MM5013: Algebra and combinatorics
Lecture notes

Per Alexandersson

May 26, 2026

Lecture 1: Introduction

1.1. Overview of the course

1. Structure: Lectures plus exercises. Exercises start directly after the break, so be prepared.
2. Book: Biggs, Discrete mathematics, 2nd Ed. Some additional notes for encryption.
3. The videos are a complement to the lectures.
4. Bonus point system — A small set of questions before each class, to be answered in Webwork. Two sets of additional problems, 3p total. Can be used for the final, and first retake. See web page for details.

There is a lot of material in the course! We will cover lots of things: Algebraic structures, counting, permutations, graph theory, and some applications (encryption, codes). Many of new concepts, but not very deep.

1.2. Divisibility

If a and b are integers, $a = kb+r$ with $0 \leq r < b$, then k is the **quotient** and r is the **remainder** in the division when a is divided by b. We say that $b \mid a$, if $a = kb$ for some integer k.

We introduce gcd, greatest common divisor.

1.2.1. Euclid's algorithm

We have some nice properties of gcd which follow from Euclid's algorithm and the definition of greatest common divisor.

Lemma 1. *We have that* $\gcd(a, b) = \gcd(a - b, b)$.

Proof. Let $d = \gcd(a, b)$. Since $d \mid a$ and $d \mid b$, we have that $d \mid a - b$. Hence, $\gcd(a - b, b) \geq d$.

On the other hand, $\gcd(a - b, b)$ divides both $a - b$ and b, so it must divide the sum, which is a. Hence, $\gcd(a - b, b)$ divides both a and b, so $\gcd(a - b, b) \leq d$.

This proves that $d = \gcd(a - b, b)$. □

Using this lemma many times, we get

- $\gcd(a, b) = \gcd(a - bk, b)$ for all $k \in \mathbb{Z}$.
- In particular, $\gcd(a, b) = \gcd(r, b) = \gcd(b, r)$ if $a = kb + r$. Note that this is one step in Euclid's algorithm.

Question 2. Find $\gcd(33, 18)$.

Solution.

$$33 = 1 \cdot 18 + 15$$
$$18 = 1 \cdot 15 + 3$$
$$15 = 5 \cdot 3 + 0$$

Corollary 3. *We have that if* $\gcd(a, b) = d$*, then we can find integers* x*,* y *such that* $ax + by = d$*.*

Question 4. Define the sequence $g_0 = 1$, $g_1 = 2$ and $g_k = 3g_{k-1} - g_{k-2}$ for $k \geq 2$. Prove that $\gcd(g_k, g_{k-1}) = 1$ for all $k \geq 1$.

Solution. The statement is clear for $k = 1$, this is our base case. Suppose the statement is true for $k - 1$. We get, by first using the recursion, then use Euclid's algorithm and finally the induction hypothesis, that

$$\begin{aligned}\gcd(g_k, g_{k-1}) &= \gcd(3g_{k-1} - g_{k-2}, g_{k-1}) \\ &= \gcd(-g_{k-2}, g_{k-1}) \\ &= \gcd(g_{k-2}, g_{k-1}) \\ &= 1.\end{aligned}$$

1.3. Prime numbers

A prime number is an integer $p > 1$ where the only numbers dividing p are 1 and p. Non-prime numbers are composite.

Proposition 5. *Each integer* n *has a prime factorization, i.e., is a product of prime numbers.*

Proof. We do induction over n. For $n = 1$, we are done, so suppose now $n \geq 2$. Either, n is already prime. If not, $n = ab$ for some smaller numbers $a > 1$, $b > 1$. By induction, a and b have prime factorizations, so n does as well. □

However, this does not prove that prime factorization is unique. Our next goal is to prove uniqueness.

Lemma 6. *If* $p \mid ab$*, then* $p \mid a$ *or* $p \mid b$*.*

Proof. Suppose p does not divide a. Then there are integers x and y such that $xa + yp = 1$. This follows from Euclid's algorithm and the fact that $\gcd(p, a) = 1$. (This is where we use the fact that p is a prime number!)

But then, multiplying both sides by b, we get

$$bxa + byp = b \iff (ab)x + p(by) = b.$$

Since p divides the left hand side, it must divide b and we are done. □

We can generalize to more than two factors, using induction.

Lemma 7. *If* $p \mid x_1 x_2 \cdots x_n$*, then* $p \mid x_i$ *for some* i*.*

Proof. For $n = 1$, it is trivial, for $n = 2$ we have the proof above. Suppose $n \geq 3$. Note,

$$x_1 x_2 \cdots x_n = x_1 \cdot (x_2 \cdots x_n)$$

so p must divide either x_1 or $(x_2 \cdots x_n)$. If it divides x_1, we're done, and if p divides $(x_2 \cdots x_n)$ it must divide one of the factors, by induction. □

Theorem 8. *Prime factorization is unique.*

Proof. Suppose

$$N = p_1 p_2 \cdots p_m = p'_1 p'_2 \cdots p'_{m'}$$

We do induction over N. If $N = 1$, there is only one factorization. If $N \geq 2$, we have that p_1 divides both sides, so $p_1 = p'_j$ for some j (using the above result). After dividing everything with p_1, (we can pretend that $j = 1$), we have that

$$\frac{N}{p_1} = p_2 \cdots p_m = p'_2 \cdots p'_{m'}$$

but by induction, these factorizations are the same, so the factorization of N is unique. □

Hence, we can write

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}.$$

1.3.1. GCD again

We can look at the factorizations of two numbers and compute the greatest common divisor from the factorizations. How?

1.3.2. Modulo notation

We use $a \equiv b \mod n$ to say a and b have the same remainder mod n. We shall sometimes use $a \equiv_n b$ to denote that a and b are equal modulo n.

Theorem 9. *If $a \equiv_n r$ and $b \equiv_n s$ then $a + b \equiv_n r + s$.*

Proof. We have that $a = qn + r$, $b = kn + s$, so $a + b = (q + k)n + (r + s)$ so dividing $a + b$ by n must give the same remainder as $r + s$. □

Theorem 10. *If $a \equiv_n r$ and $b \equiv_n s$ then $a \cdot b \equiv_n r \cdot s$.*

Proof. We have that $a = qn + r$, $b = kn + s$, so

$$ab = qkn^2 + qns + knr + rs = n(qkn + qs + kr) + rs$$

so ab gives the same remainder as rs. □

It follows that if $a \equiv_n r$ then $a^m \equiv_n r^m$.

Note that $a \equiv_n b$ if and only if $a - b \equiv_n 0$.

We introduce $\mathbb{Z}_n$ for the remainders mod n. Note that we can add, subtract, and multiply these. This is the main topic for next class.

1.3.3. Check-sums

Is it possible that $149291^2 = 22287802671$? Note $149291 \equiv_3 1 + 1 + 2 + 1 \equiv_3 2$, so $LHS \equiv_3 1$. We then have $22287802671 = 2 + 2 + 2 + 2 + 1 + 2 + 2 + 1 + 1 \equiv_3 0$ so they cannot be equal.

Question 11. Calculate the remainder when 2^{1026} is divided by 17.

Solution. We have that

$$2^{1026} = 4 \cdot 2^{1024} = 4 \cdot (2^4)^{256} = 4 \cdot 16^{256} \equiv_{17} 4(-1)^{256} = 4$$

So, the answer is 4.

1.3.4. Equations involving modulo

Solving $5x \equiv_8 7$ is the same as solving the Diophantine equation $5x + 8y = 7$ and then selecting all non-negative solutions x which are less than 8.

Question 12. Solve the equations $x^2 \equiv_7 4$ and $x^2 \equiv_7 3$.

Solution. We simply compute the squares of $0, \ldots, 6$. We get

$$0, 1, 4, 2, 2, 4, 1.$$

(Why is this symmetric?) Hence, $2^2 = 4$ and $5^2 = 4$, but there are no solutions to the second equation.

Question 13. Solve the Diophantine equation $x^2 + 1 = 3y$.

Solution. Taking mod 3 on both sides, we must find if $x^2 + 1$ can ever be divisible by 3. But $(3a + r)^2 + 1 \equiv_3 r^2 + 1$ is never equal to 0, as r^2 is either 0 or 1 mod 3.

Question 14. Solve the equations $x^2 \equiv_8 1$.

Solution. Here, we find that 1, 3, 5 and 7 are all solutions.

Question 15. In $\mathbb{Z}_6$, solve the system

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

Solution. 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 to $3x = 3$, 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 $\mathbb{Z}_6$):

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

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

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

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

Question 16. Let $a_1, \ldots, a_{10}$ be some integers. Show that there is some difference $a_i - a_j$ which is divisible by 9.

Solution. We look at all possible remainders mod 9. Since we have 10 remainders in total, but only 9 possible values $0, \ldots, 8$, two of these must be equal, say a_i and a_j. Then $a_i - a_j$ has remainder 0 mod 9, and is therefore divisible by 9.

1.4. Exercises in Biggs

```
Read 8.1--8.6 and 13.1--13.3
 8.1: 1, 2
 8.2: 1
 8.3: 1
13.1: 1, 2, 4
13.2: 1, 3
13.3: 1, 3, 4, 5.
```

Lecture 2: Rings

2.1. Invertible elements

Recall[1] that U_m denotes the invertible elements in $\mathbb{Z}_m$. Moreover, a is invertible if and only if $\gcd(a, m) = 1$. The number of invertible elements in $\mathbb{Z}_m$ is denoted $\phi(m)$, **Euler's phi function**. We have $\phi(m)$ as the number of elements in $\{1, \ldots, m\}$ which are relatively prime to m.

2.2. Euler's theorem and Fermat's little theorem

If $y \in \mathbb{Z}_m$ is invertible, then $y^{\phi(m)} = 1$. Thus, y^{-1} is $y^{\phi(m)-1}$.

Euler's theorem[2] implies Fermat's theorem, since every $a \neq 0$ in $\mathbb{Z}_p$ is invertible, and $\phi(p) = p - 1$, so $a^{p-1} = 1$.

Proof sketch. Let $U = U(\mathbb{Z}_m)$. Then any $y \in U$, we have that $yU = U$ as sets. Note also that $|U| = \phi(m)$. It follows that if $u = \{x_1, \ldots, x_{\phi(m)}\}$ then

$$x_1 \cdot x_2 \cdots x_{\phi(m)} = (yx_1) \cdot (yx_2) \cdots (yx_{\phi(m)}).$$

This implies that $y^{\phi(m)} = 1$. □

Question 17. Find a positive integer x, such that $2^x \equiv 1 \bmod 23$, and $3^x \equiv 9 \bmod 31$.

Solution. We know that all values $x = 22k$ for $k \in \mathbb{N}$ solve the first equation by using Fermat's little theorem. Similarly, all values $x = 30m + 2$ solve the second equation for $m \in \mathbb{N}$. Thus, we seek solutions to $22k = 30m + 2$ or $11k - 15m = 1$. We have $(k, m) = (-4, -3)$ is a solution, so

$$(k, m) = (-4 + 15s, -3 + 11s), s \in \mathbb{Z}$$

are possible solutions. Taking $s = 1$ gives $k = 11$ and $x = 22 \times 11 = 242$ is a solution.

2.3. Rings

A **ring** is a set, together with two operations, addition and multiplication.

Definition 18 (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 $a, b, c \in R$.

[1] From the video.
[2] Proved in the video.

3. (Commutativity) $a + b = b + a$ for all $a, b \in R$.
4. (Existence of identity) There is some $0 \in R$, such that $0 + a = a + 0 = a$ for all $a \in R$.
5. (Existence of inverses) For every $a \in R$, there is a $-a \in R$ such that $a + (-a) = 0$.

For the $*$ operator:

1. (Closedness) $a * b \in R$ for all $a, b \in R$.
2. (Associativity) $a * (b * c) = (a * b) * c$ for all $a, b, c \in R$.
3. (Existence of identity) There is some $1 \in R$, such that $1 * a = a * 1 = a$ for all $a \in R$.

Distributive law:

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

2.3.1. Examples of rings

- The sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are all rings under the usual addition and multiplication.
- $\mathbb{Z}_m$ is always a ring.
- $M_{n,n}(K)$, 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.

Here, K is any of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$.

Example 19. The following sets are rings:

$$\mathbb{R}[x], \quad \mathbb{Z}_3[x], \quad \mathbb{Z}[x, y].$$

Question 20. We now do some computations in rings of the form $\mathbb{Z}_m[x]$.

- What are the zeros of $2x^2 + 4x + 1 \in \mathbb{Z}_6[x]$? **No zeros**
- What are the zeros of $2x^2 + 4x \in \mathbb{Z}_6[x]$? **Four zeros.**
- Compute the product $(2x+3)(3x+2)$ in $\mathbb{Z}_6[x]$. **Same as $6x^2+13x+6$, which simplifies to x.**

2.3.2. The neutral element and identity element are unique

An element is a neutral element if $a + 0 = a$ for all $a \in R$. Suppose we have two neutral elements, $0, 0'$. Then

$$0 = 0 + 0' = 0'$$

so there can only be one. Same proof goes for identity element:

$$1 = 1 \cdot 1' = 1'.$$

2.3.3. Inverses are unique

Suppose $xy = 1$, so that y is an inverse to x. Suppose now we also have $xz = 1$. Then, $xy - xz = 0$ so $x(y - z) = 0$. Multiply by y (an inverse of x) on both sides, and we get $(y - z) = 0$, so $y = z$.

Question 21. Prove that $a \times 0 = 0$ and that $a \times (-1) = -a$ in a ring.

Solution. First, $a \times 0 = a \times (0 + 0) = a \times 0 + a \times 0$. Now subtract $a \times 0$ on both sides.

We have $a \times (-1) + a \times (1) = a \times (1 - 1) = a \times 0$, so $a \times (-1)$ is the additive inverse of a.

2.3.4. Discuss: Are these rings?

1. Even integers under $+$ and $*$. **No, no multiplicative identity is missing.**
2. Polynomials P in $\mathbb{Q}[x, y]$ such that $P(x, y) = P(y, x)$. **Yes**
3. Functions of the form $P(x)/x^k$, where $P(x) \in \mathbb{Q}[x]$ and $k \in \mathbb{N}$ under addition and multiplication. **Yes.**
4. The set of linear functions, $f(x) = ax + b$ with $a, b \in \mathbb{Q}$. Determine if $(R, +, \circ)$ is a ring or not, where $\circ$ is composition.

   It is not a ring, since $f \circ (g + h) \neq f \circ g + f \circ h$.

Question 22. Suppose $a, b \in R$ such that $ab = ba$, then $(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$.

Solution. If we expand $(a + b)^n$ we get all 2^n words, consisting of a's and b's of length n. The given information tells us that we may rearrange the order of the letters, and there are then exactly $\binom{n}{k}$ words with exactly k as and $n - k$ bs.

Question 23. Let R be the set (x, y) with $x \in \mathbb{Z}_2$, $y \in \mathbb{Z}_3$, with

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2) \qquad (x_1, y_1) \cdot (x_2, y_2) = (x_1 \cdot x_2, y_1 \cdot y_2).$$

Show that R is a ring, find the identity element and determine $U(R)$.

