Discrete mathematics

Per Alexandersson

Combinatorics and counting

Introduction to counting

Here is a collection of counting problems. Questions and suggestions are welcome at `per.w.alexandersson@gmail.com`.

Version: 15th February 2021,22:25

Exclusive vs. independent choice. Recall that we *add* the counts for exclusive situations, and *multiply* the counts for independent situations. For example, the possible outcomes of a dice throw are exclusive:

$$(\text{Sides of a dice}) = (\text{Even sides}) + (\text{Odd sides})$$

The different outcomes of selecting a playing card in a deck of cards can be seen as a combination of *independent* choices:

$$(\text{Different cards}) = (\text{Choice of color}) \cdot (\text{Choice of value}).$$

Labeled vs. unlabeled sets is a common cause for confusion. Consider the following two problems:

- Count the number of ways to choose 2 people among 4 people.
- Count the number of ways to partition 4 people into sets of size 2.

In the first example, it is understood that the set of chosen people is a *special* set — it is the *chosen set*. We choose two people, and the other two are not chosen. In the second example, there is no difference between the two couples. The answer to the first question is therefore

$$\binom{4}{2}, \qquad \text{counting the chosen subsets: } \{12, 13, 14, 23, 24, 34\}.$$

The answer to the second question is

$$\frac{1}{2!}\binom{4}{2}, \qquad \text{counting the partitions: } \{12|34, 13|24, 14|23\}.$$

That is, the issue is that there is no way to distinguish the two sets in the partition. However, now consider the following two problems:

- Count the number of ways to choose 2 people among 5 people.

- Count the number of ways to partition 5 people into a set of size 2 and a set of size 3.

In this case, the answer to both questions is $\binom{5}{3}$. The reason for this is that we can distinguish between the two sets in the partition in the second question, for example, *the set of size* 2 is unique.

We always consider people to be unique, and therefore labeled. This means that in a group of n people, we can talk about the first person, the second person, and so on. In a group of n *identical* objects, there is no á priori notion of the first object.

Overview of formulas

Every row in the table illustrates a type of counting problem, where the solution is given by the formula. Conversely, every problem is a *combinatorial interpretation* of the formula. In this context, a *group* of things means an unordered set.

PROBLEM	TYPE	FORMULA
Choose a group of k objects from n different objects	Binomial coefficient	$\binom{n}{k}$
Partition n different objects into m labeled groups, with k_i elements in group i	Multinomial coefficients	$\binom{n}{k_1, \ldots, k_m}$
Partition n different objects into k non-empty groups, where there is no order on the sets	Partitions, Stirling numbers	$S(n,k)$
Partition n different objects into k labeled groups (which could be empty)	Multiplication principle	k^n
Partition n identical objects into m labeled groups	Dots and bars	$\binom{n+m-1}{m-1}$
Same, but with non-empty groups	Dots and bars	$\binom{n-1}{m-1}$
Order n different objects	Permutations	$n!$
Choose and order k different objects from n different objects	Permutations	$\frac{n!}{(n-k)!}$
Choose and order n objects, where there are k_i identical objects of type i	Multinomial coefficients	$\binom{n}{k_1, \ldots, k_m}$
Choices for (X,Y) if there are x choices for X and, independently, y choices of Y	Multiplication-principle	$x \cdot y$
Number of elements in $A \cap B \cap C$	Inclusion-exclusion	$\lvert A \cup B \cup C\rvert = \lvert A\rvert + \lvert B\rvert + \lvert C\rvert - \lvert A \cap B\rvert - \lvert A \cap C\rvert - \lvert B \cap C\rvert + \lvert A \cap B \cap C\rvert$

Binomial- and multinomial coefficients

Whenever $n \geq 0$ and $0 \leq k \leq n$, we define the *binomial coefficients* as

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}. \quad \text{(Binomial coefficients)}$$

Sometimes the notation $C(n,k)$ for $\binom{n}{k}$ is used.

The binomial coefficients satisfy the following recursion:

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}. \quad (1)$$

To choose k objects among $\{1,2,\dots,n\}$, we either exclude n, and choose k objects among $\{1,2,\dots,n-1\}$ *or* we include n, and choose additional $k-1$ objects among $\{1,2,\dots,n-1\}$.

We have the *binomial theorem*:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \quad \text{(Binomial theorem)}$$

A generalization of the binomial coefficients are the *multinomial coefficients*. Whenever $k_1 + k_2 + \ldots + k_r = n$, they are defined as

$$\binom{n}{k_1, k_2, \dots, k_r} = \frac{n!}{k_1! \cdots k_r!}. \quad \text{(Multinomial coefficients)}$$

Stirling numbers

The Stirling numbers $S(n,k)$ can be computed recursively via a table, where every row is obtained from the previous via

$$S(n,k) = S(n-1,k-1) + k \cdot S(n-1,k).$$

and using the fact that $S(n,1) = S(n,n) = 1$.

Proof: To partition $\{1,2,\cdots,n\}$, into k groups, we either let n be in its own group, and partition $\{1,2,\dots,n-1\}$ into $k-1$ groups, or we partition $\{1,2,\dots,n-1\}$ into k groups and choose which of the k groups n belongs to.

Counting problems

Problem. 1

You are creating a 4-digit pin code. How many choices are there in the following cases?

(a) With no restriction.

(b) No digit is repeated.

(c) No digit is repeated, digit number 3 is a 0.

(d) No digit is repeated, and they must appear in increasing order.

(e) No digit is repeated, 2 and 5 must be present.

Problem. 2

How many shuffles are there of a deck of cards, such that $A\heartsuit$ is not directly on top of $K\heartsuit$, and $A\spadesuit$ is not directly on top of $K\spadesuit$?

A standard deck has 52 cards, divided into four suits ($\heartsuit$, $\spadesuit$, $\diamondsuit$, $\clubsuit$). There are 13 cards of each suit, $2, 3, \dots, 10$, J, Q, K, A, the Jack, Queen, King and Ace

Problem. 3

How many different words can be created by rearranging the letters in `SELFIESTICK`?

Problem. 4
How many flags can we make with 7 stripes, if we have 2 white, 2 red and 3 green stripes?

Problem. 5
We have four different dishes, two dishes of each type. In how many ways can these be distributed among 8 people?

Problem. 6
In how many ways can 8 people form couples of two?

Problem. 7
We go to a pizza party, and there are 5 types of pizza. We have starved for days, so we can eat 13 slices, but we want to sample each type at least once. In how many ways can we do this? Order does not matter.

Problem. 8
How many rth order partial derivatives does $f(x_1, \ldots, x_n)$ have?

Problem. 9
How many integer solutions does $x_1 + x_2 + \cdots + x_n = r$ have, with $x_i \geq 0$?

Problem. 10
How many integer solutions does the equation

$$x_1 + x_2 + x_3 + x_4 = 15$$

have, if we require that $x_1 \geq 2$, $x_2 \geq 3$, $x_3 \geq 10$ and $x_4 \geq -3$?

Problem. 11
How many integer solutions are there to the system of inequalities

$$x_1 + x_2 + x_3 + x_4 \leq 15, \qquad x_1, \ldots, x_4 \geq 0?$$

Problem. 12
Count the number of non-negative integer solutions to

$$3x_1 + 3x_2 + 3x_3 + 7x_4 = 22.$$

Problem. 13
Compute the number of surjections $f : A \to B$ if $|A| = n$ and $|B| = k$.

Problem. 14
You are going to an amusement park. There are four attractions, (haunted house, roller coaster, a carousel, water ride). You buy 25 tokens. Each attraction cost 3 tokens each ride, except the roller coaster that costs 5. Obviously, you want to ride each ride at least once, but the order of the rides does not matter.

In how many ways can you spend your tokens? You may have some remaining tokens in the end of the day.

Problem. 15

At an amusement park, you pay for attractions using tokens. There are five different attractions which cost 3 tokens each, and one attraction which cost 5 tokens. You have 42 tokens and you want to use all of them. How many different selections of attractions are there?

Problem. 16

How many words can you create of length 6, from the letters `a`, `b`, `c` and `d` if

- you must include each letter at least once, and
- `a` must appear exactly once.

Problem. 17

Eight different exam questions are to be distributed among three students, such that each student receives at least one question. However, two of the questions are very easy and must be given to different students. In how many ways can this be done?

Problem. 18

Prove that $S(n+1, k+1) \geq S(n, k)$ whenever $n \geq 1$ and $1 \leq k \leq n$.

Problem. 19

How many words can be made by rearranging `aabbccdd`, such that no `'a'` appears somewhere to the right of some `'c'`?

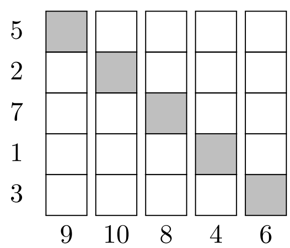
Problem. 20

You have 2 copies of the letter `'A'` and and unlimited supply of the letters `'B'`, `'C'` and `'D'`. How many words of length 10 can you make from these, such that

- all the `A`'s are used
- the third letter is an `A`, and
- there is no `B` appearing between the `A`'s?

Problem. 21

Count the number of ways to place the numbers $1, 2, \ldots, 10$ on the left and bottom side of the square below, such that for each gray box, the number on its left is smaller than the number below it.



Problem. 22

A certain juice bar serves three types of fruit juice, which are available in two different sized cups. In how many ways can you place an order of five drinks?

Problem. 23

On campus, there is a kiosk selling four different types of small candies, 4 sek apiece. You have 40 sek available and you want to spend all of it on a bag of candies. (a) How many different bags can you make? You must answer with an integer.

(b) Same question, but there is also a fifth type, which costs 5 sek each.

Problem. 24

There are 10 people, who will participate in *generic sport*. They divide themselves into five pairs.

(a) In how many ways can the people be divided into pairs?

(b) The five teams will travel to the sport venue in two identical minivans. In how many ways can the teams distribute themselves among the minivans, so that no van is empty?

You need to to answer with an integer in both questions.

Problem. 25

We are to construct a flag with 5 stripes. We have six available stripes of the following types: 2 red, 2 blue, 2 yellow. How many flags can be made under these restrictions? The order of the stripes on the flag matter. You should answer with an integer.

Mailbox-principle

Problem. 26

What is the maximum number of rooks you can place on an 8×8 chessboard so that no two rooks can attack each other?

Problem. 27

Alice and Bob are dining at a Chinese restaurant, where there are 10 small dishes available. Each dish is priced between 50 and 100 yuan. They decide to order several dishes each, in such a manner that all dishes are different. Moreover, they want to ensure that the price of the dishes Alice chooses have the same total price as the ones Bob selects.

Show that such a choice is possible.

Problem. 28

Let S be a subset of $\{1, 2, \ldots, 2n\}$ such that S has $n + 1$ elements. Prove that there are different elements a, b in S such that a divides b.

This is quite a challenging problem!

Binomial identities

In this section, we prove combinatorial identities by giving an interpretation of the different terms and factors involved. The go-to strategy is that the simpler side of the identity tells some story story, and we add some *refinement* or details to the story to get an interpretation of the more complicated side. For example, a poker player can immediately tell you how to prove and interpret the "combinatorial" identity

$$52 = 13 + 13 + 13 + 13.$$

The left hand side count the number of cards. The right hand side *refines* the situation, by counting the number of cards in each suit.

