot 5 = 20 \equiv_{11} = 9$ is the multiplicative inverse of 5, modulo 11. Therefore,

$$5x = 4 \iff x = 9 \cdot 4.$$

Now, $9 \cdot 4 = 36 = 33 + 3 \equiv_{11} 3$. So, we conclude that $x = 3$ is the solution.

Solution. 8

The second equation allow us to write $y = 3 - 2x$. This inserted in the first equation gives

$$x + 2(3 - 2x) = 2 \iff x + 6 - 4x = 3.$$

Since $6 \equiv_6 0$, the equation reduces to $3x = -3$, which is equivalent with $3x = 3$, since $-3 \equiv_6 3$. However, we *cannot* divide both sides by 3, since this is not an operation that can be done in $\mathbb{Z}_6$. So to solve

$3x = 3$ in $\mathbb{Z}_6$, we get the Diophantine equation $3x + 6y = 3$. This is ordinary integers, so we can instead solve $x + 2y = 1$.

We see that $x = 3$, $y = -1$ is a solution, so the general solution is $x = 3 + 2k$, with $k \in \mathbb{Z}$. Thus, $x = 1, 3, 5$ are the possible solutions in $\mathbb{Z}_6$.

Each of these cases is inserted in the second equation (and we solve in $\mathbb{Z}_6$):

$$x = 1 \Rightarrow 2 + y = 3 \Rightarrow y = 1$$

$$x = 3 \Rightarrow 6 + y = 3 \Rightarrow y = 3$$

$$x = 5 \Rightarrow 4 + y = 3 \Rightarrow y = 5$$

Thus, the possible solutions are $(x, y) = (1, 1), (3, 3)$ and $(5, 5)$.

Solution. 9

Gaussian elimination gives

$$\begin{cases} 3x + 3y & = 1 \\ 4x - y & = 2 \end{cases} \iff \begin{cases} 15x & = 7 \\ 4x - y & = 2 \end{cases} \iff \begin{cases} 4x & = 7 \\ 4x - y & = 2 \end{cases} \iff \begin{cases} 4x & = 7 \\ -y & = 2 - 7 \end{cases}$$

Since 4 is invertible in $\mathbb{Z}_{11}$ (we have that $3 \cdot 4 = 12 = 1$), we can solve for x and get $x = 3 \cdot 7 = 10$ and $y = 5$ as the only solution.

Solution. 10

This is left as an exercise for the moment.

Solution. 11

We need to show that adding two even functions is still even, and that the product of two even functions is still even. We also need to verify that 0 and 1 are even functions, which they are. Finally, if f is even, then we note that $-f$ is also even.

Since 0 is not an odd function, we do not have a 0 element, and the set of polynomials which are odd, is not a subring.

Solution. 12

Since R' and R'' are rings, we have that $0, 1 \in R'$ and $0, 1 \in R''$. Hence, $0, 1 \in R' \cap R''$, so the intersection contains the identity elements for addition and multiplication.

It remains to check that $R' \cap R''$ is closed under addition, multiplication and taking additive inverse.

Solution. 13

Suppose $R \subseteq \mathbb{Z}$ is a subring. Then we must have $0, 1 \in R$. But since R must be closed under addition, we must have that $1 + 1 + \cdots + 1 \in R$, so all non-negative integers are in R. Moreover, we must have additive inverses, so all negative integers must therefore be in R as well. Hence, $R = \mathbb{Z}$.

Solution. 14

We have that 0 and 1 are in R, these correspond to just using the empty word. It is evident from the definitions that R is closed under addition and multiplication. Moreover, addition is commutative and associative (we can think of our expressions as vectors if we like, where different words are different basis vectors). Multiplication is associative, since concatenation is. Finally, by definition, the distributive law holds, so we are done.

Solution. 15

We know that since $\mathbb{Z}_3$ is a field, we have polynomial division in $\mathbb{Z}_3[x]$. Hence,

$$x^{100} + 2x + 2 = (x^2 + 2)q(x) + (ax + b)$$

for some $q \in \mathbb{Z}_3[x]$ and $a, b \in \mathbb{Z}_3$. Here, $ax + b$ is of course the remainder we are looking for.