Question 24. Let $x \in R$ be an element in a ring such that $1 - x$ is invertible. Show that

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

Proof. We have that

$$\begin{cases} (1 - x)(1 + x + x^2 + \cdots + x^n) = 1 - x^{n+1} \\ (1 + x + x^2 + \cdots + x^n)(1 - x) = 1 - x^{n+1}, \end{cases}$$

and multiplying by $(1 - x)^{-1}$ (from the left, or from the right) then gives the result. □

2.4. Subrings

Definition 25. A set $R' \subseteq R$ is said to be a **subring** of $R = (R, +, *)$ if $(R', +, *)$ is a ring and we have that the multiplicative identity in R also lies in R'.

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[3].

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

Example 26. 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,

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

are all symmetric polynomials. As a non-example, $x + 7y$ is not symmetric.

Question 27. Let R' and R'' both be subrings of some ring R. Show that the intersection $R' \cap R''$ is also a subring of R.

Question 28. Let $R \subseteq \mathbb{Q}[x]$ be the set of all polynomials which are even[4] functions. Show that R is a subring of $\mathbb{Q}[x]$.

Show that the set of polynomials which are odd[5] functions is *not* a subring.

Question 29. Let $M \coloneqq \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. Note that M is a subset of the real numbers. Show that M is a subring of $\mathbb{R}$.

Find the multiplicative inverse of $3 + 4\sqrt{2}$. Which elements in M have a multiplicative inverse?

Solution. All non-zero elements have inverses. We can use $(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$.

Question 30. Show that $\mathbb{Z}$ does not contain a smaller subring. Then describe two different subrings of $\mathbb{Q}$.

Solution. Suppose $R \subseteq \mathbb{Z}$ is a subring. Then $0, 1 \in R$. But if $1 \in R$, then $1 + 1 + \cdots + 1 \in R$ so all positive integers are in R also. Since R must be closed under additive inverse, all negative integers must be in R as well.

Every subring of $\mathbb{Q}$ must contain $\mathbb{Z}$. We know that $\mathbb{Z}$ is a subring of $\mathbb{Q}$. As an example of a larger subring of $\mathbb{Q}$, we can take all rational numbers which can be expressed in the form

$$R = \left\{ \frac{a}{2^k} \text{ such that } a \in \mathbb{Z} \text{ and } k \geq 0 \right\}.$$

One then needs to verify that R is closed under the ring operations.

Question 31. Describe an infinite sequence of subrings $R_1 \subset R_2 \subset R_3 \subset \cdots$.

Solution. We can let R_j be all rational numbers which can be expressed in the form $\frac{a}{b}$ where the prime factorization of b only involves the first j primes.

Question 32. Let $R \subset \mathbb{Q}[x]$ be the subset of polynomials of the form

$$R_1 = \{a_n x^{2n} + a_{n-1}x^{2n-2} + \cdots + a_1 x^2 + a_0 : a_i \in \mathbb{Q}\},$$

and let $R_2 \subset \mathbb{Q}[x]$ be the subset

$$R_2 = \{a_n x^{3n} + a_{n-1}x^{3n-3} + \cdots + a_1 x^3 + a_0 : a_i \in \mathbb{Q}\}.$$

Show that R_1 and R_2 are subrings of $\mathbb{Q}[x]$, and describe the ring $R_1 \cap R_2$.

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

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

2.5. Back to modular arithmetic

Question 33. In $\mathbb{Z}_{11}$, solve the system

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

Solution. 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.

Question 34. In $\mathbb{Z}_6$, solve the system

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

Solution. 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 to $3x = 3$, since $-3 \equiv_6 3$. However, we *cannot* divide both sides by 3, since this is not[6] an operation that can be done in $\mathbb{Z}_6$ So to solve $3x = 3$ in $\mathbb{Z}_6$, we get the Diophantine equation $3x + 6z = 3$. This is ordinary integers, so we can instead solve $x + 2z = 1$.

We see that $x = 3$, $z = -1$ 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 $\mathbb{Z}_6$):

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

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

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

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

2.6. Exercises in Biggs

Same problems as for the next lecture.

```
Read Chapter 22
22.1: 1,2,3
22.2: 1 (Find the sizes of the sets)
22.3: 1i, 3
22.4: 1,2,4
22.5: 1,2,3,4,5
22.6: 1
22.7: 1,2,3,4,5,6
22.8: 1
```

[6]The element 3 is not invertible in $\mathbb{Z}_6$, if it was, we could have multiplied both sides by its inverse

Lecture 3: Fields

3.1. Fields

A **field**[1] is a ring, with the addition that multiplication is commutative, and that all non-zero elements have a multiplicative inverse.

- The sets $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are all fields under the usual addition and multiplication.
- $\mathbb{Z}_p$ is a field whenever p is a prime.

As with subring, we also have the notion of **subfield**.

We proved earlier that

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

is a field, since every non-zero element has an inverse. Hence, this is a subfield of $\mathbb{R}$.

Lemma 35. *If $ab = 0$, then $a = 0$ or $b = 0$ in a field.*

Note that this is not always true in rings!

3.2. Polynomials over a field

We can now consider $K[x]$, polynomials with coefficients in a field. We can define the **degree** of $f(x)$ as the largest exponent of x appearing. We define the degree of 0 to be $-\infty$. A polynomial is **monic** if its leading coefficient is 1.

Question 36. Show that $\deg(fg) = \deg(f)\deg(g)$ in a field K.

Solution. If $f = ax^m + \cdots$ and $g = bx^n + \cdots$, then $fg = abx^{m+n} + \cdots$. Since K is a field, ab cannot be 0, so the degree of the product must be $m + n$.

Remark 37. This property does not hold in general in rings: $(2x + 3)(3x + 2) = x$ in $\mathbb{Z}_6$, so it may happen that the degree decreases. Moreover, it sounds wrong to say that $(2x + 3)$ divides x.

Divisibility of polynomials over a field is defined as follows. If $f = gh$ then g **divides** f. Note that the intuition we have about the degrees of f, g and h is compatible with this notion.

Question 38. Consider $x^3 + 3x^2 + 4x + 2$ in $\mathbb{Z}_5[x]$. Compute the quotient and remainder when divided by $x + 2$.

Solution. The quotient is $x^2 + x + 2$, remainder is 3.

[1] Kropp in Swedish

3.3. Quotient, reminder and Euclid's algorithm for polynomials

Lemma 39 (Biggs, 22.5)**.** *If $f, g \in K[x]$ with g non-zero, there exist unique polynomials $q(x), r(x) \in K[x]$ such that*

$$f(x) = q(x)g(x) + r(x)$$

where $\deg(r) < \deg(g)$.

Proof. We prove this by induction on the degree of $f(x)$. First, if $\deg(g) > \deg(f)$, we take $q(x) = 0$ and $r(x) = f(x)$.

Now if $\deg(g) \leq \deg(f)$, there is a unique[2] c and $k \coloneqq \deg(f) - \deg(g)$ such that

$$f(x) - cx^k g(x)$$

has degree strictly lower than $f(x)$. By induction hypothesis, we can then write

$$f(x) - cg(x) = \tilde{q}(x)g(x) + r(x) \implies f(x) = \left(\tilde{q}(x) + cx^k\right) g(x) + r(x),$$

so f itself is expressed in the desired fashion.

Uniqueness can be proved by supposing there are two different such representations:

$$f = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x).$$

Taking the difference gives $(q_1(x) - q_2(x))g(x) = r_1(x) - r_2(x)$. But the left hand side has degree at least same as g, while the right hand side has degree strictly smaller than that of g, unless $q_1 = q_2$, in which case $r_1 = r_2$. So we have uniqueness. □

3.3.1. Euclid's algorithm

Since we are sure the degree is always reduced when dividing, we have that the analogous version of Euclid's algorithm holds for polynomials in $K[x]$ as well.

We must show that for $f, g, q \in K[x]$ we have

$$\gcd(f, g) = \gcd(f - q \cdot g, g),$$

and from this we use the same approach as in the first lecture.

Question 40. Compute $\gcd(x^5 + x^4 + 2x^3 + 2x^2 + 2x + 1, x^4 + 2x^3 + 3x^2 + 2x + 1)$ in $\mathbb{Z}_5$.

Solution. We have

$$\begin{aligned}
x^5 + x^4 + 2x^3 + 2x^2 + 2x + 1 &= x \cdot (x^4 + 2x^3 + 3x^2 + 2x + 1) + 4(x^4 + x^3 + 4x + 4) \\
x^4 + 2x^3 + 3x^2 + 2x + 1 &= 1(x^4 + x^3 + 4x + 4) + x^3 + 3x^2 + 3x + 2 \\
x^4 + x^3 + 4x + 4 &= x(x^3 + 3x^2 + 3x + 2) + 3(x^3 + 4x^2 + 4x + 3) \\
x^3 + 3x^2 + 3x + 2 &= 1(x^3 + 4x^2 + 4x + 3) + 4(x^2 + x + 1) \\
x^3 + 4x^2 + 4x + 3 &= x(x^2 + x + 1) + 3(x^2 + x + 1) \\
x^2 + x + 1 &= 1(x^2 + x + 1) + 0
\end{aligned}$$

Answer: $x^2 + x + 1$.

[2] By considering the leading coefficients.

3.3.2. Factoring polynomials

Proposition 41 (Factorization theorem)**.** *For a polynomial $f \in K[x]$, we have that $f(\alpha) = 0 \iff (x-\alpha) \mid f(x)$ holds.*

Proof. First of all, if $(x-\alpha)$ divides f, then $f(x) = (x-\alpha)g(x)$ and evidently $f(\alpha) = 0$. Now, if $f(\alpha) = 0$ consider

$$f(x) = (x-\alpha)g(x) + r(x), \qquad \deg(r) = 0, \text{ so } r \text{ is a constant.}$$

If we put in $x = \alpha$, we find that $r = 0$. □

If follows that a polynomial of degree k, can have at most k zeros. Proof by induction. True if $k \leq 1$. Now, if f has a zero, then $f = (x-\alpha)g(x)$ with g having degree $k-1$. But then g has at most $k-1$ roots (by induction).

Question 42. Prove that $x^p - x$ factors as $x(x+1)(x+2)\cdots(x+p-1)$ in $\mathbb{Z}_p[x]$.

Proof. The left hand side is 0 for all elements in $\mathbb{Z}_p$. Hence, it must have $(x-j)$ as factor for all $j \in \mathbb{Z}_p$, so we factor out these. But now, the degrees agree, so the polynomials must be the same, as elements in $\mathbb{Z}_p[x]$. □

Question 43. Verify that $x^3 + 3x^2 + 1 = (x+2)^2(x+4)$ as polynomials in $\mathbb{Z}_5$.

Solution.

$$(x+2)^2(x+4) = x^3 + 8x^2 + 20x + 16 \equiv_5 x^3 + 3x^2 + 1.$$

3.4. Irreducible polynomials

A polynomial f in $K[x]$ is **irreducible** if it cannot be written as a product of two non-constant polynomials g and h with coefficients in K. In particular, irreducible polynomials have no zeros (in K).

Determine over which of the fields $\mathbb{Z}_5$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$, the polynomials x^2+1 and x^2-2 are irreducible.

Question 44. Discuss: Which of these are irreducible as elements in $\mathbb{Z}_5$?

1. $x^2 + x + 3 \equiv_5 (x+2)(x+4)$
2. $x^2 + 3x + 1 \equiv_5 (x+4)^2$
3. $x^2 + 4x + 2$
4. $x^2 + 3x + 3$

Question 45. Is $x^4 + x^2 + 1$ irreducible in $\mathbb{Z}_2$?

Solution. There are no linear factors since the polynomial has no zeros (by plugging in $x = 0$ and $x = 1$). The only possibility is then

$$\begin{aligned} x^4 + x^2 + 1 &\equiv_2 (x^2 + ax + b)(x^2 + cx + d) \\ &\equiv_2 acx^2 + adx + ax^3 + bcx + bd + bx^2 + cx^3 + dx^2 + x^4. \end{aligned}$$

We compare coefficients:

$$\begin{cases} bd & = 1 \\ bc + ad & = 0 \\ b + ac + d & = 1 \\ a + c & = 0 \end{cases}$$

First row implies $b = d = 1$, and the last row that $a = c$. This gives $a = c = 1$ in row 2 and we have

$$x^4 + x^2 + 1 \equiv_2 (x^2 + x + 1)(x^2 + x + 1).$$

Question 46. Find the remainder when $x^{100} + 2x + 2$ is divided by $x^2 + 2$ in $\mathbb{Z}_3$.

Solution. 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 $2x$.

Question 47. Can $f(x) = x^{22} + 5x^{17} + ax^{12} + 8x^5 + 2$ be irreducible for all values of a, when considered as a polynomial in $\mathbb{Z}_{19}[x]$?

Solution. We have that $f(1) = 1 + 5 + a + 8 + 2 = 16 + a$. So, if we choose $a = 5$, we have that $f(1) = 0$, making it reducible.

Question 48. Suppose $f(x) \in K[x]$ is given by $f(x) = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0$ is palindromic, in the sense that $a_j = a_{k-j}$ for all $0 \leq j \leq k$. Prove that if $f(\alpha) = 0$ then $f(\alpha^{-1}) = 0$ also.

Solution. First note that f cannot have 0 as a root, since $a_0 = a_k \neq 0$. We now see that

$$\alpha^k f(\alpha^{-1}) = a_k + a_{k-1}\alpha + a_{k-2}\alpha^2 + a_1\alpha^{k-1} + a_0\alpha^k = f(\alpha)$$

where we in the last step used the fact that f is palindromic. Hence, $f(\alpha^{-1}) = 0$ if $f(\alpha) = 0$.

3.4.1. Factorization of polynomials

Theorem 49. *A polynomial of degree n over a field, can have at most n roots.*

Proof. Proof by induction. For constants, this is evident. Then, if f is a polynomial of degree n, with α as a root, then $f(x) = (x - \alpha)g(x)$ with $g(x)$ having degree $n - 1$. Now, $g(x)$ have at most $n - 1$ roots (by induction hypothesis) so we are done. □

Theorem 50 ((Biggs, Thm. 22.7))**.** *Every polynomial over a field can be factored uniquely as a product of irreducible polynomials.*

See exercises 22.7, 1–6 below.

Question 51. (Biggs 22.7.1) Show that if $r(x)$ is non-constant and $s(x)$ non-zero, then

$$\deg r(x)s(x) > \deg s(x).$$

Solution. The conditions tells us that $\deg(r) \geq 1$ and $\deg(s) \geq 0$. From this, we can easily deduce that

$$\deg r(x)s(x) = \deg(r) + \deg(s) > \deg(s).$$

Question 52. (Biggs 22.7.2) Show that if $f(x)$ is non-constant, then f is either irreducible or

$$f(x) = g(x)h(x)$$

for some non-constant g, h whose degrees are less than that of f.

Solution. If f is irreducible, the only possible factorizations $f(x) = g(x)h(x)$ are when one of g and h is constant. Hence, if f is not irreducible, we can find non-constant g, h such that $f(x) = g(x)h(x)$. By previous exercise, $\deg f(x) = \deg g(x)h(x)$ is strictly greater than the degrees of g and h.

Question 53. (Biggs 22.7.3) Show that if 1 is the gcd of $r(x)$ and $s(x)$, and $r(x)$ is a divisor of $s(x)t(x)$ then $r(x)$ is a divisor of $t(x)$.