A classical identity is

$$2^n = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n}. \tag{2}$$

We know that the left hand side count the number of binary words of length n. The right hand side *refines* this count — term k counts the number of binary words with exactly k bits equal to 1.

It is important to emphasize that we add *exclusive* counts, a binary word is counted by exactly one of the binomial coefficients.

Problem. 29

Show by using a combinatorial argument that

$$\binom{n}{r} = \sum_{k=0}^{r} \binom{n-m}{k}\binom{m}{r-k} \text{ whenever } 0 \leq m, r \leq n.$$

Problem. 30

Prove that

$$\binom{n}{2}2^{n-2} = \sum_{k=2}^{n} \binom{n}{k}\binom{k}{2} \text{ whenever } n \geq 2.$$

Problem. 31

Prove that

$$2n \cdot 3^{n-1} = \sum_{k=1}^{n} k \cdot 2^k \binom{n}{k}.$$

Problem. 32

Show that if a, b are non-negative integers, we have

$$\binom{a+b}{a}\binom{a+b}{b} = \sum_{k=0}^{a+b} \binom{a+b}{k}\binom{a+b-k}{a-k}\binom{b}{b-k}.$$

Problem. 33

Show

$$\binom{n+0}{0} + \binom{n+1}{1} + \binom{n+2}{2} + \cdots + \binom{n+r}{r} = \binom{n+r+1}{r}.$$

Problem. 34

Let $m \geq n$ and show that

$$\binom{m+n}{n} = \sum_{k=0}^{n} \binom{m}{k}\binom{n}{k}.$$

Tip: First use $\binom{n}{k} = \binom{n}{n-k}$.

Problem. 35

Let $m \geq n$ and show that

$$\binom{m+n}{k} = \sum_{i=0}^{k} \binom{m}{k}\binom{n}{k-i}.$$

Problem. 36

Prove the identity

$$n \cdot 4^{n-1} = \sum_{k=0}^{n} \binom{n}{k} 3^k (n-k).$$

Problem. 37

Show that

$$\sum_{k=0}^{n} \frac{1}{k+1}\binom{n}{k} = \frac{2^{n+1}-1}{n+1}.$$

Problem. 38

Prove that

$$\binom{n+2}{k} = \binom{n}{k} + 2\binom{n}{k-1} + \binom{n}{k-2}.$$

Problem. 39

Show that

$$\sum_{k=0}^{n} \frac{1}{k+1}\binom{n}{k} = \frac{2^{n+1}-1}{n+1}.$$

Combinatorial bijections

Here are a few examples of combinatorial bijections. The bijections in the solutions are just suggestions, there should be plenty of other possible bijections.

Problem. 40

Let S_n be the set of permutations of $\{1, 2, \ldots, n\}$ and let Q_n be the set of integer vectors $\mathbf{w}$ of length n, with the property that $1 \leq \mathbf{w}_i \leq i$ for all i. Describe a bijection between S_n and Q_n.

Problem. 41

Let B_n denote the set of binary words with n digits. Moreover, let C_n be the set of *integer compositions* of n. For example,

For example, B_3 consists of the 2^3 words 000, 001, 010, 011, 100, 101, 110, 111.

$$C_4 = \{(4), (1,3), (2,2), (3,1), (1,1,2), (1,2,1), (2,1,1), (1,1,1,1)\}$$

Describe a bijection from B_{n-1} to C_n.

Problem. 42

Consider a labeled tree on n vertices, where 1 is considered the root vertex. We say that the tree is *decreasing* if the labels appear in a decreasing manner on every path from a vertex to the root, see Fig. 1.

Show that the number of such decreasing trees on n vertices is $(n-1)!$, by constructing a bijection from the set of trees, to permutations of $\{1, 2, 3, \dots, n\}$ ending with a 1.

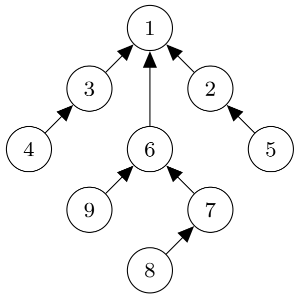


Figure 1: An example of an increasing tree.

Inclusion–Exclusion

Problem. 43

There are five people of different height. In how many ways can they stand in a line, so there is no 3 consecutive people with increasing height?

Problem. 44

Count the number of decks of cards, where no king is on top of the ace of the same suit.

Problem. 45

Count the number of decks of cards, where no king is on top of any ace.

Problem. 46

We have a smorgosbord, with 50 dishes, — 5 countries are represented, and there are 10 dishes from each. We want to make a plate with 8 dishes (no duplicates), but make sure that no country is missing. How many ways?

Problem. 47

We have k different boxes and r different objects. We want to distribute the objects into the boxes such that at no box is empty. In how many ways can this be done?

Observe that this is the same as the number of surjections from the set of boxes to the set of objects.

Problem. 48

There are five people of different height. In how many ways can they stand in a line, so there are no 3 consecutive people appear in order, either increasingly or decreasingly?

In other words, among any three adjacent people, the medium-tallest of them is not standing in the middle.

Problem. 49

How many permutations in S_6 are there, where 1 is not in a 3-cycle, and 2 is also not in a 3-cycle?

Reading comprehension

To see the intricacies in combinatorial reasoning, we now review a variety of counting problems.

Try to identify which of these choices allow for *repetition*, and which are ordered and unordered. Before proceeding, review the difference between *labeled* and *unlabeled* sets.

Words such as line, queue, list and shelf indicate an order, while words such as set, group, pile and bag indicate unordered arrangements. Additionally, people are always considered unique — no two persons are alike and they have names. You need to be aware if there are several sets, queues or groups involved: The two sets

$$\{\{a, b\}, \{c, d\}\} \text{ and } \{\{d, c\}, \{a, b\}\}$$

are considered equal. However, the two arrangements (with *named* sets)

$$A = \{a, b\}, B = \{c, d\} \text{ and } A = \{d, c\}, B = \{a, b\}$$

are considered different. Note that this intricacy can only occur for sets (or lists) of equal sizes.

Problem. 50

There are 8 people available. Count the number of ways

(a) to choose 6 of them and arrange them in a line.

(b) to choose 6 of them and place them into lines named A and B, with 3 in each.

(c) to choose 6 of them and place them into two equal-sized unlabeled lines.

(d) to choose 6 of them to make a group.

(e) to choose 6 of them and place them into groups named A and B, with 3 in each.

(f) to choose 6 of them and make two equal-sized unlabeled groups.

(g) to choose 6 of them and make three equal-sized unlabeled groups.

Problem. 51

There are 8 red balls available[1]. Count the number of ways

[1] These are identical!

(a) to choose 6 of them and arrange them in a line.

(b) to choose 6 of them to make a group.

(c) to choose 6 of them and give them to three people, some might not get any.

(d) to choose 6 of them and give them to three people, each person get at least one.

(e) to choose 6 of them and make three non-empty (unlabeled) groups.

(f) to choose 6 of them and divide them into piles.

Problem. 52

There are 8 types[2] of cookies available in a store. Count the number of ways

(a) to pick 6 of them and arrange them in a line.

(b) to pick 6 of them and place them into lines named A and B, with 3 in each.

(c) to pick 6 of them and place them into two equal-sized unlabeled lines.

(d) to pick 6 of them to make a group.

(e) to pick 6 of them and place them into groups named A and B, with 3 in each.

(f) to pick 6 of them and make two equal-sized unlabeled groups.

(g) to pick 6 of them and make three equal-sized unlabeled groups.

(h) For 10 people to choose a cookie type, and each type is selected by at least one person.

[2] This indicates that repetition is allowed — the same type can be used several times

Groups, rings and permutations

Introduction to abstract algebra

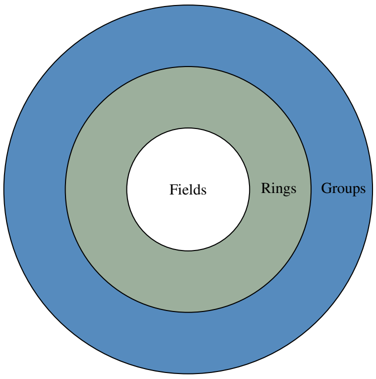


Figure 2: How to view groups, rings and fields.

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.

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:

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

We usually refer to a ring[3] 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 $a*b$.

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

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[4].

[4] That is, it is closed under "minus"

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 $a \in K$.

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[5] that send a polygon P to itself, under composition.

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

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[6] if $ab = ba$ for all a, b in G.

[6] Also known as commutative

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[7] cyclic group, and let H be a subgroup. Then H is of the form

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

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

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 $d = \gcd(a_1, a_2, \dots, a_k)$ 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?

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

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, $\times$, 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 $\pi \in S_n$ 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 $\pi \in S_n$, 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 $\pi \in S_n$ 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. 53
Find the inverse of 2 in $\mathbb{Z}_{11}$.

Problem. 54
Find the inverse of 5 in $\mathbb{Z}_{13}$.

Problem. 55
Does 3 have a multiplicative inverse in $\mathbb{Z}_9$?

Problem. 56
Is it possible that $149291^2 = 22287802671$? Can you compute the remainder on both sides when dividing by some p?

Problem. 57
Calculate the remainder when 2^{1026} is divided by 17.

Problem. 58
Can we solve $2x \equiv_6 4$? What about $2x \equiv_6 5$?

Problem. 59
Solve $5x \equiv_{11} 4$, (or equivalently, solve $5x = 4$ in $\mathbb{Z}_{11}$).

Problem. 60
In $\mathbb{Z}_6$, solve the system

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

Problem. 61
In $\mathbb{Z}_{11}$, solve the system

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

Problem. 62
In $\mathbb{Z}_{19}$, solve the system

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

Additional problems on rings

Problem. 63

Let $R \subseteq \mathbb{Q}[x]$ be the set of all polynomials which are even[8] functions. Show that R is a subring of $\mathbb{Q}[x]$.

Show that the set of polynomials which are odd[9] functions is *not* a subring.

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

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

Problem. 64

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. 65

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

Problem. 66

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.

Problem. 67

Let p be a prime number.

1. Let $a \in \mathbb{Z}_p$. Show that the polynomial $p_a(x) \in \mathbb{Z}_p[x]$ given by by
$$p_a(x) = \prod_{j \in \mathbb{Z}_p \setminus \{a\}} (x - j)$$
is non-zero if $x = a$, but zero everywhere else.

2. Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be any function. Show that there is some polynomial $p(x) \in \mathbb{Z}_p[x]$ of degree at most $p - 1$, such that
$$f(x) = p(x) \text{ for all } x \in \mathbb{Z}_p.$$
Hint: Show that we can write
$$f(x) = \sum_{j=0}^{p-1} c_j p_j(x)$$
where $c_j \in \mathbb{Z}_p$ is chosen appropriately.

3. Find a polynomial $p \in \mathbb{Z}_5[x]$ of degree at most 4, such that
$$p(0) = 1, p(1) = 4, p(2) = 3, p(3) = 2, p(4) = 0.$$

Field problems

Problem. 68
Compute the remainder when $x^{100} + 2x + 2$ is divided by $x^2 + 2$, in $\mathbb{Z}_3$.

Additional problems on fields

Problem. 69
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. 70
Let $a \in G$ for some group. Show that a and a^{-1} have the same order.