We now substitute $x = 1$ och $x = 2$ into the above relation, as these are two zeros of $x^2 + 2$. We obtain

$$1^{100} + 2 + 2 \equiv_3 a + b \qquad 2^{100} + 4 + 2 \equiv_3 2a + b.$$

Simplifying, noting that $2^{100} \equiv_3 (-1)^{100} = 1$, we have

$$\begin{cases} a + b & = 2 \\ 2a + b & = 1. \end{cases}$$

Finally, $a = 2$, $b = 0$ so the remainder is $2x$.

Solution. 16

Clearly, K is a subset of the real numbers, and it is easy to show that it is closed under addition, multiplication and taking additive inverses. Hence, K is a subring of $\mathbb{R}$. The multiplication is commutative, so the only thing we need to verify, is that $a + b\sqrt{2}$ has a multiplicative inverse whenever $a, b \neq 0$.

Since we are dealing with usual multiplication, we need to show that the real number

$$\frac{1}{a + b\sqrt{2}}$$

is also an element in K. To show this, we need to express this in the form $a' + b'\sqrt{2}$. Now,

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2}.$$

This is indeed an element in K, since it is equal to

$$\frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2},$$

and both the coefficients $\frac{a}{a^2-2b^2}$ and $\frac{-b}{a^2-2b^2}$ are rational numbers.

If we are going to be picky, we must actually also prove that $a^2 - 2b^2$ is non-zero whenever $a, b \neq 0$. But if $a^2 = 2b^2$, then $\sqrt{2} = a/b$, which is impossible if a, b are rational numbers.

Solution. 17

Suppose $a^k = e$ for some integer k. Multiplying both sides with a^{-k} gives $e = a^{-k}$. In other words, $a^k = e \iff a^{-k} = e$. It follows that the smallest positive k making the left hand side true, must also be the smallest k making the right hand side true.

Why equality and not only implication?

What is the definition of order?

Solution. 18

Let k be an integer such that $(ab)^k = e$. That is,

$$(ab)^k = abab \cdots ab = e$$

Multiply from the left with a^{-1} and then from the right with $b^{-1}a^{-1} \cdots b^{-1}$. This gives

By using that $(ab)^{-1} = b^{-1}a^{-1}$.

$$e = a^{-1}b^{-1} \cdots b^{-1} = (ba)^{-k}$$

In other words $(ba)^{-1}$ also have the property that when it is raised to the kth power, it becomes the identity. In fact, we have the equality $(ab)^k = e \iff (ba)^{-k} = e$.

Since $(ba)^{-1}$ and ba have the same order, we are now done.

Solution. 19

We have that

$$(ab)^{mn} = \underbrace{(ab)(ab)\cdots(ab)}_{mn \text{ times}} = a^{mn}b^{mn}$$

Now, $a^{mn} = (a^m)^n$ and $b^{mn} = (b^n)^m$, so both these are the identity element. Hence $a^{mn}b^{mn} = e^2 = e$ and we are done.

Solution. 20

Let H be the set of elements with finite order. We need to show that H is closed under taking inverses, and multiplication. We know from previous exercises that the order of an element and its inverse is the same. Hence, if g has finite order, so does g^{-1}, and H is therefore closed under taking inverse.

Suppose now that a and b have finite orders m and n, respectively. Then from previous exercise, we know that $(ab)^{mn} = e$, so in particular (ab) must have finite order. Hence, ab must be in H, so H is also closed under multiplication.

But it might be that ab has an order *smaller* than mn, but this is fine!

Solution. 21

Suppose that a^2 has order k. Then $a^{2k} = e$, so in particular $k \geq 9$. On the other hand, $(a^2)^9 = a^{18} = e$, so the order of a^2 is at most 9. Therefore, it must be equal to 9.

We know that $(a^9)^2 = e$, so a^9 is its own inverse.

Solution. 22

Let H be the cyclic subgroup generated by a. We have that order$(a) = |H|$. By Lagrange's theorem, $m \cdot |H| = |G|$ for some $m \in \mathbb{N}$, and we can then compute that

Why is order$(a) = |H|$ true?

$$a^n = a^{m \cdot |H|} = \left(a^{|H|}\right)^m = e^m = e.$$

Solution. 23

We show the equivalence as follows:

$$\begin{aligned} a^k = e \quad &\iff \quad ba^kb^{-1} = beb^{-1} \\ &\iff \quad b\underbrace{aa\cdots a}_{k}b^{-1} = e. \end{aligned}$$

The first step is done by multiplying on the left with b and on the right with b^{-1}, and then we just rewrite and expand. Subsequent manipulation gives

$$\begin{aligned} a^k = e \quad &\iff \quad ba(b^{-1}b)a(b^{-1}b)a\cdots a(b^{-1}b)ab^{-1} = e \\ &\iff \quad (bab^{-1})(bab^{-1})\cdots(bab^{-1}) = e \\ &\iff \quad (bab^{-1})^k = e. \end{aligned}$$

The first step here is done by inserting $e = b^{-1}b$ between the a's. As multiplication by e does not change the expression, this step is valid. The second step is just regrouping.