Solution. We can perform Euclid's algorithm and deduce that there are polynomials $a(x), b(x)$ such that

$$a(x)r(x) + b(x)s(x) = 1 \implies a(x)r(x)t(x) + b(x)s(x)t(x) = t(x).$$

Also, by definition of divisibility, there is some $r(x)$ such that

$$r(x)k(x) = s(x)t(x)$$

so

$$a(x)r(x)t(x) + b(x)r(x)k(x) = t(x)$$

Now, the left hand side is a multiple of $r(x)$ so $r(x) \mid t(x)$.

Question 54. (Biggs 22.7.4) If $r(x)$ is irreducible and $r(x) \mid s_1(x) \cdots s_k(x)$ then $r(x) \mid s_i(x)$ for some i.

Solution. We do induction over k. If $k = 1$, then there is nothing to prove. Assume now the statement is true for $k - 1$ factors. Since r is irreducible, we have $\gcd(r, s_1) \in \{1, r\}$. If $\gcd(r, s_1) = r$ we are done. If $\gcd(r, s_1) = 1$ we use previous exercise and deduce that $r \mid s_2(x) \cdots s_k(x)$, which by induction gives that $r \mid s_i$ for some i.

Question 55. (Biggs 22.7.5) Suppose

$$f(x) = g_1(x) \cdots g_r(x) = h_1(x) \cdots h_s(x)$$

where the g_is and h_js are monic irreducible, then $r = s$ and the two expressions are just rearrangements of one another.

Solution. We can do induction over the maximum number of factors which appears on both sides. We have that $g_1 \mid h_1 \cdots h_s$ so by previous exercise, $g_1 \mid h_j$ for some j. But this means $g_1 = h_j$, and we can divide both sides by g_1. This reduces the number of factors, and by induction hypothesis, unique factorization holds.

3.5. Exercises in Biggs

Same problems as previous lecture.

```
Read Chapter 22
22.1: 1,2,3
22.2: 1 (Find the sizes of the sets)
22.3: 1i, 3
22.4: 1,2,4
22.5: 1,2,3,4,5
22.6: 1
22.7: 1,2,3,4,5,6
22.8: 1
```

Lecture 4: Encryption

We now make the very reasonable assumption that communication channels such as Facebook, WhatsApp, Wechat, Snapchat are monitored.

4.1. Diffie–Hellman key exchange

Alice and Bob pick a number g and a prime p in public. They perform the following computations in $\mathbb{Z}_p$.

Alice chooses some a and Bob chooses b, in private. Alice sends g^a and Bob sends g^b. They can then both compute $g^{ab} = (g^a)^b = (g^b)^a$. This is now a common secret—Eve, who is listening to the channel, can only see (p, g, g^a, g^b) but this is not enough information to efficiently compute g^{ab}.

The reason is that given g and $g^a \pmod p$ it is hard to find a. This is called the **Discrete logarithm problem**.

Remark 56. It is important to choose g, so that g^a can take many different values. In fact, we pick g so that $\{g^1, g^2, g^3, \dots, g^{p-1}\}$ in fact are $\{1, 2, \dots, p-1\}$. Thus, if $p > 10^{100}$, we need to check 10^{100} potential values of a.

4.1.1. Quantum computers

Quantum computers can (theoretically) break RSA and the Diffie–Hellman key exchange. Current state-of-the art[1] quantum computers can factor 15 (2001), 21 (2012), $1,099,551,473,989$ (2019), and $261,980,999,226,229$ (2022).

4.2. RSA

We shall need the following lemma in the theory for RSA.

Lemma 57. *If p and q are* different *primes, then $a^{(p-1)(q-1)} = 1$ in $\mathbb{Z}_{pq}$, whenever a is not divisible by p or q.*

Proof. It suffices to show that $a^{(p-1)(q-1)} - 1$ is divisible by pq. First of all, we know that $a^{p-1} = 1 \bmod p$, so $a^{(p-1)(q-1)} - 1$ is a multiple of p. In the same manner, $a^{(p-1)(q-1)} - 1$ is a multiple of q. This implies $a^{(p-1)(q-1)} - 1$ is a multiple of pq and we are done. □

4.2.1. Overview of RSA

Choose in secret, two different primes p, q. In reality, 2048 bits, about 600 digits.

1. Set $n \coloneqq pq$ and $m \coloneqq (p-1)(q-1)$.

[1] As of March 2023

2. Construct e, d such that $ed \equiv_m 1$. This is done by first selecting e and then use Euclid's algorithm. We have

$$ed - mk = 1 \text{ (Diophantine equation to be solved, } e \text{ and } m \text{ are known).}$$

The number e is our **encryption key** and d is the **decryption key**.

3. So far we have $ed = k(p-1)(q-1)+1$. Let now $a < pq$ be the message we wish to send. This is **encrypted** by computing $a^e \mod n$. Even if someone knows a^e and e, it is hard to recover a.

4. Decryption is performed as follows: We receive a^e, and raise it to the tth power, and compute mod $n = pq$:

$$(a^e)^d = a^{ed} = a^{k(p-1)(q-1)+1} = a[a^{(p-1)(q-1)}]^k \equiv_{pq} a \cdot 1^k = a.$$

Here we have used the lemma that states that $a^{(p-1)(q-1)} \equiv_{pq} 1$.

In conclusion, p, q and d constitute the private key (secret) but n and e are public.

Question 58. A friend has the public key ($n = 21$, $e = 5$) and wishes to send $a = 4$. What do we send?

Solution. We compute $a^e = 4^5 \mod 21$. We have

$$4^5 \equiv 4 \cdot 16^2 \equiv 4 \cdot (-5)^2 \equiv 4 \cdot 25 \equiv 4 \cdot 4 \equiv 16.$$

So we send 16.

Question 59. We have the public-private key pair $n = 3 \cdot 7$, $e = 5$ and $d = 17$. Someone has sent us 16. What was the original message?

Solution. We know that $a^e \equiv_{pq} 16$ so the original message is $a^{de} \equiv_{pq} a$. So we must compute $16^d \mod pq = 21$. We have

$$16^{17} \equiv (-5)^{16+1}.$$

Now we perform repeated squaring and obtain

$$\begin{aligned}(-5)^2 &\equiv 25 \equiv 4\\ (-5)^4 &\equiv 4^2 \equiv 16 \equiv -5\\ (-5)^8 &\equiv (-5)^2 \equiv 25 \equiv 4\\ (-5)^{16} &\equiv 4^2 \equiv 16 \equiv -5.\end{aligned}$$

So

$$(-5)^{16+1} \equiv (-5)^{16} \cdot (-5) \equiv (-5)^2 \equiv 25 \equiv 4.$$

The original message was therefore 4.

Question 60. Is $(e = 16, d = 159)$ with $p = 13$, $q = 19$ a valid key-pair?

Solution. We can compute $m = (p-1)(q-1) = 12 \times 18$. In order for (e, d) to work, we must have that $ed \equiv_m 1$ holds. But since $\gcd(e, m) \geq 2$ this cannot be true. It follows that $(e = 16, d = 159)$ is not a valid key-pair for $n = pq$.

Question 61. Let $p_1, p_2, \ldots, p_k$ be different primes and set $n = p_1 p_2 \cdots p_k$. If a is not divisible by any of the p_i, prove that $a^{(p_1-1)(p_2-1)\cdots(p_k-1)} = 1$ in $\mathbb{Z}_n$.

Proof. It suffices to show that $a^{(p_1-1)(p_2-1)\cdots(p_k-1)} - 1$ is divisible by n. We know that $\gcd(a, p_1) = 1$ so by Fermat's little theorem, we know

$$a^{p_1-1} \equiv_{p_1} 1.$$

If we raise both sides to $(p_2 - 1)(p_3 - 1) \cdots (p_k - 1)$ we find that

$$a^{(p_1-1)(p_2-1)\cdots(p_k-1)} \equiv_{p_1} 1.$$

This statement also holds for any of the other primes, so we may conclude that

$$p_i \mid a^{(p_1-1)(p_2-1)\cdots(p_k-1)} - 1 \text{ for all } i.$$

But then $a^{(p_1-1)(p_2-1)\cdots(p_k-1)} - 1$ is a multiple[2] of $p_1 p_2 \cdots p_k = n$ and we are done. □

Question 62. (a) An RSA-crypto has the parameters $n = 55$ and encryption key $e = 17$. Find the decryption key d and decrypt the message $b = 5$.

(b) Let $p = 5$, $q = 21$, from which

$$n = 105, \qquad m = 80$$

are calculated. With the encryption key $e = 7$, we have produced $d = 23$. Use these keys to first encrypt the message $a = 3$, and then decrypt the result. *Find a reason why you did not recover the original message.*

Solution. (a) We have that $n = 55 = 5 \times 11$ so $p = 5$, $q = 11$ and $m = (p-1)(q-1) = 40$. We now seek d such that $de \equiv_{40} 1$. Since $e = 17$, this leads to solving the Diophantine equation

$$17d + 40m = 1.$$

Standard procedure gives

$$40 = 2 \cdot 17 + 6$$
$$17 = 3 \cdot 6 - 1$$

Thus

$$1 = 3 \cdot 6 - 17 = 3(40 - 2 \cdot 17) - 17 = 3 \cdot 40 - 7 \cdot 17$$

Hence, $d = -7 \equiv_{40} 33$. To decrypt the message $b = 5$, we need to compute $5^3 3 \bmod 55$. Repeated squaring gives

$$5^2 \equiv 25$$
$$5^4 \equiv 25^2 \equiv 625 \equiv 20$$
$$5^8 \equiv 20^2 \equiv 400 \equiv 15$$
$$5^{16} \equiv 15^2 \equiv 225 \equiv 5$$
$$5^{32} \equiv 5^2 \equiv 25$$

Thus, $5^{33} \equiv_{40} 25 \cdot 5 = 125 \equiv 15$. The original message is therefore $a = 15$.

[2]This also requires that the p_is are prime numbers.

Part (b): We encrypt the message as $b = a^e$, so we need to compute 3^7 mod 105. Since $3^4 = 81$, $3^5 = 243 \equiv_{105} 33$. Thus, $3^7 \equiv_{105} 33 \cdot 9 = 297 \equiv_{105} 87$.

To decrypt this message, we need to compute $87^{23} \equiv_{105} -18^{23} \equiv_{105} -18^{16+4+2+1}$. Same strategy as above gives (mod 105):

$$\begin{aligned} 18^2 &\equiv 324 \equiv 9 \\ 18^4 &\equiv 81 \equiv -24 \\ 18^8 &\equiv 24^2 \equiv 576 \equiv 51 \\ 18^{16} &\equiv 51^2 \equiv 2500 + 100 + 1 \equiv 81. \end{aligned}$$

Thus, $b^d = -18^{23} = -81 \cdot (-24) \cdot 9 \cdot 18 \equiv 33$. This is not the same as the original message, 3.

The issue is that $n = 105$ is not a product of two different primes since $q = 3 \times 7$. Hence we cannot expect the algorithm to work.

Lecture 5: Sets and maps

5.1. Injections, surjections, bijections

An **injection** is a map $f : X \to Y$ such that

$$x_1 \neq x_2 \implies f(x_1) \neq f(x_2).$$

Informally, different values are mapped to different values.

A **surjection** is a map $f : X \to Y$ such that

$$\text{for every } y \in Y \text{ there is some } x \in X \text{ such that } y = f(x).$$

Informally, everything in Y is hit by at least one element in X.

A **bijection** is a function which is both injective and surjective.

Observe that the existence of an injection or surjection between sets puts some constraints on the cardinalities of the sets. In this course, we shall only consider the cardinalities of finite sets, $\mathbb{N}$, $\mathbb{R}$ and $2^{\mathbb{N}}$.

Question 63. Determine for each of the following functions, if it is injective and/or surjective.

a) $f : \mathbb{N} \to \mathbb{N}$, $f(x) = x + 1$.

b) $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = x + 1$.

c) $f : \mathbb{Z} \to \mathbb{Z}$, where

$$f(x) = \begin{cases} x + 31 \text{ if } x \text{ is odd} \\ x - 47 \text{ if } x \text{ is even.} \end{cases}$$

d) $f : \mathbb{N} \to \mathbb{N}$, $f(x) = \lfloor x/2 \rfloor$.

e) $f : \mathbb{N} \to \mathbb{N}$, $f(x) = 1 + (x - 4)^2$.

Solution. a) injective, b) bijective, c) bijective, d) surjective e) neither.

5.1.1. Finite sets

Let X and Y be finite sets with the same size, and let $f : X \to Y$. Then the following statements are equivalent:

- f is injective;
- f is surjective
- f is bijective.

This proposition does not hold for infinite sets.

5.1.2. Composition of injections, surjections and bijections

Theorem 64. *Let $f : A \to B$ and $g : B \to C$ be maps. Then the composition $g \circ f : A \to C$ is*

- *injective, if both f and g are;*
- *surjective, if both f and g are;*
- *bijective, if both f and g are.*

A function has an **inverse** if and only if it is a bijection.

Question 65. Let $f : \mathbb{Z}_6 \to \mathbb{Z}_6$ be defined by $f(x) = 3x^2 + 1$. Describe a function $g : \mathbb{Z}_6 \to \mathbb{Z}_2$ such that the composition $g \circ f$ becomes a surjection.

Solution. The function $f(x)$ only assumes the values 1 and 4, so we can take

$$g(x) \coloneqq \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{otherwise.} \end{cases}$$

Question 66. An **involution** is a map which is its own inverse. Show that for any involution $f : X \to X$ with $X = \{1, 2, 3, \ldots, 99\}$ there must be some $x \in X$ with $f(x) = x$.

Proof. We shall prove the stronger statement: Let $n \geq 1$ and X be a set of cardinality $|X| = 2n-1$. Then any involution $f : X \to X$ has a fixed-point. The base case $n = 1$ is easy since then X only contains one element, so f maps this element to itself. Now suppose $f : X \to X$ with $|X| = 2n - 1$ and $n \geq 2$ and assume that the statement holds for involutions on sets of size $2n-3$. Consider any element $a \in X$. Then either $f(a) = a$ and we are done. Otherwise, $f(a) = b$ and $f(b) = a$ since f is an involution. But this means that we can consider f as an involution $f : X \setminus \{a, b\} \to X \setminus \{a, b\}$. By induction, the function on this set of size $2(n - 1) - 1 = 2n - 3$ has a fixed-point. □

5.2. Infinite sets and Cantor's diagonal argument

There is a video that shows that there is a bijection between $\mathbb{N}$ and $\mathbb{Q}$. Moreover, one can show (via Cantor's diagonal argument) that there is *not* a bijection between $\mathbb{N}$ and $\mathbb{R}$.

Question 67. Let $\mathcal{F}$ be the set of functions $f : \mathbb{N} \to \mathbb{N}$. Show that the cardinality of $\mathcal{F}$ is greater than that of $\mathbb{N}$. In other words, prove that there is no bijection $\beta : \mathbb{N} \to \mathcal{F}$.

Solution. Use Cantor's diagonal argument.

Question 68. Let $\mathcal{P}(\mathbb{N})$ denote the set of all subsets of $\mathbb{N}$. Produce a bijection $f : \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N})$.

Solution. The goal is to construct a bijection which sends $S \in \mathcal{P}(\mathbb{N})$ to a pair of sets $(T_1, T_2) \in \mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N})$. We can let the odd numbers in S determine the elements in T_1, and the even numbers in S determine T_2. For example, we can create T_1 and T_2 from S via the following rule:

$$\begin{cases} s \in T_1 & \text{if and only if } 2s - 1 \in S \\ s \in T_2 & \text{if and only if } 2s \in S. \end{cases}$$

It is not hard to see that this is a bijection, since the odd numbers $\{1, 3, 5, 7, \ldots\}$ are obtained from $\mathbb{N}$ via the map $x \mapsto 2x - 1$, and the even numbers $\{2, 4, 6, 8, \ldots\}$ constitute the image of the map $x \mapsto 2x$.