Problem. 71
Let $(G, \circ)$ be a group. Suppose that there is some $x \in G$, such that $x \circ g = g \circ x$ for all $g \in G$.

- Prove that $x^{-1} \circ g = g \circ x^{-1}$.
- Prove that $x^k \circ g = g \circ x^k$ for all $k \geq 1$.

Problem. 72
Let $a, b \in G$. Show that ab and ba have the same order.

Problem. 73
Suppose $ab = ba$, and that $a^m = b^n = e$. Show that $(ab)^{mn} = e$.

Problem. 74
Suppose $a, b \in G$ and that $ab = ba$. Moreover, a has order n and b has order m. Show that the smallest subgroup in G containing a and b has mn elements if $\gcd(m, n) = 1$.

Problem. 75
Show that all elements with finite order in an Abelian group, is a subgroup.

Problem. 76
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. 77
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. 78

Let $g \in G$, where G is a cyclic group of order n generated by g. Show that for all integers $k \geq 0$, we have that

$$g^k \text{ and } g^{n/\gcd(n,k)}$$

generate the same cyclic subgroup.

Problem. 79

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

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

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

Problem. 80

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. 81

Let G be the set of functions of the form $f(x) = ax + b$ where $a, b \in \mathbb{Q}$ and $a \neq 0$. Let $\circ$ denote function composition, so that if $f(x) = ax + b$, $g(x) = cx = d$, then

$$f \circ g = f(g(x)) = a(cx + d) + b.$$

This makes $(G, \circ)$ into a group.

1. Determine the neutral element in G and find the inverse to the function $h(x) = 3x + 5$.
2. Give an example of an element in G which has order 2.
3. Find all elements in G that has finite order. For partial points, show that there is no element in G with order 3.

Problem. 82

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

Problem. 83

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

Problem. 84

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

Problem. 85

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

Problem. 86

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

Problem. 87

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

Problem. 88

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

Problem. 89

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

Problem. 90

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 $\text{order}(a) = 4$ and $\text{order}(b) = 2$ then $\text{order}(ab) = 8$.

(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.

Problem. 91

Let G be a group and a, b are elements in G. Find possible values for $x, y \in G$ (expressed in terms of a and b) such that

$$x^2 = b^2 ya \text{ and } yx = b^{-1} abx.$$

Problem. 92

Let $(\mathbb{Z}_n^\times, \cdot)$ denote the group of invertible elements in $\mathbb{Z}_n$, with multiplication as group operation.

1. List all elements in $\mathbb{Z}_{15}^\times$.
2. Use inclusion-exclusion to show that there are exactly $pq - p - q + 1$ elements in $\mathbb{Z}_{pq}^\times$.
3. Prove that for $g \in \mathbb{Z}_{pq}^\times$, we have $g^{(p-1)(q-1)} = 1$. Note that this is equivalent to the generalized Fermat's little theorem.

Problem. 93

Let $G = \mathbb{Q} \setminus \{2\}$, that is the set of rational numbers not equal to 2. We define a group $(G, \circ)$ where

$$a \circ b := 2a + 2b - ab - 2.$$

Answer the following questions:

- Is G Abelian?
- Find the neutral element in G.

- Determine the inverse of 5, in G.

Problem. 94

Consider the group $G = (\mathbb{Z}_{60}, +)$.

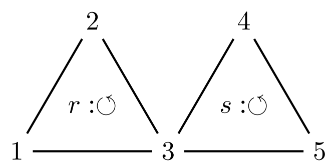
(a) Determine a subgroup H of G such that every non-zero element in H has order 5, *e.g.*, write down all elements in H.

(b) Let K be the smallest cyclic subgroup of G that contains both the elements 4 and 57. Determine a generator for K.

The motivation is more important than the answer.

Problem. 95

Consider the figure below, where each triangle can be rotated and the numbers on the vertices rotate as well. Compositions of such rotations form a group G.



Answer the following questions:

(a) Is the group commutative?

(b) Determine the inverse of r.

(c) Determine the order of $r \circ s$.

(d) Does G have a subgroup of size 7?

Multiplication tables

Problem. 96

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

$\circ$	**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

(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. 97
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

(3)

(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. 98
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. 99

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. 100

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. 101

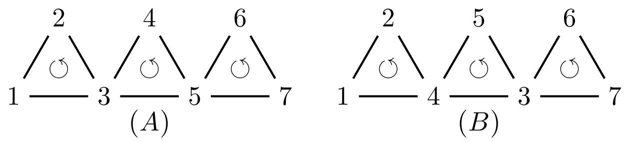
Prove that a permutation is even if and only if its inverse is even.

Problem. 102

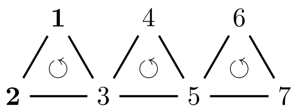
Let π be a permutation such that $\mathrm{order}(\pi)$ is odd. Prove that π must be even.

Problem. 103

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).



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. 104

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

Problem. 105

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

Problem. 106

(a) Determine the number of inversions in the permutation $(1\ 4\ 5\ 2)(3)$.

(b) Let $\pi \in S_8$ be a permutation with 6 inversions. What are the possible number of inversions of the permutation $\pi \circ (1\ 2) \circ (3\ 4)$?

Problem. 107

How many elements in S_8 can be expressed as a product of k disjoint transpositions, where

$$(a)\ k=1 \qquad (b)\ k=2 \qquad (c)\ k=3.$$

Problem. 108

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

Problem. 109

Let S_8 be the group of permutations on 8 elements.

(a) Find a cyclic subgroup of S_8 with 3 elements.

(b) Find an Abelian subgroup of S_8 with 9 elements that is not cyclic, and write down all its elements.

Problem. 110

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.

Group actions and Burnside's lemma

Problem. 111

Let S_n act on some set X. Show that if σ and π have the same type, then $|\operatorname{Fix}(\sigma)| = |\operatorname{Fix}(\pi)|$.

Problem. 112

The squares in a 2×3-rectangle X can be colored red, green or blue. A subgroup $G \subseteq \mathrm{S}_6$ act on X by permuting the two rows, or the three columns.

1. Show that $G \cong \mathrm{S}_3 \times \mathrm{S}_2$.
2. Find how many orbits there are of X under G.

Graph theory

Problem. 113

Draw the bipartite graph $K_{3,2}$ such that no edges cross — that is, it should be clear that $K_{3,2}$ is planar.

Problem. 114

Suppose that a 5-regular graph G admits two disjoint Hamiltonian cycles (they do not share any edges). Show that G has an edge-coloring using 5 colors.

Problem. 115

Let G_n, $n \geq 2$ be the graph defined on pairs of integers (a, b), $1 \leq a, b \leq n$, such that (a, b) is connected by an edge with (c, d) if and only if

$$|a - c| = 1 \text{ or } |b - d| = 1 \text{ or both.}$$

a) Compute the number of vertices G_n.

b) Show that the number of edges in G_n is $2(n-1)(n^2 - n + 1)$.

c) Prove that G_n is not planar for $n \geq 3$.

Problem. 116

Let G_n be the graph with vertex set $\{-n, -(n-1), \dots, -1, 1, 2, 3, \dots, n-1, n\}$, with $n \geq 2$. The edges of G are as follows: Every negative vertex has an edge with all other negative vertices. Every positive vertex has an edge with with all other positive vertices. Finally, we also have the edges $\{-1, 1\}$ and $\{-2, 2\}$.

(a) Draw G_4.

(b) For what n does G_n have an Euler trail?

(c) Show that G_n has a Hamiltonian cycle.

Problem. 117

A (simple) connected planar graph is called *silly* if every vertex has degree at least 2 and it has exactly three regions in a planar drawing — including the outer region.

(a) Draw a silly graph with 10 vertices.

(b) Show that a silly graph cannot have a vertex with degree 5 or more.

Problem. 118

A *forest* is a disjoint union of trees. Suppose a forest have 100 vertices and 80 edges, how many trees are there in the forest?

Problem. 119

Let G be a connected simple planar graph. Suppose that G is a *triangulation*, where every *bounded* region is bounded by exactly three edges.

Prove that we can color the bounded regions of G with 4 colors, such that regions sharing an edge have different colors.

Problem. 120

A connected planar graph G has been drawn with 5 regions and 9 vertices. Determine the number of edges in G.

Problem. 121

A connected simple planar graph G has degree d for every vertex. For $d = 3, 4, 5$, find the minimum number of edges in G and the corresponding number of vertices. Draw such graphs.

Problem. 122

A connected simple planar graph G has the property that there is no region with more than c edges around it, and every vertex has degree at least d. Let r be the number of regions and v be the number of vertices. Prove that

$$\frac{r}{v} \geq \frac{d}{c}.$$

Problem. 123

Determine the number of Hamiltonian paths in the graph K_n.

Problem. 124

Let G be a bipartite graph with an odd number of vertices. Show that G does not have a Hamiltonian cycle.

Problem. 125

Let $G = (V, E)$ be the graph consisting of the vectors (a, b, c) where $a, b, c \in \{0, 1, 2\}$. Two vectors are connected by an edge if and only if the Euclidean distance between them is 1. Prove that G does not have a Hamiltonian cycle. Furthermore, prove that there is no Hamiltonian path starting at $(0, 0, 0)$ and ending at $(1, 1, 1)$.

Problem. 126

Recall the notion of a *knight* in chess. A *knights tour* on a standard 8×8 chessboard is a path where a knight visits every square exactly once, and then end at the same square as where it started.

1. Prove that there is no knights tour on a $n \times n$ chessboard if n is odd.

2. Prove that there is no knights tour on a $4 \times n$ chessboard.

Problem. 127

Let $G = (V, E)$ be a plane graph, and let F denote the set of faces. Show that $\frac{1}{2}|F|$ of the faces can be marked such that every cycle in G contains an edge in a marked face. Prove that the bound is sharp.

Problem. 128

An *acyclic orientation* of G is an assignment of directions to each edge, such that there is no directed cycle in G.

(a) Prove that for any graph with at least one edge, the number of acyclic orientations is an even number.

(b) Prove that for any graph, there is at least one vertex with no outgoing edges (edges pointing out). Such a vertex is called a *sink*.

(c) Prove that for any orientation of K_n, there is always a unique sink.

(d) Prove that if G is an orientation, and we add a vertex v and all directed edges $u \to v$ for $u \in G$, then the new orientation on this new graph is also acyclic.

(e) Use induction on the number of vertices to prove that K_n has exactly $n!$ acyclic orientations.

Problem. 129

(This one is quite tricky!) Let G be a connected graph with 100 vertices (representing people) and each vertex has degree 5, (representing being friends on Facebook). We model an "epidemic" event as follows: 15 people starts to play Farmville. Every person who is friends with at least 3 other people playing Farmville, will also start to play the game. These new players will influence their friends and so on.

However, show that no matter how the graph looks like, there will always be some people who never starts to play Farmville.

Solutions

Solution. 1

(a) There are 4 independent choices, so 10^4.

(b) $10 \cdot 9 \cdot 8 \cdot 7$.

(c) Choose the remaining three: $9 \cdot 8 \cdot 7$.

(d) $\binom{10}{4}$.

(e) Pick two additional digits and count all permutations: $\binom{8}{2} \times 4!$.

These must be chosen in an unordered fashion, since we later count all 4! permutations of the unordered digits.