If we are really picky, we can say that we use the associativity of the group operation.

This result allow us to use the same reasoning as in earlier exercises, and conclude that a and bab^{-1} have the same order.

Solution. 24

It is enough to show that H_b is closed under multiplication and taking inverses.

Closedness under inverses is straightforward: We note that if $bab^{-1} \in H_b$, then $ba^{-1}b^{-1} \in H_b$ is in H as well. Furthermore,

$$(bab^{-1})(ba^{-1}b^{-1}) = ba(b^{-1}b)a^{-1}b^{-1} = b(aa^{-1})b^{-1} = e,$$

so the inverse of bab^{-1} is given by $ba^{-1}b^{-1}$.

Closedness under multiplication follows a similar pattern: Suppose ba_1b^{-1} and ba_2b^{-1} are elements in H_b. Then their product $(ba_1b^{-1})(ba_2b^{-1}) = b(a_1a_2)b^{-1}$ must also be in H_b, since a_1a_2 is an element in G.

Convince yourself why this is enough to verify.

Solution. 25

The cosets are produced by multiplying H (on the right) with elements in $\mathbb{Z}_{12}$. Group multiplication in $\mathbb{Z}_{12}$ is addition mod 12. The three cosets are

$$\begin{aligned} \{0,3,6,9\} \quad & \text{By adding } 0,3,6 \text{ or } 9 \text{ to } H \\ \{1,4,7,10\} \quad & \text{By adding } 1,4,7 \text{ or } 10 \text{ to } H \\ \{2,5,8,11\} \quad & \text{By adding } 2,5,8 \text{ or } 11 \text{ to } H. \end{aligned}$$

Note that the union of the cosets give the entire group $\mathbb{Z}_{12}$.

Solution. 26

The elements are $e = (0,0)$, $(0,1)$, $(1,0)$ and $(1,1)$, and group operation is given by element-wise addition mod 2.

It is straightforward to verify that $(0,0)$ has order 1, and all other elements have order 2.

Since the group has size 4, subgroups can only have 1, 2 or 4 elements. The subgroups are

$$\{e\}, \{e,(0,1)\}, \{e,(1,0)\}, \{e,(1,1)\} \text{ and } \mathbb{Z}_2 \otimes \mathbb{Z}_2.$$

The identity element is always the only possible subgroup with only one element.

Subgroups of size 2 must have e and one additional element, and by checking, all three other elements generate a subgroup of size 2.

Solution. 27

Case by case checking shows that

$$\operatorname{order}(0) = 1, \quad \operatorname{order}(1) = \operatorname{order}(3) = 4, \qquad \operatorname{order}(2) = 2.$$

Since $\mathbb{Z}_4$ is a cyclic group — it has 1 as a generator, all subgroups are also cyclic.

Due to Theorem 9.

It is therefore enough to see what group each element generates. Since 1 and 3 have order 4, these generate the entire group. The only non-trivial[8] subgroup is therefore the one generated by 2, namely $\{0,2\}$. The subgroups are therefore

$$\{e\}, \quad \{0,2\}, \quad \mathbb{Z}_4.$$

Solution. 28

We have

$$\operatorname{order}((0,0)) = 1, \quad \operatorname{order}((1,0)) = \operatorname{order}((2,0)) = 3,$$

and

$$\operatorname{order}((0,1)) = 2, \quad \operatorname{order}((1,1)) = \operatorname{order}((2,1)) = 6.$$

Since $(1,1)$ has order 6, it is a generator for the group, and $\mathbb{Z}_3 \otimes \mathbb{Z}_2$ is cyclic. All subgroups are therefore also cyclic, and by Lagrange, the non-trivial subgroups must have size 2 or 3. The non-trivial subgroups are therefore

$$\{e,(1,0),(2,0)\} \text{ and } \{e,(0,1)\}.$$

Solution. 29

Note that $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic, and therefore isomorphic to $\mathbb{Z}_6$.