Question 69. A robot starts in some integer point in the plane (x_0, y_0). Every day forward, the robot moves $v_x \in \mathbb{Z}$ steps East and $v_y \in \mathbb{Z}$ steps North. The values of v_x and v_y are fixed and do not change. You do not know where the robot started or the values of v_x and v_y. However, every day you are allowed to check some coordinate (x, y) and see if the robot is there or not.

Describe a strategy which is guaranteed to find the robot after a finite number of days.

5.3. Combinatorial bijections

Let B_n be the set of binary words with n digits. Note that there are 2^n elements B_n. For example,

$$B_3 = \{000,\ 001,\ 010,\ 011,\ 100,\ 101,\ 110,\ 111\}$$

Let C_n be the number of **integer compositions** of n, i.e., the different ways of expressing n as a sum of positive integers. For example,

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

Describe a bijection between B_{n-1} and C_n.

Full solution can be found in the text Alexandersson – Discrete mathematics.

5.4. Exercises in Biggs

```
Read  5.2, 5.4, 6.1, 6.5--6.6, 9.2--9.4, 9.7
6.2: 1, 2
6.4: 1--3, 5
6.5: 1, 5
6.6: 1, 2
6.7: 1, 4--6, 9--11
9.2: 1
9.3: 1,2
9.7: 2,3
```

Lecture 6: Combinatorics I

The videos talk about ordered and unordered choice, with and without repetition. See the table in Alexandersson – Discrete Mathematics.

6.1. Counting maps

Question 70. Let $X = \{1, 2, 3\}$, $Y = \{a, b, c\}$ and $Z = \{a, b, c, d, e\}$.

(a) How many maps $f : X \to Y$ are there?

(b) How many bijections $g : X \to Y$ are there?

(c) How many injections $h :\to Z$ are there?

Solution.

$$\text{(a) } 3^3 \quad \text{(b) } 3! \quad \text{(c) } 5 \cdot 4 \cdot 3.$$

6.1.1. Discussion

Question 71. From 9 we shall pick two disjoint groups of people. In how many ways can this be done if

(a) the group sizes are 2 and 3;

(b) both groups have size 2;

(c) both groups have size 2 and they are named group A and group B.

Solution. (a) $\binom{9}{2}\binom{7}{3}$ (b) $\frac{1}{2}\binom{9}{2}\binom{7}{2}$ (c) $\binom{9}{2}\binom{7}{2}$

6.2. The stars and bars method

The **stars and bars** method is used when we want to count unordered choice with repetition. The bars are used to separate the different types of choices.

Question 72. 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?

Solution. Order of drinks does not matter, and there are $3 \cdot 2 = 6$ 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.

Question 73. 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.

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

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

ways to do this.

Question 74. How many integer solutions are there to the system of inequalities

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

Solution. 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.

Question 75. 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.

Solution. 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 stars-and-bars formula tells 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.

6.3. Binomial identities

Question 76. Prove that

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

Solution. 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

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

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

Alternative proof: Start with $(2x+y)^n$, expand with the binomial identity. Take the derivative with respect to x on both sides, and then put $x = y = 1$.

Question 77. Prove that

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

Solution. 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.

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.

6.4. Pigeon-hole principle or mailbox-principle

Theorem 78 (Mailbox principle)**.** *If X and Y are finite sets with $|X| > |Y|$ and $f : A \to B$, then there must be some $i \neq j$ such that $f(i) = f(j)$.*

Question 79. What is the maximum number of rooks you can place on an 8×8 chessboard so that no two rooks can attack each other?

Question 80. 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.

Solution. 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[1] 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.

[1] At least!

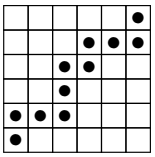
Question 81. In an 57×8-board(*57 rows with 8 squares in each*), three coins are placed in each row.

1. Show that there are four squares forming a rectangle, where there is a coin in each corner.
2. The same problem for an 29×8-board.

Solution. a) There are $\binom{8}{3} = 56$ possible rows, so two rows must be equal. Hence, we have a rectangle.

b) We can pretend there are only 2 coins in each row. There are $\binom{8}{2} = 28$ such arrangements of rows, so with 29 rows, there are two such equal rows.

Question 82. In a 6×6-grid, one can make paths starting in the box in the lower left hand corner, and ending in the upper right hand corner. In each step of the path you either walk to the box above, or to the box on the right.



a) Calculate the total number of such paths—answer with an integer.

b) Suppose that each box contains an integer between 0 och 22. The *value* of a path is the sum of all the boxes which has been visited. Show that there are two different paths with the same value.

Solution. a) In a path, one needs to take exactly 5 steps up, and 5 steps to the right. There are therefore 10 steps in total and we must choose which 5 of these are up-steps. Hence, there are

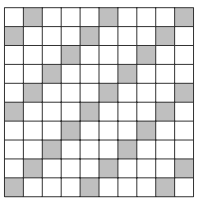
$$\binom{10}{5} = \frac{10 \cdot 9 \cdot 8 \cdot 7 \cdot 6}{5 \cdot 4 \cdot 3 \cdot 2} = 2 \cdot 9 \cdot 2 \cdot 7 = 63 \cdot 4 = 252$$

such paths.

b) Every path visits exactly 11 boxes, so the maximal value possible for a path is $11 \times 22 = 242$. Therefore, there are 243 possible values, but we saw that there are 252 different paths. The mailbox principle then implies that there are at least two paths with the same value.

Question 83. Consider a 10×10 board with 100 squares. Can this board be covered with 25 tetris pieces of the shape □□□□?

Solution. Suppose there is such a covering. We color the board as follows:



There are 26 black squares on the board, which forces at least one tetris piece to contain at least two black squares. But this is impossible.

6.5. Exercises in Biggs

```
Read 6.2-6.4, 10.1-10.4, 11.1-11.3
6.2: 1-2
6.4: 1-3
10.1: 2-3
10.2: 1-2, 4-5
10.3: 1-3
10.4: 1-3
```

Question 84. (*Biggs 6.7.8 (Erdős–Szekeres theorem)*) Consider a sequence $x_1, \ldots, x_r$ of distinct natural numbers. Let m_i be the length of the longest increasing subsequence, starting from x_i and n_i be the length of longest decreasing subsequence starting from x_i. Show that $f : \{1, 2, \ldots, r\} \to (m_i, n_i)$ is an injection. Deduce that $x_1, \ldots, x_{nm+1}$ has either an increasing subsequence of length $m + 1$ or a decreasing subsequence of length $n + 1$ (or both).

Solution. Suppose $i < j$ and let us compare (m_i, n_i) and (m_j, n_j). In order for f to be surjective, we need to show that these pairs differ.

1. If $x_i < x_j$, then $m_i > m_j$, as we can append x_i, and make a longer increasing subsequence.
2. If $x_i > x_j$, then $n_i > n_j$, as we can append x_i, and create a longer decreasing subsequence.

Hence, all pairs (m_i, n_i) are different. Now, if are is no increasing subsequence of length $m + 1$, and no decreasing subsequence of length $n + 1$, then the number of pairs here can be at most $m \times n$.

But if $r = mn + 1$, this is impossible, as we then would need an injection $[nm + 1] \to [nm]$.

Lecture 7: Combinatorics II

7.1. Multinomials and Stirling numbers

Multinomial coefficients: We have that

$$\binom{n}{a,b,c,d} = \frac{n!}{a!b!c!d!}$$

is the number of words consisting of a letters A, b letters B, and so on, with a total length of $n = a + b + c + d$.

Question 85. We have four different dishes, two dishes of each type. In how many ways can these be distributed among 8 people?

Solution. 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.

Question 86. How many flags can we make with 7 stripes, if we have 2 white, 2 red and 3 green stripes?

Solution. It is given by the multinomial coefficient

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

7.2. Stirling numbers

Stirling numbers: $S(n,k)$ counts the number of ways to partition n different objects into k non-empty piles. *The piles are not named!* The main recursion for the Stirling numbers is the following:

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

Here are the values of $S(n,k)$ for $1 \leq k \leq n$:

$$\begin{array}{cccccc}
1 & & & & & \\
1 & 1 & & & & \\
1 & 3 & 1 & & & \\
1 & 7 & 6 & 1 & & \\
1 & 15 & 25 & 10 & 1 & \\
1 & 31 & 90 & 65 & 15 & 1
\end{array}$$

Remark 87. The number of surjections from $\{1, 2, \ldots, n\}$ to $\{1, 2, \ldots, k\}$ is $k!S(n, k)$.

Question 88. How many words of length 6 can be made using letters from $\{a, b, c\}$ when

(a) there is no additional requirement.

(b) The letters must appear in alphabetical order.

(c) Each letter must appear at least once.

Solution. (a) We get 3^6

(b) By using stars and bars, $\binom{6+2}{2}$.

(c) Same as counting surjections $f : \{1, \ldots, 6\} \to \{a, b, c\}$, so we get $3! \cdot S(6, 3)$.

7.3. Inclusion–exclusion

Venn-diagram:

$$|A \cup B \cup C| = |A| + |B| + |C| - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$$

Theorem 89 (Inclusion–Exclusion)**.** *For finite sets $A_1, A_2, \ldots, A_n$ we have that*

$$\left| \bigcup_{j=1}^{n} A_j \right| = \sum_{k=1}^{n} (-1)^{k+1} \sum_{i_1, i_2, \ldots i_k} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}| .$$

Proof. We want to ensure that an element in $A_1 \cup A_2 \cup \cdots \cup A_n$ is counted exactly once in the right hand side (when taking the signs into consideration). Suppose x appears in *exactly* $1 \leq m \leq n$ of the sets. By symmetry, we can assume that x belongs to $A_1, A_2, \ldots, A_m$ but none of the other sets. Then

- for $k = 1$, x is counted $\binom{m}{1}$ times, one for each of $|A_1|, \ldots, |A_m|$;
- for $k = 2$, x is counted $(-1)\binom{m}{2}$ times, once in each intersection $|A_i \cap A_j|$; and so on until
- for $k = m$, where x is counted $(-1)^{m+1}$ times, in the single term $|A_1 \cap A_2 \cap \cdots \cap A_m|$.

In x is counted $\sum_{k=1}^{m} (-1)^{k+1} \binom{m}{k}$. But we have that

$$\begin{aligned} \sum_{k=1}^{m} (-1)^{k+1} \binom{m}{k} &= 1 + \sum_{k=0}^{m} (-1)^{k+1} \binom{m}{k} \\ &= 1 - \underbrace{\sum_{k=0}^{m} (-1)^{k} \binom{m}{k}}_{\text{binomial theorem}} \\ &= 1 - (1-1)^m = 1 \end{aligned}$$

so x is counted exactly once. Since this argument holds for every x in the union in the left hand side, we have that both sides agree. □

Question 90. Determine the number of functions $f : \{1, 2, 3, 4\} \to \{1, 2, 3, 4, 5\}$ with the property that $f(1) \neq f(2)$ and $f(3) \neq f(4)$.

Solution. We get $5^4 - 5^3 - 5^3 + 5^2$.

Question 91. How many numbers from $\{1, \ldots, 100\}$ are divisible by either 3, 5 or 11?

Solution. We count. Simple division tells us that there are

- 33 numbers divisible by 3,
- 20 numbers divisible by 5, and
- 9 numbers divisible by 11.

Moreover,

- 6 numbers divisible by 3 and 5,
- 3 numbers divisible by 3 and 11,
- 1 numbers divisible by 5, and 11.

Finally, no number is divisible by all three. Hence, we get

$$33 + 20 + 9 - (6 + 3 + 1) = 62 - 10 = 52.$$

Question 92. How many partitions are there of the numbers $\{1, 2, \ldots, 8\}$ into four sets, such that 1 and 2 are not in the same set and 2 and 3 are not in the same set.

Solution. The answer is

$$S(8, 4) - S(7, 4) - S(7, 4) + S(6, 4)$$

corresponding to *all partitions*, $1, 2$ *in the same block*, $2, 3$ *in the same block*, and $1, 2, 3$ *in the same block*.

Question 93. 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?

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

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

Question 94. How many permutations of the letters `aabbbcde` are there, under the following conditions.

(a) No additional requirement.

(b) The subword `aa` may not appear.

(c) Neither `aa` nor `bbb` may appear as subwords.

Solution. We have the following answers:

(a) $\frac{8!}{2!3!}$.

(b) $\binom{8}{2,3,1,1,1} - \binom{7}{3,1,1,1,1}$.

(c)

$$\binom{8}{2,3,1,1,1} - \binom{7}{3,1,1,1,1} - \binom{6}{2,1,1,1,1} + \binom{5}{1,1,1,1,1} = \frac{8!}{2!3!} - \frac{7!}{3!} - \frac{6!}{2!} + 5!$$

Question 95. 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?

Solution. 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.

Question 96. 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?

Solution. 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

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

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 (Either 123 and 234 are increasing, or 123 and 234 are both decreasing). Similar to the previous reasoning, this gives

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

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

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

Question 97. Answer the following questions:

(a) How many monic polynomials of degree 2 are there in $\mathbb{Z}_7[x]$?

(b) How many *irreducible* monic polynomials of degree 2 are there in $\mathbb{Z}_7[x]$?

Solution. (a) A monic polynomial of degree 2 in $\mathbb{Z}_7[x]$ is of the form $x^2 + ax + b$, where $a, b \in \mathbb{Z}_7$. This gives $7^2 = 49$ different polynomials.

(b) (b) A *reducible* polynomial of degree 2 factors as $(x+p)(x+q)$, but the order of p and q does not matter. There are 7 polynomials with a double-zero, and $\binom{7}{2} = 21$ polynomials with different zeros. The number of irreducible polynomials in $\mathbb{Z}_7[x]$ is therefore $49 - (7 + 21) = 21$.

Question 98. 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 $K\spadesuit$?

Solution. It is easier to first count the number of forbidden shuffles.

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

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

7.3.1. Explicit formula for Stirling numbers

Question 99. We have k different boxes and n different objects. We want to distribute the objects into the boxes such that at no box is empty[1]. In how many ways can this be done?

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

$$\binom{k}{1}(k-1)^n - \binom{k}{2}(k-2)^n + \binom{k}{3}(k-3)^n + \cdots + (-1)^k \binom{k}{k-1}(1)^n$$

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

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

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

Note that this gives a formula for the Stirling numbers:

$$S(n,k) = \frac{1}{k!}\sum_{j=0}^{k}(-1)^j\binom{k}{j}(k-j)^n.$$

Question 100. *(From USAMO 1972:3)* We generate a list of n numbers in $1,\ldots,9$ with equal probability. What is the probability that the product is a multiple of 10?

Solution. The total number of such selections is 9^n—choose each of the n numbers independently. We now want to compute the number of selections resulting in a product *not* divisible by 10. This can fail in the following two ways: *The product is not divisible by* 2 and *The product is not divisible by* 5.