Solution. 2

It is easier to first count the number of forbidden shuffles. We have two different types of forbidden arrangements, see Fig. 3.

The number of decks with $A\heartsuit$ on top of $K\heartsuit$ is 51!, since we can remove the $A\heartsuit$, shuffle the remaining 51 different cards, and then place the ace of hearts on top of the king of hearts. In the same manner, we have 51! forbidden decks involving $A\spadesuit$.

Finally, we need to count the number of elements in the intersection, i.e., decks where both of the forbidden configurations occur. We remove $A\heartsuit$ and $A\spadesuit$, shuffle the 50 cards, and insert the aces on the respective kings. This gives 50! shuffles. The number of forbidden configurations is therefore $51! + 51! - 50!$, and the total number of good decks is

$$52! - 2 \times 51! + 50!.$$

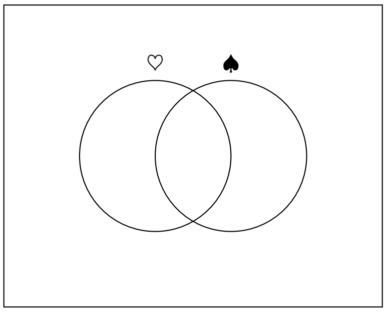


Figure 3: The total deck of cards, 52!, and the two intersecting forbidden subsets.

Solution. 3

Since there are duplicates of E, S and I, there are $11!/2^3$ different words.

Solution. 4

It is given by the multinomial coefficient

$$\binom{7}{2,2,3} = \frac{7!}{2! \times 2! \times 3!} = 210.$$

Solution. 5

It is given by the multinomial coefficient

$$\binom{8}{2,2,2,2} = \frac{8!}{2^4}$$

It is the same as counting number of different words we can create from `AABBCCDD`. For example, the word `ADCBBCDA` assign dish A to person 1 and person 8.

Solution. 6

It is easier to consider the couples as labeled. We first pick 2 people to form couple A, then 2 other people to form couple B and so on. The number of ways to create *labeled* couples is

$$\binom{8}{2,2,2,2} = \frac{8!}{2^4}.$$

However, all permutations of the 4 labels produce the same set of couples, so we need to divide this by 4!. The answer is therefore $\frac{8!}{4! \times 2^4}$.

Solution. 7

First, we sample the 5 types. That leaves space for 8 more, which we can choose freely, with repetition. The dots-and-bars formula tells us that there are

$$\binom{8+5-1}{5-1} = \binom{12}{4}$$

ways to do this.

Solution. 8

There are n types of derivatives and we need to select r of these with repetition allowed. Order does not matter in which we compute derivatives, so dots and bars give

$$\binom{r+n-1}{n-1}.$$

Solution. 9

Dots and bars give

$$\binom{r+n-1}{n-1}.$$

Solution. 10

Let $y_1 = x_1 - 2$, $y_2 = x_2 - 3$, $y_3 = x_3 - 10$ and $y_4 = x_4 + 3$.

We get a new equation where $y_i \geq 0$ and

$$(y_1 + 2) + (y_2 + 3) + (y_3 + 10) + (y_4 - 3) = 15, \qquad \Leftrightarrow$$
$$y_1 + y_2 + y_3 + y_4 = 3$$

Dots and bars gives $\binom{3+4-1}{4-1}$ integer solutions.

Solution. 11

We add one extra variable to turn the inequality to an equality:

$$x_1 + x_2 + x_3 + x_4 + s = 15, \qquad s, x_i \geq 0.$$

This gives $\binom{15+5-1}{5-1}$ integer solutions.

Solution. 12

We divide into cases. The only possible values for x_4 are $x_4 = 0, 1, 2, 3$, since otherwise the left hand side is too large.

Case $x_4 = 0$: We get $3(x_1 + x_2 + x_3) = 22$. No solutions as the right hand side is not a multiple of 3

Case $x_4 = 1$: We get $3(x_1 + x_2 + x_3) = 15$, so $x_1 + x_2 + x_3 = 5$ which has $\binom{7}{2} = 21$ solutions.

Case $x_4 = 2$: We get $3(x_1 + x_2 + x_3) = 8$, no solutions.

Case $x_4 = 3$: We get $3(x_1 + x_2 + x_3) = 1$, no solutions.

Therefore, there are 21 solutions in total.

Solution. 13

There are $k!S(n, k)$ surjections — the quantity $k!$ is responsible for the labeling.

Solution. 14

We first ride all rides once. That leaves 11 tokens which can be spent as we please. We can ride the roller coaster 0, 1 or 2 times with the remaining tokens:

- 0 **times**. We need to count non-negative integer solutions to $3h + 3c + 3w \leq 11$. This is the same as solving $h + c + w + r = 3$ where r represents the number of remaining tokens. Number of solutions: $C(3 + 4 - 1, 3)$
- 1 **time**. Same strategy gives non-negative solutions to $3h + 3c + 3w \leq 6$, or $h + c + w + r = 2$. This gives $C(2 + 4 - 1, 2)$ number of solutions.
- 2 **times**. After riding the coaster 2 times, we have one token left and cannot ride anything else. Only 1 solution.

Total number of ways: $\binom{6}{3} + \binom{5}{2} + 1 = 20 + 10 + 1 = 31$.

Solution. 15

This is equivalent with solving $3x_1 + 3x_2 + 3x_3 + 3x_4 + 3x_5 + 5y = 42$, $x_i, y \geq 0$. We see that $0 \leq y \leq 8$ (we cannot afford 9 rides on the expensive attraction).

Case by case analysis of y show that $y = 0$, $y = 3$, $y = 6$ are the only possible choices for the remaining tokens to be a multiple of 3. This means we can ride cheap rides either 4, 9 or 14 times, so we want to add up the number of solutions to

$$x_1 + \cdots + x_5 = R, \qquad R \in \{4, 9, 14\}.$$

This gives the total answer

$$\binom{4+5-1}{5-1} + \binom{9+5-1}{5-1} + \binom{14+5-1}{5-1}.$$

Solution. 16

This problem is not a clear-cut standard problem as in the introduction. However, the fact that each letter appears at least once imposes a lot of restriction, as we only need to decide which two additional letters to add to `abcd`.

This is a strong hint that we need to divide the problem into sub-cases. The fewer cases the better.

- We add two different letters. Thus, the letters appearing are one of `abbccd`, `abbcdd` or `abccdd`. To calculate the number of words we can make from `abbccd`, we use a multinomial coefficient, $\binom{6}{2,2,1,1}$.
- We add the same letter twice. This gives `abbbcd`, `abcccd` or `abcddd`, and each of these options give $\binom{6}{3,1,1,1}$ words.

Expanding the multinomials and putting it all together, there are in total

$$3\frac{6!}{(2!)^2} + 3\frac{6!}{3!}$$

words satisfying the requirements.

Solution. 17

Without the extra restriction, the number of ways to do this is $3!S(8,3)$: The Stirling number count ways to distribute the different questions into three non-empty sets and the $3!$ account for the different ways to distribute the sets among the students.

To construct the forbidden configurations, we can remove one of the easy questions and distribute the remaining 7 questions among the students. The student who gets the easy question is then also given the second easy question. We see that this can be done in $3!S(7,3)$ ways.

The final answer is therefore $3!S(8,3) - 3!S(7,3)$.

Solution. 18

The recursion for Stirling numbers tell us that

$$S(n+1,k+1) = (k+1)S(n,k+1) + S(n,k)$$
$$\Leftrightarrow$$
$$S(n+1,k+1) - S(n,k) = (k+1)S(n,k+1)$$

and since $(k+1)S(n,k+1) \geq 0$, the inequality must be true.

Solution. 19

We notice that if the positions of the `b`'s and `d`'s are fixed, then the positions of the remaining letters is uniquely determined by the restriction. For example,

$$\texttt{b}\square\square\texttt{d}\square\texttt{b}\square\texttt{d} \quad \Longrightarrow \quad \texttt{baadcbcd}.$$

To create a valid word, it is enough to first choose 2 positions of the 8 available for the `b`'s and then 2 positions for the `d`'s. This can be done in $\binom{8}{2,2,4} = \frac{8!}{2!\times 2!\times 4!}$ ways.

Solution. 20

There are two cases to consider, either the `A` in the third position is the first `A` in the word, or it is the second.

IF THE FIRST `A` appears in the third spot, the word is of the form `XXAY..YA..` with only `C`'s and `D`'s between the `A`'s, and the `X` are one of the letters in `BCD`.

There can be between 0 and 6 letters between the two `A`'s. The number of words with k letters between the `A`'s is given by $2^k \times 3^{8-k}$, since we need to choose either `C` or `D` for the k letters and there are three choices for each of the remaining $8-k$ spots. Summing over the possible values of k gives

$$\sum_{k=0}^{6} 2^k 3^{8-k} = 3^8 \sum_{k=0}^{6} \left(\frac{2}{3}\right)^k.$$

This is a geometric sum and the formula for geometric sum gives

Recall that $\sum_{j=0}^{n} r^j = \frac{1-r^{n+1}}{1-r}$.

$$3^8 \times \frac{1-(2/3)^7}{1-(2/3)} = 3^8 \times \frac{\frac{3^7-2^7}{3^7}}{1/3} = 3^2(3^7-2^7).$$

THERE ARE NOW TWO MORE CASES to consider — words of the forms `AYA...` or `XAA....` There are 2×3^7 words of the first form and 3^8 words of the second form.

Because the `Y` has two options, and the remaining open spots have three

ADDING THE RESULTS FOR ALL CASES give us in total

$$3^9 - 9\times 2^7 + 2\times 3^7 + 3^8.$$

Solution. 21

There are 10! ways to distribute the numbers without any restriction. However, for each square, only one of the two choices is valid — if it is invalid, we can switch the number to the left of the gray square with the number below. These switches can be done independently, so there are therefore $10!/2^5$ ways to fill in the boxes in the prescribed manner.

A different solution would be that we select an (unordered) pair for each gray square and place them in a valid fashion. Picking 5 pairs (one for each gray box), gives $\binom{10}{2,2,2,2,2}$ choices.

Solution. 22

Order of drinks does not matter, and there are $3\times 2 = 6$ different types of drinks. The stars and bars method gives

$$\binom{5+6-1}{6-1} = \binom{10}{5} = \frac{10\cdot 9\cdot 8\cdot 7\cdot 6}{5\cdot 4\cdot 3\cdot 2} = \frac{20\cdot 9\cdot 4\cdot 7\cdot 6}{20\cdot 6} = 36\cdot 7 = 252$$

ways of ordering drinks.

Solution. 23

Let x_i be the number of candies of type i. We seek the number of solutions to

$$4x_1 + 4x_2 + 4x_3 + 4x_4 = 40 \iff x_1 + x_2 + x_3 + x_4 = 10$$

with $x_i \geq 0$. The bars-and-stars formula tell us that the number of solutions is

$$\binom{10+3}{3} = \frac{13!}{10!3!} = \frac{13 \times 12 \times 11}{6} = 13 \times 11 \times 2 = 286.$$

(b) Divide into cases, depending on the number of 5 sek candies you buy. Since you need to spend all the money, and each small candy is worth 4 sek , one can only buy a multiple of four of the 5 sek candy. Thus, one can buy 0, 4 or 8 pieces of the expensive candy.