However, in S_3 there is no element of order 6 — remember that the order of a permutation is the lowest common multiple of the cycle lengths. There is no way to have cycles of length 2 and 3 at the same time in a permutation. This proves that the groups are not isomorphic.

[8] All groups G have G itself and $\{e\}$ as subgroups, so we say that these are trivial. All other subgroups are non-trivial.

Another example would be to find two elements in S_3 that does not commute. The group $\mathbb{Z}_6$ is commutative, while S_3 is not commutative.

Solution. 30

Lagrange's theorem tells us that possible subgroups have sizes $1, 2, 3, 4, 6, 8, 12$ or 24. Since $\mathbb{Z}_{24}$ is cyclic, all subgroups are cyclic as well. We can present subgroups in a diagram as follows, ordered by inclusion. We use the notation

$$k\mathbb{Z}_n := \{0, k, 2k, \dots, (n-1)k\}.$$

For example,

$$8\mathbb{Z}_3 = \{0, 8, 16\}.$$

The subgroups are therefore as follows:

$$\begin{tikzcd}
\{e\} \arrow[r] \arrow[d] & 12\mathbb{Z}_2 \arrow[r] \arrow[d] & 6\mathbb{Z}_4 \arrow[r] \arrow[d] & 3\mathbb{Z}_8 \arrow[d] \\
8\mathbb{Z}_3 \arrow[r] & 4\mathbb{Z}_8 \arrow[r] & 2\mathbb{Z}_{12} \arrow[r] & \mathbb{Z}_{24}
\end{tikzcd}$$

Solution. 31

Since G is Abelian,

$$c^2 = g_1 g_1 g_2 g_2 \cdots g_n g_n,$$

and we can rearrange all factors as we wish. For each factor $g_i g_i$, there are two cases to consider:

- Either $g_i g_i = e$, in the case g_i is its own inverse, or
- g_i has some other inverse, g_j. In this case, we can rearrange these two pairs such that we have $(g_i g_k)(g_i g_k) = e^2 = e$.

Every element is therefore canceled by some other element in the big product, and the result is the identity element e.

Solution. 32

As we saw in the previous exercise, if $k|n$, then $k\mathbb{Z}_{n/k}$ is a subgroup of $\mathbb{Z}_n$. Furthermore, we can only have cyclic subgroups and every cyclic subgroup is of this form. In other words

$$H \text{ is a subgroup of } \mathbb{Z}_n \iff H = k\mathbb{Z}_{n/k} \text{ for some } k \text{ dividing } n.$$

It suffices to compute the number of divisors of n. We have $5 \times 3 \times 2 = 30$ divisors, as for each prime number p in the factorization of n, we must choose how many times it appear in a divisor.

For example, there are five possible choices for $p = 2$, namely 2^0, $2^1, \dots, 2^4$.

Solution. 33

(a) No, this statement is false. Take for example $a = 1$ and $b = 2$ in $(\mathbb{Z}_4, +)$.

(b) Yes, this is true. One can easily check that if $\xi = e^{2\pi i/n}$ then

$$H = \{1, \xi, \xi^2, \xi^3, \dots, \xi^{n-1}\}$$

is a set of n different numbers, it is generated by ξ, and $\xi^n = 1$. Thus, H is a cyclic subgroup.

In fact, the elements in H are the n different complex solutions to $x^n - 1 = 0$.

(c) Yes, this is true — consider all elements of the form

$$K = \{(g, e) : g \in G\}.$$

Then $|K| = |G|$ and it is a routine exercise to show that K is indeed a subgroup.

Solution. 34

We have the following:

(a) G is not commutative, because $b \circ a = c$, but $a \circ b = d$.

(b) We just concluded that G is not commutative, so it cannot be cyclic.

(c) We look in the row of d, and see that $d \circ c = e$, so $d^{-1} = c$.

(d) Any subgroup of size 2 must be of the form $\{e, x\}$, where $x^2 = e$. We look in the table, and see that $a^2 = b^2 = f^2 = e$, so $\{e, a\}$, $\{e, b\}$ and $\{e, f\}$ are all subgroups of size 2.

(e) There are no subgroups of size 4 since that would violate Lagrange's theorem.

The table tells us that $|G| = 6$.

(f) A subgroup of size 3 must be cyclic since 3 is a prime. The table gives that $c \circ c = d$ and that $c \circ d = e$. Therefore, $c \circ c \circ c = e$, and c is an element of order 3. It follows that $\{e, c, d\}$ is a subgroup of order 3.