Not being divisible by 2, means that it is a product of the numbers in $\{1,3,5,7,9\}$, so there are 5^n such selections. Similarly, there are 8^n selections where the product is not divisible by 5. Finally, being not divisible by either 2 or 5, is 4^n. Hence, the total number of selections which give divisibility by 10, is therefore (by inclusion-exclusion)

$$9^n - 8^n - 5^n + 4^n.$$

Thus, the probability of being a multiple of 10 is:

$$\frac{9^n - 8^n - 5^n + 4^n}{9^n}$$

which, as $n \to \infty$ is equal to 1.

Question 101. *(Biggs, Chapter 11.4, Example 2)* A bijection f from $\{1,2,\ldots,n\}$ to itself is called a **derangement** if it has no fixed-points. That is, there is no x such that $f(x) = x$. Show that the number of such derangements, is equal to

$$\sum_{k=0}^{n}(-1)^k\frac{n!}{k!}.$$

Solution. Let X be the set of bijections and let A_j be the set of bijections where j is a fixed-point. Clearly, $|X| = n!$, and we are interested in

$$|X - (A_1 \cup A_2 \cup \cdots \cup A_n)|.$$

The number of bijections where j is a fixed-point is $(n-1)!$, since we know $f(j) = j$, and we then choose a bijection on the remaining $n-1$ elements. In a similar manner, we can show that if $j_1, j_2, \ldots, j_k$ are different, we have that

$$|A_{j_1} \cap A_{j_2} \cap \cdots \cap A_{j_k}| = (n-k)!,$$

since we have k different elements which are required to be fixed-points. The principle of inclusion-exclusion states that $|X - A_1 \cup A_2 \cup \cdots \cup A_n|$ is given by

$$\begin{aligned} n! - \sum_{j_1}^{n}|A_{j_1}| + \sum_{j_1<j_2}^{n}|A_{j_1}\cap A_{j_2}| - \sum_{j_1<j_2<j_3}^{n}|A_{j_1}\cap A_{j_2}\cap A_{j_3}| + \cdots \\ + (-1)^{n+1}\sum_{j_1<j_2<\cdots<j_n}|A_{j_1}\cap A_{j_2}\cap\cdots\cap A_{j_n}|. \end{aligned}$$

There are $\binom{n}{k}$ ways to choose $j_1 < j_2 < \cdots < j_k$, and we know the sizes of the intersections, so the number of derangements is given by

$$n! - \binom{n}{1}(n-1)! + \binom{n}{2}(n-2)! - \binom{n}{3}(n-3)! + \cdots + (-1)^n \binom{n}{n}(n-n)!.$$

Rewriting this as a sum, we get

$$\sum_{k=0}^{n}(-1)^k \binom{n}{k}(n-k)! = \sum_{k=0}^{n}(-1)^k \frac{n!}{k!}$$

and we are done.

Probability that a random permutation is a derangement:

$$\frac{1}{n!}\sum_{k=0}^{n}(-1)^k \frac{n!}{k!} = \sum_{k=0}^{n}\frac{(-1)^k}{k!} \approx e^{-1} = 1/2.718 \approx 0.37$$

7.4. Exercises in Biggs

```
Read 10.5, 12.1-12.3, 11.4-11.5
10.1: 2, 3
10.2: 1, 2, 4, 5
10.3: 1-3
10.4: 1-3
10.5: 1, 2
11.4: 1-3
11.5: 1, 2
12.1: 1, 2
12.3: 1, 2, 5
12.7: 12
```

Lecture 8: Equivalence relations

8.1. Special properties of relations

A **relation** on some set X is a subset of $X \times X$. We write $x\mathcal{R}y$ if (x, y) is part of the relation. We have special symbols for commonly used relations, for example $<$, $\leq$ and $\equiv_n$.

Relations $\mathcal{R}$ can be *reflexive*, *symmetric* and *transitive*.

- **Reflexive:** $x\mathcal{R}x$ holds for all x in the set.
- **Symmetric:** $x\mathcal{R}y \implies y\mathcal{R}x$.
- **Transitive:** $x\mathcal{R}y \wedge y\mathcal{R}z \implies x\mathcal{R}z$.

Question 102. Let M be the set of all *non-empty* subsets of $\{1, 2, \ldots, 5\}$. Note that M has 31 elements. Determine which of the following relations are *reflexive*, *symmetric* and *transitive*, respectively.

Relation M	Reflexive	Symmetric	Transitive
Is subset of, $\subseteq$	·	·	·
Has the same smallest element	·	·	·
Has the same size as	·	·	·
Has no intersection with	·	·	·
Has a strictly less total sum	·	·	·
$A \mathcal{R} B$ iff $(A \cap \{1, 2, 3\}) \subseteq (B \cap \{1, 2, 3\})$	·	·	·
$A \mathcal{R} B$ iff $\lvert A \cup B \rvert = 5$	·	·	·
$A \mathcal{R} B$ iff $A \setminus B = \{1\}$	·	·	·

Solution. The following table indicates which properties hold.

Relation M	Reflexive	Symmetric	Transitive
Is subset of, $\subseteq$	♡	·	♡
Has the same smallest element	♡	♡	♡
Has the same size as	♡	♡	♡
Has no intersection with	·	♡	·
Has a strictly less total sum	·	·	♡
$A \mathcal{R} B$ iff $(A \cap \{1, 2, 3\}) \subseteq (B \cap \{1, 2, 3\})$	♡	·	♡
$A \mathcal{R} B$ iff $\lvert A \cup B \rvert = 5$	·	♡	·
$A \mathcal{R} B$ iff $A \setminus B = \{1\}$	·	·	♡

8.2. Equivalence classes

Relations for which are all three properties (reflexive, symmetric, transitive) hold are called **equivalence relations**. Such a relation partitions the set A into equivalence classes.

Examples of such relations: $a \sim b$ if $f(a) = f(b)$. $\equiv_p$. "Have the same color".

All elements which are equivalent under a particular equivalence relation, form an **equivalence class**. It is common to use $[a]$ to denote *the set of all elements equivalent to* a. It is natural to ask how many equivalence classes there are, and if there is some natural **representative** from each equivalence class. For example, we let the elements in $\mathbb{Z}_n$ be the representatives for the integers under the $\equiv_n$ relation. We may also ask if all equivalence classes have the same cardinality.

Equivalence relations can be interesting on their own, but in practice, they are often studied when there is some additional underlying structure. For example, how does the equivalence relation behave together with addition or multiplication?

Question 103. How many different equivalence relations can one define on a set with 4 elements, and exactly 2 equivalence classes?

Solution. An equivalence relation is defined by its set of equivalence classes. In our case, we need to partition the 4 elements into two non-empty sets. The number of ways to do this is $S(4, 2)$, a Stirling number.

Question 104. Show that the relation $\sim$, defined by $a \sim b$ iff $|a - b| \leq 5$, is not an equivalence relation.

Solution. Transitivity fails. We have $0 \sim 5$ and $5 \sim 10$ but we do not have $0 \sim 10$.

Question 105. We define the following relation on polynomials in $\mathbb{R}[x]$; write $P \sim Q$ if and only if $P(1) = Q(1)$.

Show that this is an equivalence relation, and describe all polynomials in the same equivalence class as $3x + 2$.

Solution. The equivalence class consists of all polynomials of the form $(x - 1)R(x) + 5$, where $R(x) \in \mathbb{R}[x]$.

Question 106. Let $B = \{0, 1\} \times \{0, 1\} \times \{0, 1\} \times \{0, 1\}$, i.e.,

$$B = \{(0, 0, 0, 0), (0, 0, 0, 1), (0, 0, 1, 0), \ldots, (1, 1, 1, 0), (1, 1, 1, 1)\}.$$

For $x, y \in B$, we write $x\mathcal{R}y$ if and only if x can be obtained from y by a series of cyclic rotations of the entries in the list. For example, $(1, 0, 1, 0)\mathcal{R}(0, 1, 0, 1)$ and $(1, 1, 1, 0)\mathcal{R}(1, 0, 1, 1)$, but $(1, 0, 1, 0)$ is not related to $(1, 1, 0, 0)$.

(a) Show that $\mathcal{R}$ is an equivalence relation.

(b) How many equivalence classes does $\mathcal{R}$ have?

Solution. a) We have that $\mathcal{R}$ is reflexive since x can be obtained from x by 0 steps (or 4 steps). Moreover, $\mathcal{R}$ is symmetric since if x can be obtained from y, we can perform the same rotations in the opposite direction to obtain y from x. Finally, $\mathcal{R}$ is transitive, since if we need s steps to go rotate x to y, and t steps to go from y to z, then we can go from x to z by performing $s + t$ steps.

b) There are six equivalence classes:

$$[(0, 0, 0, 0)], [(0, 0, 0, 1)], [(0, 0, 1, 1)], [(0, 1, 0, 1)], [(0, 1, 1, 1)] \text{ and } [(1, 1, 1, 1)].$$

Question 107. Let us define the relation $\sim$ on polynomials in $\mathbb{R}[x]$, where $P \sim Q$ if and only if (x^2+1) divides the difference $P - Q$.

1. Show that every polynomial in $\mathbb{R}[x]$ is equivalent to some polynomial of the form $a + bx$.
2. Show that $a + bx \sim c + dx$ if and only if $a = b$ and $c = d$.
3. Show that if $P_1 \in [P]$ and $Q_1 \in [Q]$ then
$$P_1 + Q_1 \in [P + Q] \text{ and } P_1 \cdot Q_1 \in [P \cdot Q].$$
This shows that we can define addition and multiplication on equivalence classes (i.e., no matter which representatives we pick from $[P]$ and $[Q]$ we take, the result is the same).
4. Compute the remainder of $(a + bx)(c + dx)$ when dividing by $x^2 + 1$.
5. Compute $(a + bi)(c + di)$.

Question 108. Let $M_{2,2}$ be the set of invertible 2×2-matrices with complex entries. We write $A \sim B$ if and only if there is some invertible matrix T such that $TAT^{-1} = B$.

1. Show that $\sim$ is an equivalence relation.
2. Show that $A \sim B$ implies that $\det A = \det B$.
3. Show that $A \sim B \iff A^{-1} \sim B^{-1}$.

Question 109. Let $\sim$ be the relation on functions from $\mathbb{N}$ to $\mathbb{N}$ where we write $f \sim g$ if and only if there is some integer N such that $f(n) = g(n)$ whenever $n \geq N$. Prove that $\sim$ is an equivalence relation and determine the cardinality of the set of equivalence classes. Prove that the each equivalence class is countable.

Solution. It is straightforward to verify the reflexive and symmetric properties of $\sim$. Suppose now that $f \sim g$ and $g \sim h$, i.e
$$n \geq N \implies f(n) = g(n) \text{ and } m \geq M \implies g(m) = h(m).$$
It then follows that
$$n \geq \max(N, M) \implies f(n) = h(n),$$
so $f \sim h$. Now, let f be a fixed function. Then, each of the sets
$$G_N \coloneqq \{g : g(N-1) \neq f(N-1) \text{ and } n \geq N \implies g(n) = f(n)\}$$
is countable, since we only need to specify the values of $g(x)$ for all $x = 1, 2, \ldots, N-1$. Moreover, every function equivalent to f belongs to some G_N, so all functions equivalent to f are in the union $\{f\} \cup G_1 \cup G_2 \cup \cdots$. This is a countable union of countable sets, so the union is countable. Hence each equivalence class is countable.

8.3. Exercises in Biggs

```
Read 7.1-7.4, 9.1, 13.1
7.2: 1-3
7.3: 1-4
7.7: 1-3
12.2: 1, 2, 5
```

For exercise 7.3.1, the number 100 is missing in the answers.

Lecture 9: Permutations

Permutations are bijections on some finite set. The set of permutations on $\{1, 2, \ldots, n\}$ is denoted S_n. The 'S' stands for the **symmetric group**.

- To describe permutations, we have **2-line notation** and **cycle form notation**. By keeping only the bottom row in the two-line notation we get the **one-line notation**.
- We have **integer partitions** and can describe these in the following notation:

$$4 + 4 + 3 + 2 + 1 + 1 = (4, 4, 3, 2, 1, 1) = [1^2\ 2\ 3\ 4^2].$$

  Integer partitions are used to describe the **cycle type** of a permutation.
- There is a formula for counting the number of permutations with cycle type $[1^{\alpha_1} 2^{\alpha_2} \ldots k^{\alpha_k}$, namely

$$\frac{n!}{1^{\alpha_1} \cdot 2^{\alpha_2} \cdot \cdots k^{\alpha_k} \cdot \alpha_1! \cdots \alpha_k!}$$

- **Conjugate permutations**: $\pi = \sigma^{-1}\tau\sigma$. Being **conjugate to** is an equivalence relation and all permutations of the same cycle type constitute an equivalence class.
- We have even and odd permutations. For $n \geq 2$, half of the permutations are even, the other half is odd. This is sgn, *(Sv. tecknet)*, and the sign is defined as $(-1)^r$, where r is the number of transpositions in some representation.

Question 110. Let $f : \mathbb{Z}_{10} \to \mathbb{Z}_{10}$ be defined by av $f(x) = 3x + 4$. *Show that f is a bijection, and describe its cycle type.*

Solution. The map gives that f is the permutation $(1, 7, 5, 9)(2, 10, 4, 6)(3)(8)$, so its type is $[1^2 4^2]$.

9.1. Permutations as matrices

This part is not in Biggs but it is a rather nice way to talk about permutations and their signs.

Consider a matrix with exactly one 1 in each row and column. Such a matrix is called a **permutation matrix**, and when we multiply by a permutation matrix on the right of a vector, we permute the entries in the vector.

$$\begin{bmatrix} 0 & 0 & 0 & \mathbf{1} & 0 & 0 \\ \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \mathbf{1} \\ 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \mathbf{1} & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{bmatrix} = \begin{bmatrix} x_4 \\ x_1 \\ x_3 \\ x_6 \\ x_2 \\ x_5 \end{bmatrix} \qquad \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 1 & 3 & 6 & 2 & 5 \end{pmatrix}$$

Each permutation $\pi \in \mathrm{S}_n$ has a corresponding permutation matrix P_π of size $n \times n$. In particular, the identity permutation corresponds to the identity matrix. Composition of permutations corresponds to matrix multiplication of the corresponding permutation matrices. In other words, $P_{\sigma\pi} = P_\sigma P_\pi$.

We shall now explore the connection between $\operatorname{sgn}(\pi)$ and $\det(P_\pi)$.

- The determinant of the identity matrix is 1.
- If $\tau = (i\ j)$ is a transposition, it is obtained from the identity matrix by swapping rows i and j. Hence, the permutation matrix corresponding to a transposition has determinant -1.
- We know that $\det(P_\sigma P_\pi) = \det(P_\sigma)\det(P_\pi)$.

We now have that if

$$\pi = \tau_1\tau_2\cdots\tau_r = \tau_1'\tau_2'\cdots\tau_s'$$

then

$$\det(P_\pi) = \det(P_{\tau_1})\cdots\det(P_{\tau_r}) = \det(P_{\tau_1'})\cdots\det(P_{\tau_s'})$$

and it follows that $\det(\pi) = (-1)^r = (-1)^s$. Hence, s and t must have the same parity and $\operatorname{sgn}(\pi) = \det(P_\pi)$.

9.2. Multiplying with a transposition

Question 111. Let $\pi \in \mathrm{S}_n$ be a permutation. Describe with words what happens when we compute $(i\ j)\pi$ and $\pi(i\ j)$ in two-line notation. That is, what is the effect of multiplying to the left of π with a transposition, versus multiplying on the right.