In each case (after dividing by 4) one can then use stars and bars to solve the problem (since the candies are unordered — it does not matter in which order they are put in the bag). That gives

$$\binom{10+4-1}{4-1} + \binom{5+4-1}{4-1} + 1$$

different bags.

Solution. 24

(a) We want to partition 10 people into groups of 2. This is a multinomial coefficient, but we need to divide by 5! as the order of the groups does not matter:

$$\frac{1}{5!}\binom{10}{2,2,2,2,2} = \frac{1}{5!}\frac{10!}{2^5} = \frac{10 \cdot 9 \cdot 8 \cdot 7 \cdot 6}{8 \cdot 2 \cdot 2} = 5 \cdot 9 \cdot 7 \cdot 3 = 15 \cdot 63 = 945.$$

(b) We have 5 different teams to be partitioned into two non-empty, unordered groups. Thus is $S(5,2) = 15$. This can be computed as $2^4 - 1 = 15$, since team 1 first pick a van, and then among the 4 remaining teams, we pick a subset that sit in the same van as team 1. However, one choice is forbidden — not all teams can be in the first van. This gives 15 options. Another way to compute $S(5,2)$ is to use the recursion.

Solution. 25

We first choose which color to exclude. There are 3 options. We now have 5 stripes remaining, where there are two pairs of stripes of the same color. The number of ways to arrange these stripes is $\binom{5}{2,2,1} = \frac{5!}{2!2!} = 30$. The answer is therefore $3 \cdot 30 = 90$.

Solution. 26

First of all, by putting 8 rooks on one of the diagonals, we see that it is possible to place 8 non-attacking rooks on a board.

However, if we place 9 or more rooks on the board, there will be some row with at least two rooks. These can attack each other. The answer is therefore 8 rooks.

Solution. 27

There are $2^{10} = 1024$ different selections of dishes, but the price for each such selection lies between 0 and 1000 yuan. Hence, there must be two different selections[10] of dishes with the same price. Let S_1 and S_2 be two such selections. It can be the case that there are some common dishes in S_1 and S_2, but these can be removed from the selections, and we still have that the price of both selections are the same.

[10] At least!

Solution. 28

Define the following sets:

$$\begin{aligned} T_1 &= \{1, 2^1, 2^2, 2^3, \dots\}, \\ T_3 &= \{3, 3 \cdot 2^1, 3 \cdot 2^2, 3 \cdot 2^3, \dots\}, \\ T_5 &= \{5, 5 \cdot 2^1, 5 \cdot 2^2, 5 \cdot 2^3, \dots\}, \\ &\dots \\ T_{2n-1} &= \{(2n-1), (2n-1) \cdot 2^1, (2n-1) \cdot 2^2, (2n-1) \cdot 2^3, \dots\}, \end{aligned}$$

where we have n such sets in total. Every integer in $I = \{1, 2, \dots, 2n\}$ is of the form $q \cdot 2^k$ for some odd number $q < 2n - 1$, and thus in T_q. Therefore, $I \subseteq T_1 \cup T_2 \cup \cdots \cup T_{2n-1}$. Furthermore, if we take any two different numbers, $a = q \cdot 2^i$ and $b = q \cdot 2^j$ from T_q with $i < j$ then $a|b$.

Finally, among $n + 1$ numbers from I, at least two of these belong to the same T_q since we only have n such sets. But in that case, the above argument showed that the smaller divides the larger.

Solution. 29

IN THE LEFT HAND SIDE, we choose r people among n people.

IN THE RIGHT HAND SIDE, the first m of the n people are given hats. To choose r among the n people, we can independently pick k of the hat-less people and $r - k$ of hat-people. Summing over all values of k then simply gives an r-subset of n people.

This is not a choice! We refine the situation by asking how many of the first m people are chosen. To help you visualize the situation, they are given hats.

Solution. 30

LEFT HAND SIDE. There's gonna be a party in a village with n people: 2 out of n people will definitely go and bring pizza. The remaining $n - 2$ people, might, or might not go.

This gives $\binom{n}{2}$.

RIGHT HAND SIDE. We sum over total number k of party people. First choose party subset of size k out of the n people. Then, among the party people, we choose two people who bring pizza.

Solution. 31

LEFT HAND SIDE. There are n people in a restaurant choosing among three wines, A, B and C, where B and C are non-alcoholic.

One person is chosen to be a designated driver, and thus has only two options. Hence, the interpretation for the left hand side is

$$\underbrace{n}_{\text{Designated driver}} \times \underbrace{2}_{\text{Drivers wine choice}} \times \underbrace{3^{n-1}}_{\text{Remaining wine choices}}.$$

Right hand side. We sum over the number of people, k, who choose either B or C. The "sober" people can thus be selected in $\binom{n}{k}$ ways. The designated driver must be chosen among these k people. Finally, the k sober people (including driver) make up their mind about B or C. The interpretation is therefore

The ones not selected here must therefore take wine A.

$$\sum_{k=1}^{n} \underbrace{\binom{n}{k}}_{\text{People choosing } B/C} \times \underbrace{k}_{\text{Designated driver}} \times \underbrace{2^k}_{\text{Choice of } B/C}.$$

In both sides, we see that the same story is told.

Solution. 32

Left hand side. There are $a+b$ people going to party — a of these bring food and b bring drinks. Some might bring both food and drinks, while other people bring nothing.

In other words, the choice of who brings food and who brings drinks is done independently, hence the multiplication.

Right hand side. We refine over the number, k, of of people who bring both food and drinks. First, we select these k generous people. Among the remaining $a+b-k$ people, we select the $a-k$ ones who only bring food. This leaves b people so far without a task and we select $b-k$ people of these who bring drinks. The interpretation of the coefficients in the right hand side is therefore

$$\sum_{k=0}^{a+b} \underbrace{\binom{a+b}{k}}_{\text{Brings both}} \times \underbrace{\binom{a+b-k}{a-k}}_{\text{Food only}} \times \underbrace{\binom{b}{b-k}}_{\text{Drinks only}}.$$

Solution. 33

Left hand side. There are $n+r+1$ people in total. We first pick a number $k = 0, 1, \dots, r$, and give hats to the first $n+k$ people. From the people with hats, we select k of the hats and paint them blue. Note that person $n+r+1$ never gets a hat.

Right hand side. Here we have subsets of exactly size r among $n+r+1$ people. Suppose we have such a subset S. There are two cases to consider:

- S does not contains person $n+r+1$. Then S is an r-subset of the first $n+r$ people. In this case, we give hats to the first $n+r$ people and paint r hats blue according to S.

This corresponds to the $\binom{n+r}{r}$ term in the left hand side.

- S do contain person $n+r+1$. In this case there is a smallest integer i, $0 \leq i < r$, such that
$$\{n+i+1, n+i+2, \dots, n+r+1\} \subseteq S.$$

With this in mind, the set $T = S \cap \{1, 2, \ldots, i-1\}$ contains i elements. We now give hats to the first $n+i$ people, and the subset of these with blue hats is determined by the set T.

This corresponds to the $\binom{n+i}{i}$ term.

Solution. 34

LEFT HAND SIDE. We have $m+n$ people, m with red hats and n with blue hats, and we count the subsets of size n.

RIGHT HAND SIDE. Remember that $\binom{n}{k} = \binom{n}{n-k}$, so that the right hand side is equal to

$$\sum_{k=0}^{n} \binom{m}{k}\binom{n}{n-k}.$$

We refine by the number, k, of people in our subset that have red hats. To create an n-subset of the $m+n$ people, we select k with red hats, and $n-k$ people blue hats, which is independent choice.

Solution. 35

LEFT HAND SIDE. We have $m+n$ people, m with red hats and n with blue hats, and we count the subsets of size k.

RIGHT HAND SIDE. We refine by the number, i, of people in our subset that have red hats. To create a k-subset of the $m+n$ people, we select i with red hats, and $k-i$ people blue hats, which is independent choice.

Solution. 36

IN THE LEFT HAND SIDE, there are n people who go on a wine tour. Since they are responsible adults, one person is selected to be the designated driver and he must stay sober. Each of the remaining $n-1$ adults can pick — independently — one out of 4 options from a menu, where the last menu item is the non-alcoholic option.

There are n choices.

IN THE RIGHT HAND SIDE, we first choose a k-subset of people who prefers one of the first three options. They then pick which of these they like. The designated driver cannot, of course, be among these k people, and is selected among the remaining $(n-k)$ people — all who also pick the non-alcoholic option. By summing over all possible values of k, we see that the situation agrees with the left hand side.

AN ALTERNATIVE SOLUTION is to expand $(3x+y)^n$ using the binomial theorem, take the derivative with respect to y on both sides, and then put $x = y = 1$.

Solution. 37
First multiply both sides with $n+1$. We need to prove

$$\sum_{k=0}^{n} \frac{n+1}{k+1}\binom{n}{k} = 2^{n+1}-1.$$

Now note that

$$\frac{n+1}{k+1}\binom{n}{k} = \frac{(n+1)n!}{(k+1)k!(n-k)!} = \frac{(n+1)!}{(k+1)!(n-k)!} = \binom{n+1}{k+1}.$$

Thus we need to prove that

$$\sum_{k=0}^{n}\binom{n+1}{k+1} = 2^{n+1}-1$$
$$\sum_{k=1}^{n+1}\binom{n+1}{k} = 2^{n+1}-1$$
$$\sum_{k=0}^{n+1}\binom{n+1}{k} = 2^{n+1}$$

but the last line is the binomial theorem.

Solution. 38
There are at least three possible approaches. A pure algebraic proof, by manipulating expressions involving factorials. A second approach is to use induction induction over n, using $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$. The third solution is to use a combinatorial argument: In the left hand side, we have $n+2$ people, n students and the teachers Svante and Per. We choose k among these. In the right hand side, we consider the possible choices where there are no teachers among the k selected, exactly one teacher, or both teachers present.

Solution. 39
First multiply both sides with $n+1$. We need to prove

$$\sum_{k=0}^{n} \frac{n+1}{k+1}\binom{n}{k} = 2^{n+1}-1.$$

Now note that

$$\frac{n+1}{k+1}\binom{n}{k} = \frac{(n+1)n!}{(k+1)k!(n-k)!} = \frac{(n+1)!}{(k+1)!(n-k)!} = \binom{n+1}{k+1}.$$

Thus we need to prove that

$$\sum_{k=0}^{n}\binom{n+1}{k+1} = 2^{n+1}-1 \iff \sum_{k=1}^{n+1}\binom{n+1}{k} = 2^{n+1}-1 \iff \sum_{k=0}^{n+1}\binom{n+1}{k} = 2^{n+1}$$

but the last line is the binomial theorem.

Solution. 40
There are several natural bijections. We shall construct a bijection using recursion over n. The base case is $n=1$, and we let f send the permutation 1 to the vector 1. Suppose now we are given $\pi \in \mathrm{S}_n$,

and we want to construct $w \in Q_n$. We let w_n be the position of n in π. Then, let π' be the permutation obtained from π, with element n removed, so that $\pi' \in \mathrm{S}_{n-1}$. We then let $w' = f(\pi')$ by recursion, and the remaining entries in w are determined by setting $w_i = w'_i$ for $i < n$.