(g) We want to find x such that $axc = f$. Solving for x by multiplying with appropriate inverses gives that $x = a^{-1} f c^{-1}$. From the table we see that $a^{-1} = a$, $c^{-1} = d$. Thus, $x = afd$. We can then read off that $a \circ f = c$, so $x = c \circ d = e$.

Be careful on which side to multiply, G is non-commutative!

Solution. 35

(a) From the table, we see from row d that multiplication with d has no effect, so d is the identity element.

(b) The group is commutative, since the table is the same under transposition (seen as a matrix).

(c) We know that d is the identity element, so the question asks if there is some x with order 3. This is not possible in a group with 5 elements.

What do we know about the group x would generate, if there was such an x?

Solution. 36

We have the following solutions:

(a) We have

$$\pi \circ \sigma = [2, 1, 5, 6, 3, 4] \qquad \sigma \circ \pi = [3, 6, 1, 5, 4, 2].$$

(b) In cycle form, we have $\pi = (123)(465)$, $\sigma = (1)(2365)(4)$

(c) The inverses are (in cycle form)

$$\pi^{-1} = (132)(456), \qquad \sigma^{-1} = (1)(2563)(4)$$

(d) The types are $\text{type}(\pi) = (3,3)$ and $\text{type}(\sigma) = (4,1,1)$.

(e) We have $\text{lcm}(3,3) = 3$ so $\text{order}(\pi) = 3$. Similarly, $\text{lcm}(1,4,1) = 1$ so $\text{order}(\sigma) = 4$.

(f) Note that $\pi^{22} = \pi^{21} \circ \pi = (\pi^3)^7 \circ \pi = e \circ \pi = \pi$, since we know that the order of π is 3.

(g) In position i, we write a subscript — the number of entries to the right that are smaller than the entry at i:

$$\pi = [2_1, 3_1, 1_0, 6_2, 4_0, 5_0], \qquad \sigma = [1_0, 3_1, 6_3, 4_1, 2_0, 5_0]$$

Adding up the subscripts give the number of inversions, so $\text{inv}(\pi) = 4$, $\text{inv}(\sigma) = 5$.

(h) We have that $\pi = (2,3) \circ (1,2) \circ (4,5) \circ (5,6)$ but there are other solution.

Solution. 37

If the entries a and b form an inversion in π, they do not form an inversion in $\text{rev}(\pi)$ and vice versa. In other words, every pair of entries, (a,b) is an inversion in exactly one of π and $\text{rev}(\pi)$. Since the total number of such pairs for a permutation in S_n is $\binom{n}{2}$, we must have that

$$\binom{n}{2} = \text{inv}(\text{rev}(\pi)) + \text{inv}(\pi).$$

This proves the result.

Solution. 38

Let σ and π be even permutations. Then we can express these as products of transpositions as follows:

$$\sigma = \tau_1\tau_2 \cdots \tau_{2k} \qquad \pi = \tau'_1\tau'_2 \cdots \tau'_{2\ell}$$

Now,

$$\sigma \circ \pi = (\tau_1\tau_2 \cdots \tau_{2k}) \circ (\tau'_1\tau'_2 \cdots \tau'_{2\ell})$$

so the composition $\sigma \circ \pi$ is a product of $2k + 2\ell$ transpositions — which is also even. This proves the first case, the other ones are proved in a similar manner.

Solution. 39

Let $\pi = \tau_1\tau_2 \cdots \tau_\ell$ be a product of transpositions. Then we can easily verify that

$$\pi^{-1} = \tau_\ell \cdots \tau_2\tau_1.$$

Verify first that $\tau^2 = e$ whenever τ is a transposition.

Hence, π and π^{-1} are both even, or both odd.

ALTERNATIVELY, suppose that π is even and pretend for a moment that π^{-1} is odd. Consider the expression $\pi \circ \pi^{-1}$. On one hand, it is even, since e is even. On the other hand EVEN∘ODD=ODD, so there is a contradiction. Thus π^{-1} must be even.

Solution. 40

Express π as a product of transpositions, $\pi = \tau_1 \cdots \tau_\ell$. Let k be the order of π, such that

$$e = \underbrace{\pi \circ \cdots \circ \pi}_{k} = (\tau_1 \cdots \tau_\ell) \cdots (\tau_1 \cdots \tau_\ell).$$

We see that e is a product of $k\ell$ transpositions, but we also know that e is an even permutation. Therefore, $k\ell$ must be an even number, and since k is odd, ℓ must be even. Therefore, π is even.