Solution. Let us consider π in 2-line notation, and treat the product $(i\ j)\pi$ first. There are some entries a and b such that $\pi(a) = i$, $\pi(b) = j$.

$$\begin{bmatrix} 1 & 2 & \cdots & a & \cdots & b & \cdots & n \\ \pi_1 & \pi_2 & \cdots & i & \cdots & j & \cdots & \pi_n \end{bmatrix}$$

If we first apply this permutation, and then the transposition $(i\ j)$, the result must then be

$$\begin{bmatrix} 1 & 2 & \cdots & a & \cdots & b & \cdots & n \\ \pi_1 & \pi_2 & \cdots & j & \cdots & i & \cdots & \pi_n \end{bmatrix}$$

so $(i\ j)\pi$ is just the same as π but the *values* i and j have been swapped.

We shall now treat the product $\pi(i\ j)$. We can write π in two-line notation as follows:

$$\begin{bmatrix} 1 & 2 & \cdots & i & \cdots & j & \cdots & n \\ \pi_1 & \pi_2 & \cdots & \pi_i & \cdots & \pi_j & \cdots & \pi_n \end{bmatrix}.$$

The product then sends i to π_j and vice versa. That is,

$$\pi(i\ j) = \begin{bmatrix} 1 & 2 & \cdots & i & \cdots & j & \cdots & n \\ \pi_1 & \pi_2 & \cdots & \pi_j & \cdots & \pi_i & \cdots & \pi_n \end{bmatrix},$$

so the effect of multiplying on the right with $(i\ j)$ is the same as swapping the *entries* at positions i and j.

9.3. Permutations as transpositions and signs

Any cycle can be factored into transpositions:

$$(x_1\ x_2\ \ldots\ x_k) = (x_1\ x_k)(x_1\ x_{k-1})\cdots(x_1\ x_3)(x_1\ x_2).$$

Verify this! Note that if k is even, then we get an odd number of transpositions.

Question 112. Write $\pi = (1\ 3\ 9)(2\ 4\ 6)(5\ 8)(7)$ as a product of transpositions.

There are several ways to compute the sign for $\pi \in \mathrm{S}_n$:

- It is given by $(-1)^r$, the number of transpositions r needed to represent π.
- It is $(-1)^{\text{number of even cycles}}$.
- It is $(-1)^{n-c(\pi)}$ where $c(\pi)$ is the number of cycles (including 1-cycles). *This can be proved using induction over n.*

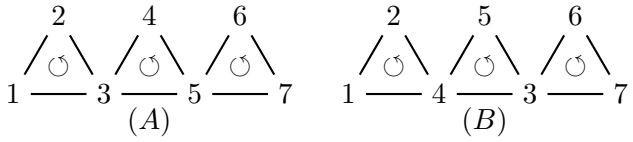
Question 113. Prove that the sign of a permutation $\pi \in \mathrm{S}_n$ is $(-1)^{n-c(\pi)}$ where $c(\pi)$ is the number of cycles.

Solution. We know that a cycle $(x_1\ x_2\ \ldots\ x_k)$ can be factored as into $k-1$ transpositions. Thus, if the cycle sizes are $k_1, k_2, \ldots, k_\ell$, then we can use total of

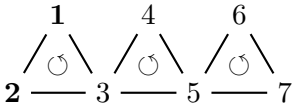
$$(k_1 - 1) + (k_2 - 1) + \cdots + (k_\ell - 1) = (k_1 + k_2 + \cdots + k_\ell) - \ell = n - \ell.$$

transpositions in a product for π. So, the sign is $(-1)^{n-\ell}$ and we are done.

Question 114. 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.

Solution. 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.

9.4. Order of a permutation

The order of a permutation is the smallest $k \geq 1$ such that $\pi^k = id$.

- What is the order of a single cycle $(1\ 2\ 3\ \cdots k)$?
- What is the order of $(1\ 2)(3\ 4\ 5)$?

We have that if the cycles have length $(c_1, c_2, \ldots, c_r)$ then the order is $\text{lcm}(c_1, c_2, \ldots, c_r)$. Note that this implies that two permutations of the same type has the same order.

Question 115. Let π be a permutation such that order(π) is odd. Prove that π must be even.

Solution. 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.

9.5. Problems

Question 116. 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) Express π as a product of simple transpositions.

Solution. 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 type$(\pi) = (3, 3)$ and type$(\sigma) = (4, 1, 1)$.

(e) We have $\text{lcm}(3, 3) = 3$ so order$(\pi) = 3$. Similarly, $\text{lcm}(1, 4, 1) = 1$ so 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) We have that $\pi = (2,3) \circ (1,2) \circ (4,5) \circ (5,6)$ but there are other solution.

Question 117. Prove that a permutation is even if and only if its inverse is even.

Solution. Let $\pi = \tau_1 \tau_2 \cdots \tau_\ell$ be a product of transpositions. Then we can easily verify that (Verify first that $\tau^2 = e$ whenever τ is a transposition.)

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

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

Question 118. Let $\pi = (1\ 5\ 7)(2\ 3)(4\ 8\ 6)$, and $\tau = (1\ 8)(2\ 5\ 4)(3\ 6\ 7)$. Find $\sigma \in \mathrm{S}_8$ such that $\tau = \sigma\pi\sigma^{-1}$.

Solution. We want σ to send each cycle of π to a cycle of τ. For example, $(157) \to (254)$, $(486) \to (367)$ and $(23) \to (18)$. Hence, take

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 8 & 3 & 5 & 7 & 4 & 6 \end{bmatrix}$$

We now have $\tau = \sigma\pi\sigma^{-1}$.

Question 119. Let A_n be the set of even permutations. Show that $|A_n| = n!/2$ whenever $n \geq 2$.

Solution. We shall prove this by using a bijection. Let B_n be the set of odd permutations. Let us define the function $f(\pi) = (1\ 2) \circ \pi$. Note that $f(f(\pi)) = \pi$, so f is invertible (it is its own inverse). Hence, f is a bijection from S_n to S_n. Now note that if $\pi \in A_n$, then $f(\pi) \in B_n$, since we go from an even number of transpositions to an odd number. Hence, we must have that $|A_n| = |B_n|$. That is, A_n contains exactly half of the elements in S_n.

Question 120. 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?

Solution. 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

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

Question 121. How many permutations $\sigma \in \mathrm{S}_8$ have the property that

(a) $\sigma(\sigma(1)) = 1$?

(b) both $\sigma(\sigma(1)) \neq 1$ and $\sigma(\sigma(2)) \neq 2$ holds?

Solution. If $\sigma(\sigma(1)) = 1$, then either $\sigma(1) = 1$, or 1 is in some two-cycle $(1\ a)$ for some $a = 2, 3, \ldots, 8$. There are 7! permutations where 1 is fixed. The number of permutations where 1 is in a 2-cycle is $7 \cdot 6!$, since we must choose a (7 ways) and the remaining 6 elements can be permuted freely. This gives a total of $2 \cdot 7!$ such permutations.

We shall use inclusion-exclusion for the second question. The number of permutations with $\sigma(\sigma(2)) = 2$ is also $2 \cdot 7!$, by the same argument as above. We must now determine the number of permutations where $\sigma(\sigma(1)) = 1$ and $\sigma(\sigma(2)) = 2$. The same reasoning as above shows that we have the following mutually exclusive alternatives.

- $\sigma(1) = 1$ and $\sigma(2) = 2$. This gives 6!.
- $\sigma(1) = 1$ and $(2\,a)$ is a 2-cycle for some $a \geq 3$. This gives $6 \cdot 5!$.
- $\sigma(2) = 2$ and $(1\,a)$ is a 2-cycle for some $a \geq 3$. This gives $6 \cdot 5!$.
- $(1\,a)$ and $(2\,b)$ are different 2-cycles for some $a, b \geq 3$, $a \neq b$. This gives $6 \cdot 5 \cdot 4!$.
- $(1\,2)$ is a 2-cycle. This gives 6!.

In total, this gives $5 \cdot 6!$ with $\sigma(\sigma(1)) = 1$ and $\sigma(\sigma(2)) = 2$, so the answer is

$$8! - 2 \cdot 7! - 2 \cdot 7! + 5 \cdot 6! = 23760.$$

9.6. Exercises in Biggs

```
Read 10.6, 12.4-12.6
10.6: 1-5
12.4: 1, 2
12.5: 1, 2
12.6: 1-3
12.7: 19
21.7: 18 (Note that there is a typo: \sigma should be \pi)
```

Lecture 10: Groups I

Definition 122 (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 $a * a' = a' * a = e$.

We usually write just ab instead of $a * b$. The group operator is usually referred to as **group multiplication** or simply multiplication.

Multiplication might not be commutative! If multiplication is commutative, the group is called **Abelian** or **commutative**.

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.

10.1. 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.
- $SL_n(\mathbb{R})$, the set of $n \times n$-matrices with determinant 1, under matrix multiplication.
- S_n, the set of permutations on $1, \ldots, n$ under composition (seen as bijections).
- Symmetries. (Can be seen as a subset of permutations.)

Definition 123 (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 has G itself and $\{e\}$ as subgroups. These are called *trivial* subgroups of G.

10.1.1. Discussion

Group or not? What is the identity element? Is the group commutative?

(a) The set of permutations in S_5.

(b) The set of even permutations in S_5.

(c) The set of odd permutations in S_5. *This is not a group!*

(d) All integer 2×2-matrices with determinant 1, under matrix multiplication.

(e) All integer 2×2-matrices with determinant ±1, under matrix multiplication.

(f) All complex numbers with absolute value 1 under multiplication.

10.2. Order of group elements

Let $g \in G$. The smallest $k \geq 1$ such that $g^k = e$ is the **order** of g. If we are in an infinite group, some elements might not have an order.

Question 124. Let $a \in G$ for some group. Show that a and a^{-1} have the same order.

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

10.3. Multiplication tables

Let $G \coloneqq \{1, -1, i, -i\} \subset \mathbb{C}$. We have that G is a group under multiplication. Write down the **multiplication table** and find the **order** of every element in G.

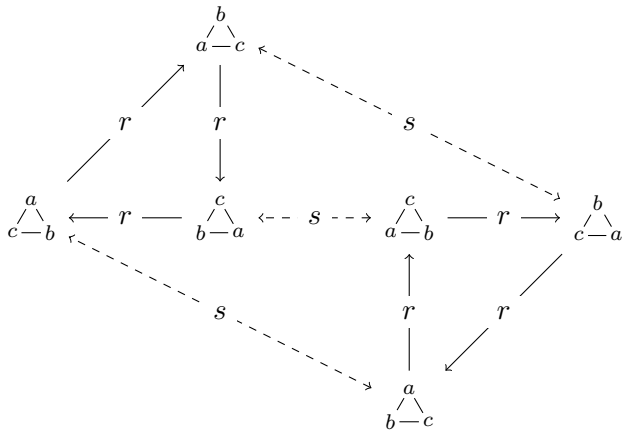
$*$	1	-1	i	$-i$
1	·	·	·	·
-1	·	·	·	·
i	·	·	·	·
$-i$	·	·	·	·

Question 125. Let $G_\triangle$ be the group of symmetries of an equilateral triangle. Show that

$$G_\triangle = \{e, s, r, r^2, sr, sr^2\},$$

where s is reflection in the y-axis, and r denotes rotation by 120°, and verify the relations $s^2 = r^3 = e$, $sr = r^2 s$ and $rs = sr^2$.

Solution. The relations can be illustrated in the following graph:



From this graph, we can deduce the following multiplication table for the group G:

$\circ$	**e**	**s**	**r**	$\mathbf{r^2}$	**sr**	$\mathbf{sr^2}$
e	e	s	r	r^2	sr	sr^2
s	s	e	sr	sr^2	r	r^2
r	r	sr^2	r^2	e	s	sr
$\mathbf{r^2}$	r^2	sr	e	r	sr^2	s
sr	sr	r^2	sr^2	s	e	r
$\mathbf{sr^2}$	sr^2	r	s	sr	r	e

In particular, the relations we are asked to verify are in this table.

Question 126. Write down all elements in $U(18)$ (that is, all invertible elements in $\mathbb{Z}_{18}$). This is a group under multiplication. Write down the multiplication table for this group.

Solution. We have $U(18) = \{1, 5, 7, 11, 13, 17\} = \{1, 5, 7, -7, -5, -1\}$. The multiplication table is

$\cdot$	**1**	**5**	**7**	**-7**	**-5**	**-1**
1	1	5	7	-7	-5	-1
5	5	7	-1	1	-7	-5
7	7	-1	-5	5	1	-7
-7	-7	1	5	-5	-1	7
-5	-5	-7	1	-1	7	5
-1	-1	-5	-7	7	5	1

We have that $\{5^0, 5^1, 5^2, 5^3, 5^4, 5^5\} = \{1, 5, 7, -1, -5, -7\}$ so the group is cyclic with 7 as a generator.

10.4. Group problems

Question 127. Let G be the set of bijections $f : \{-3, -2, -1, 1, 2, 3\}$ with the property that $f(-x) = -f(x)$ for all x. Compute $|G|$ and show that G is a group under function composition.

Solution. We first note that if we know $f(1)$, $f(2)$ and $f(3)$ then we also know $f(-1)$, $f(-2)$ and $f(-3)$. There are 6 choices for $f(1)$, then 4 choices for $f(2)$ and 2 choices for $f(3)$. We can express this as $|G| = 2^3 \cdot 3!$.

We know that the bijections on a set form a group, so it suffices to show that G contains the identity, and is closed under multiplication (composition) and taking inverses. The identity

element is the unique function with $f(x) = x$, and this lies in G. Suppose now that $f \in G$ and y is some element in $\{-3, -2, -1, 1, 2, 3\}$. There is then some x, such that $f(x) = y$, and $f(-x) = -y$. It follows that $f^{-1}(y) = x$ and $f^{-1}(-y) = -x$. Hence, the inverse also has the property that $-f^{-1}(y) = f^{-1}(-y)$.

Finally, suppose $f, g \in G$. Then by properties of f and g, we have

$$f(g(-x)) = f(-g(x)) = -f(g(x))$$

so the composition sends $-x$ to $-f(g(x))$ and we have shown that the set G is closed under composition.

Question 128. Let S_8 be the group of permutations on 8 elements. Find an Abelian subgroup of S_8 with 9 elements, and write down all its elements.

Solution. 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. The group is Abelian—the (123) and the (456)-cycles do not interact, and both (123) and (456) generate Abelian subgroups.

Question 129. Let G be an Abelian group. Fix some integer $k \geq 1$ and let $H_k \coloneqq \{g \in G : g^k = e\}$. Show that H_k is a subgroup of G.

Solution. It suffices to show that H_k is closed under taking inverses, and multiplication. Suppose $h \in H_k$. Then, $h^k = e$ and if we multiply both sides with $(h^{-1})^k$ we arrive at $e = (h^{-1})^k$. Hence, H_k is closed under taking inverses. Now, if $g, h \in H_k$ we have (by commutativity) that

$$(gh)^k = g^k h^k = e^2 = e$$

and the set H_k is also closed under multiplication. Hence, H_k is a subgroup of G.

Question 130. Suppose $G = \{g_1, \ldots, g_n\}$ is a finite Abelian group and let $c = g_1 g_2 \cdots g_n$. Prove that $g^2 = e$.

Solution. 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.