The key property here is to note that given a permutation $\pi' \in \mathrm{S}_{n-1}$, and an integer w_n, with $1 \leq w_n \leq n$, we can uniquely recover π by inserting n at position w_n in π'. This shows that every step in the recursion is a bijection, and it follows that w uniquely determines π.

HERE IS AN EXAMPLE on how we can construct the word w from the permutation $[7, 6, 8, 3, 1, 9, 4, 2, 5]$.

$$\begin{aligned}
[7,6,8,3,1,9,4,2,5] &\sim [] \\
[7,6,8,3,1,4,2,5] &\sim [6] \\
[7,6,3,1,4,2,5] &\sim [3,6] \\
[6,3,1,4,2,5] &\sim [1,3,6] \\
[3,1,4,2,5] &\sim [1,1,3,6] \\
[3,1,4,2] &\sim [5,1,1,3,6] \\
[3,1,2] &\sim [3,5,1,1,3,6] \\
[1,2] &\sim [1,3,5,1,1,3,6] \\
[1] &\sim [2,1,3,5,1,1,3,6] \\
[] &\sim [1,2,1,3,5,1,1,3,6]
\end{aligned}$$

In the first step, we find the largest element (which is 9) in the permutation, and insert its position in w. This determines the last element in w. In the second step, we find the new largest element (which is 8) in the permutation, and insert its position in w. Repeat this process until the permutation is empty.

Below is a Mathematica implementation of the above bijection.

```
(* Base case. *)
f[{1}]:={1};

(* General case. *)
f[pi_List]:=With[{n=Max@pi},
Append[
  (* Apply bijection to pi' to get
     all but the last entry of w *)
  f[DeleteCases[pi,n]]
  ,
  (* The position of n in pi is the
     last entry in w. *)
  Position[pi,n][[1,1]]
]];
```

Solution. 41

IN ORDER TO DESCRIBE a bijection f, we must have a way to construct an element in C_n, given some binary word $w \in B_{n-1}$. The easiest way to do this is to give an example. In general, one has to be careful and argue that the construction is indeed a bijection.

EXAMPLE: $n = 9$, $w =$ `00110101`. We draw 9 balls and put the digits of w between the balls.

$$\bigcirc_0 \ \bigcirc_0 \ \bigcirc_1 \ \bigcirc_1 \ \bigcirc_0 \ \bigcirc_1 \ \bigcirc_0 \ \bigcirc_1 \ \bigcirc$$

The 1s in the binary word are replaced by separators, and we count the number of balls between the separators.

$$\bigcirc \quad \bigcirc \quad \bigcirc | \quad \bigcirc | \quad \bigcirc \quad \bigcirc | \quad \bigcirc \quad \bigcirc | \quad \bigcirc$$

3 1 2 2 1

The final list of integers, $(3, 1, 2, 2, 1)$, has total sum 9 and we have that $f(00110101) = (3, 1, 2, 2, 1)$.

SINCE WE START with n balls, we are sure that the method above results in a list with sum n. Moreover, since there is at most one separator between two adjacent balls, we are sure that the integers are positive. Hence, the procedure above does give an integer composition of n. Given $\alpha \in C_n$, we also fairly easy see how to reverse the steps outlined above and recover a corresponding binary word in B_{n-1}. Hence, the map f is a bijection.

Solution. 42

Let P_n be the set of permutations of $\{1, 2, 3, \dots, n\}$ ending with a 1, and let T_n be the set of increasing trees on n vertices.

GIVEN A PERMUTATION in P_n, we construct the edges of a decreasing tree as follows: For each number $i \geq 2$ in P, find the first number $j < i$ to the right of i. Then we let $i \to j$ be an edge in the tree. Since 1 is the rightmost number in P it is evident that such a j always exists. By construction, we cannot have two edges $i \to j_1$ and $i \to j_2$ where $i > j_1$ and $i > j_2$, and it also follows that every vertex $i > 2$ is connected to a unique smaller vertex. This ensures that the resulting edges really describe a tree in T_n.

IN THE OTHER DIRECTION, given a decreasing tree in T_n, we can invert the above construction as follows: First start with the permutation $\pi = 1$. We visit the vertices $i = 2, 3, \dots$ in the tree in this order, and if vertex i is a child of j, then insert i directly after j in the permutation, until we have processed all vertices. The result is a permutation $\pi \in P_n$.

FOR EXAMPLE, the tree in the question corresponds to the permutation 524387961.

Solution. 43

First number the spots in the line, 12345. Let A be the event that the people at spots 123 are in height order, B be the event that 234 are in order and C the event that 345 are in order.

We seek $5! - |A \cup B \cup C|$ where the last term is computed via inclusion-exclusion. Notice that $|A| = |B| = |C| = \binom{5}{3}2!$ since we choose three out of the five people to be in order, and then put the remaining two people in the two possible ways in the last two spots. In the same manner, it follows that $|A \cap B| = |B \cap C| = \binom{5}{4}$. However, $|A \cap C| = 1$ and $|A \cap B \cap C| = 1$, since this means that the people in all five spots must appear in increasing order. Thus, there are

$$5! - 3\binom{5}{3} \cdot 2! + \left[2\binom{5}{4} + 1\right] - 1$$

different valid lines of people.

Solution. 44

Let our sets A_1, A_2 A_3 and A_4 be the decks where *king i is on top of ace i.*

We computed before that $|A_1| = 51!$, and $|A_1 \cap A_2| = 50!$. Similarly, $|A_1 \cap A_2 \cap A_3| = 49!$ and $|A_1 \cap A_2 \cap A_3 \cap A_4| = 48!$. Therefore, the number of forbidden decks is

$$\binom{4}{1}|A_1| - \binom{4}{2}|A_1 \cap A_2| + \binom{4}{3}|A_1 \cap A_2 \cap A_3| - \binom{4}{4}|A_1 \cap A_2 \cap A_3 \cap A_4|$$

This evaluates to

$$4 \cdot 51! - 6 \cdot 50! + 6 \cdot 49! - 1 \cdot 48!$$

and the number of good decks is then

$$52! - 4 \cdot 51! + 6 \cdot 50! - 6 \cdot 49! + 1 \cdot 48!.$$

Solution. 45

Let our sets A_1, A_2 A_3 and A_4 be the decks where *king i is on top of an ace.*

Now,

- $|A_1| = 4 \cdot 51!$, since there are 4 aces to put below king 1.
- $|A_1 \cap A_2| = 4 \cdot 3 \cdot 50!$, there are 4 aces for king 1, and 3 remaining ace-choices for king 2.
- $|A_1 \cap A_2 \cap A_3| = 4 \cdot 3 \cdot 2 \cdot 49!$, and
- $|A_1 \cap A_2 \cap A_3 \cap A_4| = 4! \cdot 48!$.

Same reasoning as before gives that the number of good decks is

$$52! - 4(4 \cdot 51!) + 6(4 \cdot 3 \cdot 50!) - 6(4 \cdot 3 \cdot 2 \cdot 49!) + 1(4! \cdot 48!).$$

Solution. 46

Let $A_1, \dots, A_5$ be the possible plates where country i *not* represented. We are interested in $|(A_1 \cup \dots \cup A_n)^c|$, which is then given by

$$\binom{50}{8} - 5\binom{40}{8} + \binom{5}{2}\binom{30}{8} - \binom{5}{3}\binom{20}{8} + \binom{5}{4}\binom{10}{8} - 0$$

Solution. 47

Let A_i be the events where box i empty. Inclusion-exclusion gives that $|A_1 \cup A_2 \cup \dots \cup A_n|$ is equal to

$$\binom{k}{1}(k-1)^r - \binom{k}{2}(k-2)^r + \binom{k}{3}(k-3)^r + \dots + (-1)^k\binom{k}{k-1}(1)^r$$

by choosing which box that is definitely empty, then two boxes which are definitely empty, and so on. Thus, the number of arrangements where *no* box is empty is given by

$$\sum_{j=0}^{k}(-1)^j\binom{k}{j}(k-j)^r.$$

Solution. 48

As in the previous exercise of same flavor, let us number the spots, and let A be the event that the people at spots 123 are in height order, B be the event that 234 are in order and C the event that 345 are in order.

We seek $5! - |A \cup B \cup C|$ where the last term is computed via inclusion-exclusion.

First note that

$$|A| = |B| = |C| = \binom{5}{3} \times 2 \times 2$$

as we first pick a 3-subset to of the people to put at the spots, then decide if they should be standing in increasing or decreasing order, and finally the remaining two people have two ways to stand in the remaining spots.

Because of symmetry, $|A \cap B| = |B \cap C|$. To have $A \cap B$, we note that the people standing at 1234 must all be sorted in the same way. Similar to the previous reasoning, this gives

Either 123 and 234 are increasing, or 123 and 234 are both decreasing

$$|A \cap B| = |B \cap C| = \binom{5}{4} \cdot 2.$$

To compute $|A \cap C|$, we need to consider different subcases.

- *A increasing and C increasing.* This forces the tallest guy to stand in the middle. We then choose 2 out of the 4 remaining to stand in front. This uniquely determines the configuration, so there are $\binom{4}{2}$ such configuration.
- *A decreasing and C increasing.* Also $\binom{4}{2}$.

- *A increasing and C increasing.* They must all be standing in increasing order. Only one way.
- *A decreasing and C decreasing.* Only one way.

Adding everything up, $|A \cap C| = 2\binom{4}{2} + 2$.

Finally, $|A \cap B \cap C|$ has only two options — everything increasing or everything decreasing. The final answer is therefore

$$5! - 3 \times 4 \times \binom{5}{3} + \left(2 \cdot 2 \cdot \binom{5}{4} + 2\binom{4}{2} + 2\right) - 2.$$

Solution. 49

There are $(5 \cdot 4) \cdot 3!$ permutations where 1 is in a 3-cycle, as we need to choose a and b in $(1\ \ a\ \ b)$, and then permute the remaining 3 elements. Same calculation holds for 2.

Now, how many permutations are there were both 1 and 2 are in 3-cycles? Two cases — either they are in separate 3-cycles,

$$(1\ a\ b)(2\ c\ d)$$

which gives 4! options, or, we have one of the cases

$$(1\ 2\ a) \text{ or } (1\ a\ 2).$$

This gives $2 \cdot 4 \cdot 3!$ additional number of cases.

Inclusion-exclusion now gives

$$6! - 2 \cdot 5! + (4! + 2 \cdot 4!) = 4! \cdot (6 \cdot 5 - 2 \cdot 5 + 3) = 4! \cdot 23.$$

Solution. 50

(a) There are $8 \times 7 \times \cdots \times 3$ ways.

(b) There are $(8 \times 7 \times 6) \times (5 \times 4 \times 3)$ ways.

(c) There are $\frac{1}{2}(8 \times 7 \times \cdots \times 3)$ ways, since the lines two pairs of lines (abc, def) and (def, abc) are considered equal configurations.

(d) There are $\binom{8}{6}$ ways.

(e) We first choose 6 people, and then choose 3 of these to be in group A: $\binom{8}{6}\binom{6}{3}$ ways.

(f) There are $\frac{1}{2}\binom{8}{6}\binom{6}{3}$ ways.

(g) There are $\binom{8}{6}\frac{1}{3!}\binom{6}{2,2,2}$ ways.

Solution. 51

(a) There is only one way.

(b) There is only one way.

(c) Bars and stars give $\binom{6+2}{2}$ ways.