Solution. 41

Each rotation act on the vertex labels according to a 3-cycle. For example, rotating the middle triangle is the permutation $(354) \in S_7$. The sign of a 3-cycle is even, as it can be expressed as a product of two transpositions. Hence, each rotation is an even transposition. Thus, every reachable configuration must be reachable via some even permutation of the labels.

However, to reach the configuration where only 1 and 2 have switched, we need an odd permutation. This is impossible.

Solution. 42

We need to count all possible ways to construct four 2-cycles. Choosing the elements to be in the two-cycles can be done in $\binom{10}{2,2,2,2,1,1}$ ways, but we need to divide by 4! because the order of the two-cycles does not matter. The answer is therefore $\frac{10!}{2^4 \times 4!}$

The permutations $(12)(34)$ and $(34)(12)$ are the same.

Solution. 43

We need to partition the permutation into 4 3-cycles. Choosing the elements to be in the 3-cycles can be done in $\binom{12}{3,3,3,3}$ ways, but we need to divide by 4! because the order of the 3-cycles does not matter. Furthermore, the elements in each 3-cycle can be ordered in two different ways. We therefore have 2 choices for each cycle. The answer is therefore $\frac{12! \times 2^4}{(3!)^4 \times 4!}$

Observe that the cycles (123) and (132) are different!

Solution. 44

It would be convenient to look for a cyclic subgroup with 10 elements, since all cyclic groups are Abelian. Every cyclic (sub)group has a generator of order 10, so we need to find a permutation in S_8 with order 10. The order of a permutation is determined by the lcm of the lengths of the cycles. We cannot fit a single cycle of length 10, but we can find a permutation with a cycle of length 5, and a cycle of length 2. For example,

$$\pi = (12345)(67)(8)$$

is in S_8 and has order 10. It follows that $\langle \pi \rangle$ — the cyclic group generated by π — is an Abelian subgroup of size 10.

Solution. 45

We can without loss of generality assume that $i < j$. Let us express the permutation $s_i s_j$ in two-line notation. We get

Recall that $s_i s_j = (i, i+1)(j, j+1)$ in cycle-notation, so this simply transposes the entries at position i with $i+1$ and j with $j+1$.

$$s_i s_j = \begin{bmatrix} 1 & \dots & i & i+1 & \dots & j & j+1 & \dots & n \\ 1 & \dots & i+1 & i & \dots & j+1 & j & \dots & n \end{bmatrix}$$

and it is easy to see that this is equal to $s_j s_i$.

For the second relation we use the same strategy, and get that

$$\begin{aligned} s_i &= \begin{bmatrix} 1 & \dots & i & i+1 & i+2 & \dots & n \\ 1 & \dots & i+1 & i & i+2 & \dots & n \end{bmatrix} \\ s_{i+1} s_i &= \begin{bmatrix} 1 & \dots & i & i+1 & i+2 & \dots & n \\ 1 & \dots & i+1 & i+2 & i & \dots & n \end{bmatrix} \\ s_i s_{i+1} s_i &= \begin{bmatrix} 1 & \dots & i & i+1 & i+2 & \dots & n \\ 1 & \dots & i+2 & i+1 & i & \dots & n \end{bmatrix} \end{aligned} \tag{A}$$

Computing $s_{i+1} s_i s_{i+1}$ instead gives

$$\begin{aligned} s_{i+1} &= \begin{bmatrix} 1 & \dots & i & i+1 & i+2 & \dots & n \\ 1 & \dots & i & i+2 & i+1 & \dots & n \end{bmatrix} \\ s_i s_{i+1} &= \begin{bmatrix} 1 & \dots & i & i+1 & i+2 & \dots & n \\ 1 & \dots & i+2 & i & i+1 & \dots & n \end{bmatrix} \\ s_{i+1} s_i s_{i+1} &= \begin{bmatrix} 1 & \dots & i & i+1 & i+2 & \dots & n \\ 1 & \dots & i+2 & i+1 & i & \dots & n \end{bmatrix} \end{aligned} \tag{B}$$

so we see from (A) and (B) that $s_i s_{i+1} s_i$ and $s_{i+1} s_i s_{i+1}$ are indeed the same permutation.