Question 131. Let G be the smallest subgroup of S_5 which contains the permutation $\pi = (1\ 2\ 3)(4\ 5)$. What is the order of π? What is the size of G? Is G Abelian?

Solution. The order of π is 6, and $|G| = 6$. Moreover, every element in G is of the form π^k, so G is Abelian.

Question 132. Let G be the smallest subgroup of S_5 which contains the permutation $\pi = (1\ 2\ 3)(4\ 5)$ and $\sigma = (12)$. Determine $|G|$. Is G Abelian?

Solution. The group has 12 elements and it is not Abelian; $(123) \circ (12) \neq (12) \circ (123)$.

10.5. Exercises in Biggs

Read 20.1-20.4
20.1: 1-2
20.2: 1-4
20.3: 1-5
20.4: 1-5

Lecture 11: Groups II

Definition 133 (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.

Theorem 134. *Every subgroup of a cyclic group is cyclic.*

Proof. Suppose G is a finite[1] cyclic group and let H be a subgroup. Then H is of the form

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

for some list of integers $L = \{a_1, \dots, a_k\}$. Since H is a subgroup it is closed under group operations. This means that L is closed under addition and subtraction, which implies that it is closed under linear combinations. In particular, we must have that $d = \gcd(a_1, a_2, \dots, a_k)$ 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. □

11.1. Lagrange's theorem

Theorem 135. *If H is a subgroup of the finite group G, then we have that $|H|$ divides $|G|$.*

Proof. It suffices to show that the existence of H allows us to partition G into k parts such that

(i) Every part has size $|H|$.

(ii) The parts do not overlap.

Hence, $|G| = k|H|$ and we are done.

First, for every element $g \in G$, consider its **left cosets** with respect to H:

$$gH \coloneqq \{gh : h \in H\}.$$

In other words, everything we can get from H by multiplying by g on the left. Note that $|gH| \leq |H|$ since we cannot create more than $|H|$ new elements by multiplying by g. But if $gh_1 = gh_2$ then $g_1 = g_2$ so we must in fact have $|gH| = |H|$. Hence, all cosets have the same size.

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

For the second part of the proof: Consider now $g_1, g_2 \in G$. Then either $g_1H = g_2H$ or $g_1H \cap g_2H = \emptyset$. Suppose $g_1H \cap g_2H$ is non-empty. This means that $g_1h_1 = g_2h_2$ for some $h_1, h_2 \in H$. But then

$$\begin{aligned} g_1h_1 = g_2h_2 &\implies \text{by "multiplying" both sides with } H \\ g_1h_1H = g_2h_2H &\implies \text{since } H \text{ is a group} \\ g_1H = g_2H & \end{aligned}$$

and we are done. What we have proved is that *different* (left) cosets are disjoint. □

Observe that Lagrange's theorem implies that every group that has a prime number of elements, must be cyclic. Every element which is not the identity must generate the full group, since otherwise we would get a subgroup whose size divides the size of the full group—impossible.

(a) Does S_5 have a subgroup of size 7? *No, impossible due to Lagrange.*

(b) Does S_5 have a subgroup of size 6? *Yes, permute only the first 3.*

(c) Does S_5 have a subgroup of size 60? *Yes, the even permutations.*

11.1.1. Direct product

Given two groups $(G, *_G)$ and $(H, *_H)$, we can create the new group (direct product) $G \times H$ where the elements are pairs $(g, h) \in G \times H$ and

$$(g_1, h_1) * (g_2, h_2) \coloneqq (g_1 *_G g_2, h_1 *_H h_2).$$

In the video, it was shown that $C_a \times C_b \cong C_{ab}$ if a and b are coprime. This generalizes to more than 2 cyclic groups.

11.2. Group homomorphisms

A **homomorphism** $\phi : G \to H$ is a map which respects the group structure. That is,

$$\phi(g_1g_2) = \phi(g_1)\phi(g_2) \text{ for all } g_1, g_2 \in G.$$

Note that ϕ does not be surjective or injective.

Lemma 136. *If $\phi : G \to H$ is a homomorphism, then $\phi(e) = e$ and $\phi(g^{-1}) = \phi(g)^{-1}$ for all $g \in G$.*

Proof. We have that

$$\phi(e) = \phi(e \cdot e) = \phi(e)\phi(e) \text{ as an identity in } H,$$

so by cancelling by $\phi(e)$ on both sides, $\phi(e) = e$. Now,

$$e = \phi(e) = \phi(g \cdot g^{-1}) = \phi(g)\phi(g^{-1})$$

so $\phi(g^{-1})$ is mapped to the inverse of $\phi(g)$ and we are done. □

A homomorphism which is also a bijection is called an **isomorphism**. If there is an isomorphism between G and H, we say that G and H are **isomorphic**, usually denoted $\cong$. Group isomorphism is an equivalence relation.

Example 137. The map $\mathrm{sgn} : \mathrm{S}_n \to \{-1, 1\}$ is a group homomorphism.

Question 138. Describe all group homomorphisms $\phi : \mathbb{Z} \to \mathbb{Z}$. Which of these are isomorphisms?

Solution. Since 1 generates $\mathbb{Z}$, it is enough to know $\phi(1)$, as this determines ϕ completely. For example, $\phi(3) = \phi(1+1+1) = \phi(1) + \phi(1) + \phi(1)$. In general, $\phi(m) = m \cdot \phi(1)$ whenever m is an integer. Thus, if $\phi(1) = a$ (where $a \in \mathbb{Z}$) the homomorphism must be of the form $\phi(x) = ax$. Also, every map of this form is a homomorphism.

Now, in order for the map to also be an isomorphism, it must be a bijection. This is only possible if $a = 1$ or $a = -1$, since the image of $\phi(x) = ax$ consists only of the numbers which are multiples of a.

Theorem 139 (Cayley's theorem)**.** *Let G be a group of size n. Then G is isomorphic with some subgroup of S_n.*

Proof. The multiplication table for G tells us how each element is supposed to permute the elements in G. From this, we can find permutations which does what we want. □

Question 140. Recall that $\mathbb{Z}$ is a group under addition and that $G = \mathbb{Z}^3$ is also a group. Show that $\phi : \mathbb{Z}^3 \to \mathbb{Z}$ defined via $\phi(x, y, z) = a - b + c$ is a homomorphism.

Question 141. If $\phi : G \to H$ is a group homomorphism, show that the set

$$\ker(\phi) \coloneqq \{g \in G : \phi(g) = e\}$$

is a subgroup of G.

Solution. We must show that $\ker(\phi)$ is closed under multiplication and taking inverses.

Suppose $g_1, g_2 \in \ker(\phi)$, so that $\phi(g_1) = \phi(g_2) = e$. But then

$$\phi(g_1 g_2) = \phi(g_1)\phi(g_2) = e \implies g_1 g_2 \in \ker(\phi).$$

Similarly,

$$\phi(g_1^{-1}) = \phi(g_1)^{-1} = e \implies g_1^{-1} \in \ker(\phi).$$

This shows that $\ker(\phi)$ is a subgroup of G.

Question 142. Let G and G' be groups and $\phi : G \to G'$ be a homomorphism. Show that if $g \in G$ has finite order, then $\mathrm{order}(g)$ is divisible by $\mathrm{order}(\phi(g))$.

Solution. Let $k = \mathrm{order}(g)$. We know that $g^k = e$, and since ϕ is a homomorphism, it follows that $\phi(g^k) = e$, so $\phi(g)^k = e$. But by Thm. 20.4 (Biggs) it now follows[2] that k is a multiple of the order of $\phi(g)$ and the conclusion follows.

Question 143. Let $n \geq 2$. Suppose that $\eta : \mathrm{S}_n \to \mathbb{Z}_3$ is a homomorphism. Show that η cannot be surjective.

Solution. Every permutation $\pi = \tau_1 \cdots \tau_k$ can be expressed as a product of transpositions. If $\eta(\tau_j) = 0$ for every transposition, then η is not surjective as it sends everything to 0. So assume $\eta(\tau) \neq 0$ for some transposition. But then $\eta(\tau^2) = \eta(\mathrm{id}) = 0$, so $\eta(\tau)^2 = 0$. In particular, $\eta(\tau)$ is an element of order 2. However, this is impossible as there is no element in $\mathbb{Z}_3$ with order 2. It follows that $\eta(\tau) = 0$ for all transpositions, and therefore for all permutations as well.

Question 144. Recall that $\mathbb{Z}_n = (\mathbb{Z}_n, +)$ is a cyclic group with n elements.

[2] If it was not, we could use Euclid's algorithm to produce a contradiction

(a) How many isomorphisms $\phi : \mathbb{Z}_7 \to \mathbb{Z}_7$ are there?

(b) How many isomorphisms $\phi : \mathbb{Z}_9 \times \mathbb{Z}_{14} \to \mathbb{Z}_9 \times \mathbb{Z}_{14}$ are there?

Solution. (a) An isomorphism between cyclic groups is uniquely determined by specifying what a generator must map to. There are 6 generators in $\mathbb{Z}_7$, so we have six choices for $\phi(1)$, each of these choices determines an isomorphism.

(b) Since 9 and 14 are relatively prime, if g generates $\mathbb{Z}_9$ and h generates $\mathbb{Z}_{14}$, then (g, h) generates $\mathbb{Z}_9 \times \mathbb{Z}_{14}$. Moreover, every generator of the direct product is of this form. The elements $\{1, 2, 4, 5, 7, 8\}$ generate $\mathbb{Z}_9$ and $\{1, 3, 5, 9, 11, 13\}$ generate $\mathbb{Z}_{14}$, so there are $6 \cdot 6 = 36$ pairs (g, h) which generate $\mathbb{Z}_9 \times \mathbb{Z}_{14}$. Hence, $\phi((1, 1))$ has 36 possible values so there are 36 isomorphisms.

11.3. Exercises in Biggs

```
Read  20.5-20.8
20.5: 1-2
20.6: 1-4
20.7: 1-3, 6
20.8: 1-4
20.10: 18 i)-ii)
22.2: 1
```

Lecture 12: Group actions

We have a **group action**[1] of G on a set X. This is defined so that $(gh)x = g(hx)$, for all $x \in X$ and $g, h \in G$, and $ex = x$ for all $x \in X$.

Example 145. The cyclic group C_n acts on words of length n (in some alphabet) by rotation.

12.1. Orbits, stabilizers and fixed points

$$\text{Orbit} \quad Gx \coloneqq \{g \cdot x : g \in G\}.$$

Everything reachable from x by some action in G.

$$\text{Stabilizer} \quad G_x \coloneqq \{g \in G : g \cdot x = x\}.$$

The elements in G which do not affect x. Note that G_x is a subgroup of G.

$$\text{Fixed-points} \quad \text{Fix}(g) \coloneqq \{x \in X : g \cdot x = x\}.$$

Elements in X which are unaffected by g.

Question 146. Let G be the *smallest permutation group* in S_5 containing $\sigma = (12)$ and $\tau = (345)$.

Let X be the subsets of $\{1, 2, \ldots, 5\}$ of size 2. We let $\pi \in G$ *act* on $\{a, b\} \in X$ via

$$\pi \cdot \{a, b\} = \{\pi(a), \pi(b)\}.$$

This defines a group action of G on X.

(a) Compute $|G|$ och $|X|$.

(b) Compute $\sigma \cdot \{1, 2\}$ and $\sigma \cdot \{2, 5\}$.

(c) Compute the orbits of $\{1, 2\}$ and $\{2, 5\}$.

(d) Compute the stabilizers of $\{1, 2\}$ and $\{2, 5\}$.

(e) Determine $\text{Fix}(\sigma)$.

Solution. (a) We have $|G| = 6$ and $|X| = \binom{5}{2} = 10$.

(b) They become $\{1, 2\}$ and $\{2, 5\}$.

(c) The orbits are $\{\{1, 2\}\}$ and

$$\{\{1, 3\}, \{1, 4\}, \{1, 5\}, \{2, 3\}, \{2, 4\}, \{2, 5\}\}.$$

[1] Swedish: gruppverkan

(d) The stabilizer of $\{1,2\}$ is the entire group, while the stabilizer of $\{2,5\}$ is just the identity permutation.

(e)
$$\mathrm{Fix}(\sigma) = \{\{1,2\},\{3,4\},\{3,5\},\{4,5\}\}.$$

Question 147. Let S_n act on some set X. Show that if σ and π have the same type, then $|\mathrm{Fix}(\sigma)| = |\mathrm{Fix}(\pi)|$.

Solution. Since the permutations have the same type, there is some τ such that $\pi = \tau^{-1}\sigma\tau$. Now,
$$\mathrm{Fix}(\pi) = \{x \in X : \pi x = x\} = \{x \in X : \tau^{-1}\sigma\tau x = x\}.$$
We can now multiply both sides in the identity with τ, and get
$$\mathrm{Fix}(\pi) = \{x \in X : \sigma(\tau x) = (\tau x)\}.$$
We have that $\tau : X \to X$ is a bijection (it has an inverse), so
$$|\mathrm{Fix}(\pi)| = |\{(\tau x) \in X : \sigma(\tau x) = (\tau x)\}|.$$
Letting $y = (\tau x)$, we then have that
$$|\mathrm{Fix}(\pi)| = |\{y \in X : \sigma y = y\}| = |\mathrm{Fix}(\sigma)|,$$
and we are done.

Question 148. Let G be a finite group acting on the set X. Assume that $g \in G$ and $k \in \mathbb{N}$.

(a) Show that $\mathrm{Fix}(g) = \mathrm{Fix}(g^{-1})$

(b) Show that $\mathrm{Fix}(g) \subseteq \mathrm{Fix}(g^k)$.

(c) Show that $\mathrm{Fix}(g) = \mathrm{Fix}(g^k)$ if g and g^k have the same order.

Solution. (a) We have
$$x \in \mathrm{Fix}(g) \iff gx = x \iff g^{-1}gx = g^{-1}x \iff x = g^{-1}x \iff x \in \mathrm{Fix}(g^{-1}).$$

(b) We have
$$g \in \mathrm{Fix}(g) \implies gx = x \implies g^k x = x \implies g^k \in \mathrm{Fix}(g).$$

(c) Suppose that g has order n so that g generates a cyclic subgroup $C \subseteq G$ of order n. Since g and g^k have the same order, we must have that g^k also generates C. This implies that there is some m, such that $(g^k)^m = g$.

Moreover, $x \in \mathrm{Fix}(g^k) \iff g^k x = x$, so $(g^k)^m x = x$ since multiplication with g^k on x fixes x. But then we have that $g^{km}x = x$, so $gx = x$, because $(g^k)^m = g$. Therefore, $x \in \mathrm{Fix}(g)$ and we are done.

12.2. Burnside's lemma

Proposition 149 (Orbit-stabilizer theorem, Thm. 21.3 Biggs)**.** *Let G act on X. Then for any $x \in X$, we have $|Gx| \cdot |G_x| = |G|$*

Proof. First note that G_x is a subgroup of G.

Let us define the map $f : G \to X$ via $g \mapsto gx$. The image of f is Gx. Suppose now $f(g) = f(h)$. This means that $gx = hx$, so $h^{-1}gx = x$. That is, $h^{-1}g \in G_x$, so $g \in hG_x$. But this is the same as saying that g and h are in the same coset of G_x. All cosets of a subgroup have the same size as the subgroup.

Thus, for every element in Gx, there are $|G_x|$ elements mapped there under f. □

Proposition 150 (Burnside's lemma)**.** *We have that*

$$\frac{1}{|G|} \sum_{g \in G} |\operatorname{Fix}(g)|$$

is the number of orbits.