(d) Bars and stars give $\binom{3+2}{2}$ ways.

(e) This is the same as counting integer partitions of 6 into 3 parts. We get three ways, $4+1+1$, $3+2+1$ and $2+2+2$.

(f) Same as previous question, but we can have as many piles as we like. We get 11 ways,

6	5+1	4+2	3+3
4+1+1	3+2+1	2+2+2	3+1+1+1
2+2+1+1	2+1+1+1+1	1+1+1+1+1+1.	

Solution. 52

(a) Each of the 6 spots has 8 options: 8^6.

(b) Also 8^6.

(c) We get $8^3 + \frac{1}{2} \times 8^3(\times 8^3 - 1)$ (the number of cases where groups are identical, plus number of cases where groups are different).

(d) Bars and stars give $\binom{6+8-1}{8-1}$ ways — the bars separate types.

(e) Bars and stars for each labeled group gives $\binom{3+8-1}{8-1}^2$.

(f) Bars and stars, but take into consideration when groups are equal, and not equal:

$$\binom{3+8-1}{8-1} + \frac{1}{2}\binom{3+8-1}{8-1}\left(\binom{3+8-1}{8-1} - 1\right).$$

(g) There are $\binom{2+8-1}{8-1}$ possible groups of size 2 — let this number be m. Then there are

$$\binom{m}{3} + m(m-1) + m = \binom{\binom{9}{7}}{3} + \binom{9}{7}\left(\binom{9}{7} - 1\right) + \binom{9}{7}$$

ways to make three equal-sized unlabeled groups. The terms represents the cases when all groups different, two groups equal, and all three groups equal, respectively.

(h) This is the same as counting surjections $f : A \to B$, where $|A| = 10$ and $|B| = 8$, since every person in A picks a type in B, and every type is chosen at least once. The number of such surjections is $8!S(10, 8)$, where $S(10, 8)$ is a Stirling number of the second kind.

Solution. 53

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. 54

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. 55

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. 56

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. 57

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. 58

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

Solution. 59

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. 60

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. 61

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. 62

This is left as an exercise for the moment.

Solution. 63

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. 64

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. 65

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. 66

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. 67

The last question has answer $4(x+1)\left(x^2+3x+4\right)$.

Solution. 68

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. 69

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. 70

Suppose $a^k = e$ for some integer k. Multiplying both sides with a^{-k} gives $e = a^{-k}$. In other words, $a^k = e \Longleftrightarrow a^{-k} = e$. 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. 71

Starting from $x \circ g = g \circ x$, we can multiply both sides from the right and from the left with x^{-1}. This gives the first identity.

We do proof by induction over k. The case $k = 1$ is given. Now suppose $x^{k-1} \circ g = g \circ x^{k-1}$. Multiply both sides on the right with x. This gives $x^k \circ g = (x \circ g) \circ x^{k-1}$. On the parenthesis, use the given fact that $x \circ g = g \circ x$, and we get $x^k \circ g = (g \circ x) \circ x^{k-1}$. Thus, $x^k \circ g = g \circ x^k$ for all $k \geq 1$ and we are done by the principle of mathematical induction.

Solution. 72

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 $(ab)^k = e \Longleftrightarrow (ba)^{-k} = e$.

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

Solution. 73

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. 74

Let H be the smallest subgroup containing a and b. Since H contains the cyclic subgroup $\{a, a^2, \ldots, a^m\}$, we have by Lagrange that

m divides $|H|$. The same reasoning for powers of b show that n divides $|H|$. Since $\gcd(m,n) = 1$, we have that mn divides $|H|$.

Now, since $ab = ba$, we have that

$$H' = \{a^i b^j : 1 \leq i \leq m, 1 \leq j \leq n\}$$

is a set which is closed under multiplication, so this is a subgroup of G containing a and b. Hence, $|H| \leq |H'|$. But, $|H'| = mn$, so $|H'| = |H|$ and we are done.

Solution. 75

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. 76

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. 77

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

Why is $\text{order}(a) = |H|$ true?

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

Solution. 79

We show the equivalence as follows:

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

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. 80

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. 81

(a) Let $e(x) = x$. Then it is easy to verify that $e(f(x)) = f(e(x)) = f(x)$, so $e(x)$ is the group identity. To find the inverse of $3x+5$, we set $y = 3x+5$ and solve for y. This gives $x = \frac{y-5}{3}$, so $h^{-1}(x) = \frac{1}{3}x - \frac{5}{3}$.

(b) We can take $f(x) = -x$. Then $f(f(x)) = -(-x)) = x$, so it has order 2.

Note that $k(x) = \frac{1}{x}$ also fulfills that $k(k(x)) = x$, but $k(x) \notin G$, so this is not a correct answer.

(c) Let $f(x) = ax+b$. If f has order n, $f^{\circ n}(x) = x$. We can compute that $(f \circ f)(x) = a(ax+b)+b = a^2x+ab+b$, and in general, $f^{\circ n}(x) = (f \circ f \circ \cdots \circ f)(x)$ is of the form

$$a^n x + b(a^{n-1} + a^{n-2} + \cdots + a + 1).$$

For this to be equal to x, we need that $a^n = 1$. If n is odd, $a = 1$, which forces $b = 0$. But in this case, $f(x) = e(x)$, and thus there are no elements of odd order ≥ 3. For n even, we also have the possibility that $a = -1$. In this case, $f(x) = -x+b$ for $b \in \mathbb{Q}$. We verify that $f(f(x)) = -(-x+b)+b = x$, so all elements of this form has order 2. Thus, the elements with a finite order in G are x and $-x+b$ for $b \in \mathbb{Q}$.

Solution. 82

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

$\{0,3,6,9\}$	By adding $0,3,6$ or 9 to H
$\{1,4,7,10\}$	By adding $1,4,7$ or 10 to H

$\{2,5,8,11\}$ By adding $2,5,8$ or 11 to H.

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

Solution. 83

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. 84

Case by case checking shows that

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

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[11] subgroup is therefore the one generated by 2, namely $\{0,2\}$. The subgroups are therefore

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

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

Solution. 85

We have

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

and

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

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. 86

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.

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. 87

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:

$$\begin{array}{ccccccc}
\{e\} & \longrightarrow & 12\mathbb{Z}_2 & \longrightarrow & 6\mathbb{Z}_4 & \longrightarrow & 3\mathbb{Z}_8 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
8\mathbb{Z}_3 & \longrightarrow & 4\mathbb{Z}_8 & \longrightarrow & 2\mathbb{Z}_{12} & \longrightarrow & \mathbb{Z}_{24}
\end{array}$$

Solution. 88

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. 89

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 $5 \times 3 \times$

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

$2 = 30$ divisors, as for each prime number p in the factorization of n, we must choose how many times it appear in a divisor.

Solution. 90

(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

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

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. 91

Note that by multiplying both sides in the second equation by x^{-1} from the right, we have that $y = b^{-1}ab$, so we have found y. We substitute this into the first equation, $x^2 = b^2(b^{-1}ab)a = baba = (ba)^2$, so $x = ba$ is one such solution. Hence, $y = b^{-1}ab$ and $x = ba$ solves the system.

Solution. 92

We have that $1, 2, 4, 7, 8, 11, 13, 14$ are the invertible elements in $\mathbb{Z}_{15}^{\times}$, that is, all integers in $\mathbb{Z}_{15}$ which are relatively prime with both 3 and 5.

For the inclusion-exclusion, note that $\mathbb{Z}_{pq}$ has pq elements. We remove all multiples of p (there are q of them), and remove all multiples of q (there are p of them). No number in $0, 1, 2, \ldots, pq - 1$ is a multiple of both p and q, except the number 0, which we have removed twice, so this is added. This gives $pq - p - q + 1$ elements left which are not divisible by either p or q. These are exactly the invertible elements.

We know that for any $g \in G$, where G is a finite group, that $g^{|G|} = 1$. Thus, $g^{(p-1)(q-1)} = 1$ for every $g \in \mathbb{Z}_{pq}^{\times}$, since we just proved that $|\mathbb{Z}_{pq}^{\times}| = (p-1)(q-1)$.

Solution. 94

(a) We can take $H = \{0, 12, 24, 36, 48\}$.

(b) Since K is a group, it is closed under group operations. For example, $4, 57 \in K$ implies that $4 + 57 \in K$. Now, $4 + 57 = 1$ with the operator $+$ in $\mathbb{Z}_{60}$. Therefore, $1 \in K$. Since 1 generates G (every element in G is of the form $1 + 1 + \cdots + 1$), it follows that $K = G$, and K is generated by 1.

Solution. 95

No, it is not commutative. It is easy to verify that $r \circ s \neq s \circ r$.

The inverse of r is r^2, since $r^3 = 1$. Rotating a triangle 3 times takes you back to where you started.

One can see that $r \circ s$ correspond to a permutation which has only one cycle of length 5. Thus this element has order 5.

All compositions of rotations can be seen as permutations in S_5. In particular, it is a subgroup of S_5. Since $|S_5| = 120$, and 120 is not divisible by 7, it cannot be the case that G has a subgroup of size 7 — this follows from Lagrange's theorem.

Solution. 96

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 $x = a^{-1}fc^{-1}$. 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. 97

(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. 98

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. 99

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. 100

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. 101

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. 102

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. 103

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. 104

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. 105

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. 106

In one line form, $(1\ 4\ 5\ 2)(3)$ is equal to $[4,1,3,5,2]$. For each entry we write how many entries to the right which are smaller:

$$4_3 1_0 3_1 5_1 2_0$$

Adding up the subscripts gives 5 inversions.

We proved in class that a simple transposition either increase or decrease the number of inversions by exactly one. Since we apply two disjoint transpositions, we can either have ± 2 or no change in the number of inversions. Hence, the answer is $4, 6$ or 8.

Solution. 107

Each transposition must be a pair of numbers. For $k = 3$, we need to select 3 disjoint pairs among 8 element. We use a multinomial coefficient, $\binom{8}{2,2,2,2}$. However, the order of the pairs do not matter, for example

$$(12)(34)(56) \text{ and } (56)(12)(34)$$

represent the same permutation in S_8. We need to divide by 3!.

The same reasoning gives that the answers for the different values of k are $\binom{8}{2}$, $\frac{1}{2!}\binom{8}{2,2,4}$ and $\frac{1}{3!}\binom{8}{2,2,2,2}$ respectively.

Solution. 108

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. 109

(a) The permutation $\pi = (123)$ written in cycle notation generates a cyclic subgroup of order 3, namely $\{id, (123), (132)\}$. (b) We can take all possible combinations of the permutations (123) and (456) and their products. This gives the permutations

$$\{id, (123), (132), (456), (123)(456), (132)(456), (465), (123)(465), (132)(465)\}.$$

We know that the order of a permutation is the least common multiple of the lengths of the cycles, so clearly, the order of the elements here is always 3 or 1. Thus, this group cannot be cyclic, as every finite cyclic group has a generator with the same order as the size of the group. The group is Abelian — the (123) and the (456)-cycles do not interact, and both (123) and (456) generate Abelian subgroups.

Solution. 110

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

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

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

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

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

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

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

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

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.

Solution. 111

Since the permutations have the same type, there is some τ such that $\pi = \tau^{-1} \sigma \tau$. Now,

$$\operatorname{Fix}(\pi) = \{x \in X : \pi x = x\} = \{x \in X : \tau^{-1} \sigma \tau x = x\}.$$

We can now multiply both sides in the identity with τ, and get

$$\operatorname{Fix}(\pi) = \{x \in X : \sigma(\tau x) = (\tau x)\}.$$

We have that $\tau : X \to X$ is a bijection (it has an inverse), so

$$|\operatorname{Fix}(\pi)| = |\{(\tau x) \in X : \sigma(\tau x) = (\tau x)\}|.$$

Letting $y = (\tau x)$, we then have that

$$|\operatorname{Fix}(\pi)| = |\{y \in X : \sigma y = y\}| = |\operatorname{Fix}(\sigma)|,$$

and we are done.

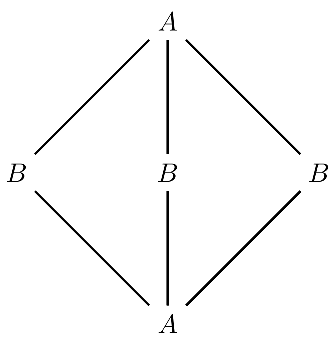
Solution. 112
If $(g, h) \in \mathrm{S}_3 \times \mathrm{S}_2$ act on X, the number of fixed-points only depend on the type of g, and type of h, respectively.

Type (g, h)	Number of permutations	$\lvert X^g \rvert$	Fixed-points
$(111, 11)$	1	3^6	$\begin{array}{\|c\|c\|c\|}\hline a & b & c \\ \hline d & e & f \\ \hline\end{array}$
$(21, 11)$	3	3^4	$\begin{array}{\|c\|c\|c\|}\hline a & a & c \\ \hline b & b & d \\ \hline\end{array}$
$(3, 11)$	2	3^2	$\begin{array}{\|c\|c\|c\|}\hline a & a & a \\ \hline b & b & b \\ \hline\end{array}$
$(111, 2)$	1	3^3	$\begin{array}{\|c\|c\|c\|}\hline a & b & c \\ \hline a & b & c \\ \hline\end{array}$
$(21, 2)$	3	3^3	$\begin{array}{\|c\|c\|c\|}\hline a & b & c \\ \hline b & a & c \\ \hline\end{array}$
$(3, 2)$	2	3^1	$\begin{array}{\|c\|c\|c\|}\hline a & a & a \\ \hline a & a & a \\ \hline\end{array}$

Burnside's lemma then gives that the number of orbits is

$$\begin{aligned}&\frac{1}{12}\left(3^6 + 3 \times 3^4 + 2 \times 3^2 + 3^3 + 3 \times 3^3 + 2 \times 3^1\right)\\ &= \frac{1}{12}\left(3^6 + 3^5 + 18 + 27 + 81 + 6\right) = 92.\end{aligned}$$

Solution. 113
Here it is important to emphasize that it is indeed a bipartite graph:



Solution. 115

There are clearly n^2 vertices, as there are n choices for the first coordinate, and n choices for the second in a pair. To count edges, we first compute the degrees of vertices.

There are three types of vertices (a, b):

Case 1: $1 < a, b < n$. Such a vertex is connected with $(a \pm 1, ?)$, $(?, b \pm 1)$, which gives $4n$ choices, but we double-count $(a \pm 1, b \pm 1)$, so it has degree $4n - 4$.

The total degree from these vertices is $(4n - 4)(n - 2)^2$, since there are $(n - 2)^2$ such vertices.

Case 2: $a = 1, 1 < b < n$. Such a vertex is connected with $(a + 1, ?)$, $(?, b \pm 1)$, which gives $n + 2n$ choices. However, we double-count edges to $(a + 1, b \pm 1)$ so the degree is $3n - 2$.

The total contribution is thus $4(n - 2)(3n - 2)$.

Case 3: $a = b = 1$. This gives $(a + 1, ?)$ or $(?, b + 1)$ so, $2n$, but $(2, 2)$ is double-counted, so we have degree $2n - 1$, and contribution $4(2n - 1)$.

The total degree sum is $(4n - 4)(n - 2)^2 + 4(n - 2)(3n - 2) + 4(2n - 1)$, so the number of edges is $2n^3 - 4n^2 + 4n - 2 = 2(n - 1)(n^2 - n + 1)$.

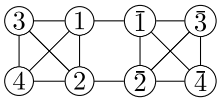
To prove non-planarity, it is easy to find a $K_{3,3}$. Alternatively, we must have $e \leq 3v - 6$ in a simple planar graph, but

$$e \leq 3v - 6 \Leftrightarrow 2n^3 - 4n^2 + 4n - 2 \leq 3n^2 - 6 \Leftrightarrow 0 \leq -(n - 2)^2(1 + 2n)$$

which is false for $n \geq 3$.

Solution. 116

(a) G_4 is the following graph:



(b) For $n = 2$, the graph looks like a cycle on 4 vertices, and thus has an Euler trail. If $n > 2$ is odd, then vertex 1, 2 and -1 and -2 all have odd degrees, so there is no Euler trail. If $n > 2$ is even, then vertices $3, 4$ and $-3, -4$ have odd degrees, so there is no Euler trail either.

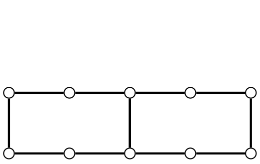
(c) The cycle

$$2, 3, 4, \ldots, n, 1, -1, -n, -(n - 1), \ldots, -4, -3, -2, 2$$

is a Hamiltonian cycle since it visits all vertices exactly once.

Solution. 117

The following is a silly graph.



Since we have 3 regions, Euler's formula tells us that $v - e + 3 = 2$, so $e = v + 1$. The handshaking lemma tell us that summing the degrees give (the vertices are called w_i as v is used to denote the number of vertices):

$$2e = \sum_{i=1}^{v} \deg(w_i).$$

Since every vertex has degree at least 2, we can write $\deg(w_i) = 2 + a_i$, where $a_i \geq$ is the *additional degree*. Thus,

$$2v + 2 = \sum_{i=1}^{v} (2 + a_i) = 2v + \sum_{i=1}^{v} a_i.$$

We see that $a_1 + a_2 + \ldots + a_v = 2$, so it is impossible for some a_i to be three or more, and thus, there cannot be any vertex with degree 5 or more.

Solution. 118

A tree with v vertices has $(v - 1)$ edges. Each tree therefore contributes with 1 to the difference between edges and vertices. We have $20 = 100 - 80$ trees.

We can also prove this by starting with 20 vertices and 0 edges. Then we add 80 leaves, (each is a vertex and and edge). This gives 20 trees, with 100 vertices and 80 edges.

Solution. 119

We show that any partial coloring of the regions can be extended by coloring a new region.

Assume we have a partial coloring of the regions and choose an uncolored region. Since the region is a triangle, it has at most 3 adjacent regions that have already been colored (with perhaps different colors). However, there is at least one available color remaining, which is used to color the last region.

Solution. 120

Use Euler's formula $v - e + r = 2$, and solve for e. This gives $e = 12$.

Solution. 121

Suppose there are v vertices. The handshaking lemma gives that $2e = dv$. Plugging this into Euler's formula gives that

$$r = 2 + e - v = 2 + e - \frac{2e}{d}.$$

Furthermore, we know that since every region has at least 3 edges, $3r \leq 2e$ so $r \leq 2e/3$. Putting this together, we get

$$\frac{2e}{3} \geq 2 + e - \frac{2e}{d} \quad \Leftrightarrow \frac{2e}{3} + \frac{2e}{d} - e \geq 2 \quad \Leftrightarrow e\left(\frac{2}{d} - \frac{1}{3}\right) \geq 2$$

Thus,

- if $d = 3$, we get that $e = 6$ at least and $v = 4$,

- if $d = 4$, we get that $e = 12$ at least and $v = 6$,
- if $d = 5$, we get that $e = 30$ at least and $v = 12$.

You can draw such graphs by placing the vertices first, and then make sure that every region is a triangle.

Solution. 122

Every region has at most c edges around it. The handshaking lemma for regions show that $2e \leq rc$. Similarly, $2e \geq vd$. Thus, $rc \geq vd$, and $r/v \geq d/c$.

Solution. 123

There are n choices for the first vertex in the path. Since it is the complete graph, we can proceed to any of the remaining $(n-1)$ vertices. From there, there are $(n-2)$ choices and so on. This gives in total $n(n-1)(n-2)\cdots 1$ such paths.

Note that we consider paths going in opposite directions to be different.

Solution. 124

If G is bipartite, we can partition the vertices into two sets, say red and blue, such that every edge is between vertices of different colors. Every cycle in G must then have an even number of vertices, since the colors of the vertices must alternate. In particular, there cannot be a cycle containing all the vertices, since there is an odd number of vertices in total.

Solution. 127

Let $E = C_1 \cup C_2 \cup \cdots \cup C_k \cup F$ be a disjoint union of edges, where each C_j is a cycle and F is a forest. Such a decomposition can be found by iteratively removing cycles, until a forest remains. Each cycle in G must therefore contain at least one edge from some C_j.

Let $G' = (V, E \setminus F)$, which is also planar. We mark the faces of G' which appear inside an even number of cycles C_j. Every edge in G' is therefore adjacent to a marked face. However, some faces in G' might be subdivided into smaller faces by edges in F, in which case all these subdivided faces are marked. Every cycle in G is then adjacent to a marked face. To show that we can do this with at most $\frac{1}{2}|F|$, note that can decide to swap the role of marked and unmarked faces.

To show that the bound is sharp, consider an odd number of concentric, disjoint cycles.

Alternatively: Take a spanning tree of the dual graph. This can be colored with two colors. Take the faces corresponding to the least used color. This gives a set of marked faces with the desired property.

Solution. 128

(a) If we reverse all edges in an acyclic orientation, we get a new (different if the number of edges is at least 1) acyclic orientation.

Thus, we can pair up all acyclic orientations with the reversed version, making it an even number.

(b) Suppose there is no sink. We can then start in any vertex, and follow any of the outgoing edges (which there at least one of). However, since we have a finite number of vertices, we must come back to some previously visited vertex. This creates a directed cycle, and this contradicts the acyclicness. Hence, we must eventually end up in a sink.

(c) A sink in any orientation of K_n must be unique. Suppose we have two sinks, u and v. However, since K_n is complete, there is an edge between u and v. This must be orientated in a way that makes either u or v a non-sink.

(d) We use induction to prove this. The base case $n = 1$ is clear. To create an acyclic orientation of K_n, we need to choose which vertex v is the unique sink. This can be done in n ways. After we pick that vertex, the remaining $n - 1$ verties (and edges between them), form a smaller complete graph, K_{n-1}. We can by induction hypothesis choose an acyclic orientation of this in $(n-1)!$ ways. This orientation is extended to an orientation on K_n by adding edges oriented towards v. This extension is acyclic by construction.

Solution. 129

For every person in G, we add an edge and a new vertex. Thus, the new graph has 200 vertices, and 100 more edges. Let an edge be called *active* if it links a player with a non-player. Initially, there are therefore at most $15 \times (5 + 1) = 90$ active edges, where the new edges also count as active.

If all original people in G were playing Farmville, there would be be 100 active edges. However, note that as a new person starts to play the game, the number of active edges stays the same or decreases. Hence, there is no way for 90 active edges to become 100.