Proof. We first note that $\sum_{g \in G} |\operatorname{Fix}(g)| = \sum_{x \in X} |G_x|$, since both sides count pairs $\{(g, x) \in G \times X : gx = x\}$. Now

$$\sum_{x \in X} |G_x| = \{\text{by Orbit-stabilizer}\} = \sum_{x \in X} \frac{|G|}{|Gx|} = |G| \sum_{x \in X} \frac{1}{|Gx|}.$$

Now, we can partition X into t disjoint orbits:

$$\sum_{x \in X} \frac{1}{|Gx|} = \sum_{t} \sum_{x \in O_t} \frac{1}{|Gx|} = t,$$

since the inner sum is always 1 (because $|Gx|$ is the number of elements in O_t).

Putting it all together,

$$\sum_{g \in G} |\operatorname{Fix}(g)| = |G| \cdot t,$$

and solving for t gives the desired result. □

Question 151. We want the group $\mathbb{Z}_3$ to act on X where $X = \{x_1, x_2, \ldots, x_8\}$. In how many ways can we create such a group action?

Solution. Since $\mathbb{Z}_3$ is a cyclic group, it is enough to know what one of its generators, g, does to every element in X. Each orbit in X must be of size 1 or size 3 due to the Orbit–Stabilizer theorem. Observe that to determine a group action we also must say exactly how each element in X is mapped to another element. We have three cases to consider.

- All orbits have size 1. This means every element is fixed by g so no choice here.
- We have one orbit of size 3 and 5 singleton orbits. There are $\binom{8}{3}$ ways to choose the elements in the orbit and 2! ways to pick the order inside the orbit. For example, for the three elements $\{a, b, c\}$ we must choose say $g(a) = b$ or $g(a) = c$.
- We have two orbits of size 3 and 2 singleton orbits. We have there are then $\frac{1}{4}\binom{8}{3,3,1,1}$ ways to distribute the elements among the orbits and $(2!)^2$ ways to pick the exact order of elements within each orbit.

The total number of group actions is therefore

$$1 + 2!\binom{8}{3} + \frac{(2!)^2}{4}\binom{8}{3,3,1,1} = 1233.$$

Question 152. We let the cyclic group $\mathbb{Z}_6$ act on binary words of length 6 by shifting the entries to the left. That is, for $a \in \mathbb{Z}_6$, we let

$$a \cdot b_0 b_1 \dots b_5 = b_{0+a} b_{1+a} \dots b_{5+a}.$$

For example,

$$2 \cdot \texttt{110010} = \texttt{001011}.$$

Use Burnside's lemma to compute the number of orbits.

Solution. We compute the number of fixed-points for each shift:

g	$Fix(g)$
1	2
2	4
3	8

g	$Fix(g)$
4	4
5	2
0	2^6

For example, if a binary word $(b_0, b_1, b_2, b_3, b_4, b_5)$ is fixed under a three-step shift, then the word is completely determined by the values of b_0, b_1 and b_2, so there are $2^3 = 8$ possible words.

Burnside's lemma now tells us that the number of orbits is $\frac{1}{6}(2 + 4 + 8 + 4 + 2 + 64) = 14$.

Question 153. *MM5013, 2021-01-05.* Fix an equilateral triangle and let X be the set of figures obtained by by writing a number from $\{1, 2, 3, 4\}$ on each vertex. Let the group $G = \{e, r, r^2, s, sr, sr^2\}$ act on X, where denotes r rotation of the triangle 120° and s swaps all 1s to 2s and vice versa. For example

$$r \cdot \begin{smallmatrix} & 4 & \\ / & & \backslash \\ 1 & - & 2 \end{smallmatrix} = \begin{smallmatrix} & 2 & \\ / & & \backslash \\ 4 & - & 1 \end{smallmatrix} \qquad \text{and} \qquad s \cdot \begin{smallmatrix} & 4 & \\ / & & \backslash \\ 1 & - & 2 \end{smallmatrix} = \begin{smallmatrix} & 4 & \\ / & & \backslash \\ 2 & - & 1 \end{smallmatrix}.$$

1. Determine the orbit of $\begin{smallmatrix} & 4 & \\ / & & \backslash \\ 1 & - & 2 \end{smallmatrix}$ under G.
2. Determine the number of fixed-points of rs.
3. Determine the number of orbits, when G acts on X.

Solution. The orbit consists of the six triangles

$$\begin{smallmatrix} & 4 & \\ / & & \backslash \\ 1 & - & 2 \end{smallmatrix}, \quad \begin{smallmatrix} & 1 & \\ / & & \backslash \\ 2 & - & 4 \end{smallmatrix}, \quad \begin{smallmatrix} & 2 & \\ / & & \backslash \\ 4 & - & 1 \end{smallmatrix}, \quad \begin{smallmatrix} & 4 & \\ / & & \backslash \\ 2 & - & 1 \end{smallmatrix}, \quad \begin{smallmatrix} & 2 & \\ / & & \backslash \\ 1 & - & 4 \end{smallmatrix}, \quad \begin{smallmatrix} & 1 & \\ / & & \backslash \\ 4 & - & 2 \end{smallmatrix}$$

If a triangle is fixed under rs, we must have that it has either no 1s or 2s, or exactly one of each. However, in the latter case, the third digit is rotated, so the triangle cannot be fixed. Hence, the only possible fixed-points are $\begin{smallmatrix} & 3 & \\ / & & \backslash \\ 3 & - & 3 \end{smallmatrix}$ and $\begin{smallmatrix} & 4 & \\ / & & \backslash \\ 4 & - & 4 \end{smallmatrix}$.

To compute the number of orbits, we use Burnside's lemma and first compute the number of fixed points for every element in G. Remember that we have proved that g and g^{-1} always have the same number of fixed points.

- Number of fixed points for e: $4^3 = 64$.
- Number of fixed points for r and r^2: 4, every vertex has the same value.

- Number of fixed points for s: 2^3, every vertex has value 3 or 4.
- Number of fixed points for sr and sr^2: 2, every vertex has value 3 or 4, and they are all the same.

Burnside's lemma now tells us that the number of orbits is

$$\frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}(g)| = \frac{1}{6}\left(64 + 2\cdot 4 + 8 + 2\cdot 2\right) = 14.$$

Question 154. *From final MM5013, 2022-08-11.* Let X be the set of words of length 6 using the letters $\{\mathtt{x},\mathtt{y},\mathtt{z}\}$, and *For example,* $\mathtt{xyzzyz} \in X$ *but* $\mathtt{xyyyyy} \notin X$. every letter must appear at least once.

The group $\mathbb{Z}_6$ acts on X where $k \in \mathbb{Z}_6$ cyclically rotates k steps to the left. For example

$$2 \cdot \mathtt{xyzzyz} = \mathtt{zzyzxy}.$$

(a) Show that $|X| = 3! \cdot S(6,3)$, where $S(6,3) = 90$ is a Stirling number.

(b) Give an example of an element in X fixed by $3 \in \mathbb{Z}_6$.

(c) Determine the number of orbits in X under the group action.

Solution. (a) A valid word $(w_1,\ldots,w_6) \in X$ can be interpreted as a surjection from $1,2,\ldots,6$ to the set $\{\mathtt{x},\mathtt{y},\mathtt{z}\}$. Thus the number of words is $3! \cdot S(6,3)$.

(b) The word $\mathtt{xyzxyz}$ is fixed by 3 since we get the same word after shifting it 3 steps to the left.

(c) We use Burnside's lemma. No word is fixed by 1 or 5, since then $w_1 = w_2 = \cdots = w_6$ but then it does not contain all three letters. Similarly, if it was fixed by 2 or 4, then $w_1 = w_3 = w_5$ and $w_2 = w_4 = w_6$ and at least one letter is missing. A word fixed by 3 is uniquely determined by w_1, w_2, w_3, and these must be a permutation of $\{\mathtt{x},\mathtt{y},\mathtt{z}\}$. There are therefore 3! fixed points. Burnside's lemma then tells us that the number of orbits is

$$\tfrac{1}{6}\left(3! \cdot S(6,3) + 3!\right) = S(6,3) + 1 = 91.$$

Question 155. 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.

(a) Show that $G \cong \mathrm{S}_3 \times \mathrm{S}_2$.

(b) Find how many orbits there are of X under G.

Solution. Any element in G, can be described as a pair (π,σ), where $\pi \in \mathrm{S}_3$ permutes the columns, and $\sigma \in \mathrm{S}_2$ tells us which of the two rows is considered the top row. These two operations are independent—they commute—and this is then enough to conclude that $G \cong \mathrm{S}_3 \times \mathrm{S}_2$.

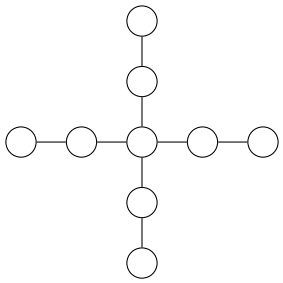
If $(g,h) \in \mathrm{S}_3 \times \mathrm{S}_2$ act on X, the number of fixed-points only depend on the type of g, and type of h, respectively.

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

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

Question 156. Let Γ be the graph on 9 vertices shown here. Let X be the set of colorings of the vertices of Γ using the colors $\{\texttt{white},\texttt{gray},\texttt{black}\}$, and where neighbors always receive different colors.



(a) Determine the number of colorings in X.

(b) The group $G=\{e,r,r^2,r^3\}$ acts on X where r rotates the figure 90° counterclockwise. Compute the number of orbits as G acts on X.

Solution. (a) The color in the middle can be chosen in 3 different ways. From there, we successively color the remaining vertices starting from the middle. This gives 2^8 choices in total, as each subsequent vertex has a neighbor where a color is already used. The total number of colorings is therefore $3\cdot 2^8$.

(b) Using Burnside's lemma, we need the number of fixed points for every element in G.

e: From (a), we have $3\cdot 2^8$ colorings.

r: Coloring the middle and one arm, determines everything. Thus, $3\cdot 2^2$.

r^2: Color the middle and two adjacent arms. This gives $3\cdot 2^4$.

r^3: Same as r, giving $3\cdot 2^2$.

Burnside then gives that the total number of orbits is

$$\frac{1}{4}\left(3\cdot 256+3\cdot 4+3\cdot 16+3\cdot 4\right)=210.$$

Question 157. Let X be the set of 2×2-matrices with rational entries. Let G be the set of *invertible* 2×2-matrices with rational entries (under multiplication). The group G acts on X by matrix multiplication on the left Which two of the three matrices

$$\begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in X$$

belongs to the same orbit under G?

12.3. Exercises in Biggs

```
Read 21.1-21.4
21.1: 1-4
21.2: 1, 2, 5, 6
21.3: 1, 2
21.4: 1, 2, 5
```

Lecture 13: Linear codes

We have a few new concepts from the videos.

Definition 158. A **code** is a subset $C \subseteq \mathbb{Z}_2^n$. We say that the code is **linear** if the set is closed under addition (that is, it is a group under addition). The **length** of a code is the value of n. By Lagrange's theorem, a linear code can only contain 2^k code words, for some k. This value of k is the **dimension** of the code.

The distance between two codewords is the number of bits where the words differ. The **minimum distance** of a code, is the minimum of all possible distances between code words. For linear codes, the minimum distance is the minimum number of ones one have in a non-zero code word.

A code can be constructed using a **check matrix** H. We let C be all solutions (in $\mathbb{Z}_2^n$) to the equation $H\mathbf{a} = 0$.

Question 159. Let

$$C = \{\texttt{000000}, \texttt{111000}, \texttt{000111}, \texttt{111111}\}.$$

(a) What is the distance between `00110` and `10101`?

(b) What is the minimal distance δ for C?

(c) How many errors can C *detect*?

(d) How many errors can C *correct*?

(e) Is C linear?

Solution. The distance δ is 3. The minimal distance is 3. Thus, it can detect $\delta - 1 = 2$ errors and correct one.

Question 160. Find the dimension and the code words associated with the check-matrix

$$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \end{bmatrix}.$$

Solution. We want to find all binary words which are mapped to 0. Gaussian elimination gives

$$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

Setting x_3 and x_4 as parameters, we have that $x_1 = x_3 + x_4$ and $x_2 = x_3 + x_4$. The **dimension** of the code is 2 since there are two parameters, and thus 2^2 code words. The actual code words are $\{\texttt{0000}, \texttt{1101}, \texttt{1110}, \texttt{0011}\}$.

13.1. Correcting errors

Theorem 161 (Biggs, 24.4)**.** *If H is a check matrix with no* 0 *column and no two columns equal, then it can correct one error.*

Proof. It is enough to show that the minimum distance is at least 3. So it is enough to show that there is no code word with only one or two bits equal to 1.

If we have only one bit in $\mathbf{a}$, then $H\mathbf{a}$ equals one of the columns in H so it cannot be the zero vector. If we have two bits set to 1 in $\mathbf{a}$, then $H\mathbf{a}$ is the sum of two of the columns in H. Again, this is non-zero due to the restrictions on H. □

Question 162. Let H below define a linear code. All columns are different and there is no column with only 0s. This implies that $\delta \geq 3$ for the associated code.

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$

Correct the single error in $\mathbf{b} = \texttt{11110}$.

Solution. Matrix multiplication gives

$$\begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$$

This is equal to the 4th column, so the 4th bit is wrong in $\mathbf{b}$.

13.2. Some theory questions

Question 163. If C_1 and C_2 are linear codes in $\mathbb{Z}_2^n$, is it true that $C_1 \cap C_2$ is also a linear code?

If H_1 is the check matrix for C_1 and H_2 is the check matrix for C_2, how can one create the check matrix for $C_1 \cap C_2$?

Solution. The answer is yes, intersection of subgroups is again a subgroup.

The two matrices have the n columns, which is the length of the code words. We can then simply take all rows in both matrices, to get a matrix for the intersection of the codes.

Question 164. Let $C_1 \subseteq \mathbb{Z}_2^3$ and $C_2 \subseteq \mathbb{Z}_2^5$ be linear codes. We construct a new code in $\mathbb{Z}_2^8$ via

$$C_3 \coloneqq \{(c_1, c_2) : c_1 \in C_1, \quad c_2 \in C_2\}.$$

For example, if $\texttt{101} \in C_1$ and $\texttt{11011} \in C_2$ then $\texttt{101 11011} \in C_3$.

(a) What is the dimension of C_3 expressed in terms of the dimensions of C_1 and C_2?

(b) If δ_1 is the minimum distance for C_1 and δ_2 is the minimum distance for C_2, what is the minimum distance for C_3?

(c) How can we create a check matrix for C_3?

Solution. (a) Note that if C_1 has 2^{k_1} code words and if C_2 has 2^{k_2} then C_3 has $2^{k_1} \cdot 2^{k_2} = 2^{k_1+k_2}$ code words. Hence, the dimensions are added.

(b) We get that $\delta_3 = \min(\delta_1, \delta_2)$. This is since we can take the first 3 bits to be 0 and the last 5 to be in C_2, or the first three bits in C_1 and the last five set to 0, and get a code-word close to the zero vector.

(c) Let H_1 and H_2 be the check matrices and they have 3 and 5 columns respectively. We then form the block matrix $\left[\begin{smallmatrix} H_1 & 0 \\ 0 & H_2 \end{smallmatrix}\right]$ with $3 + 5 = 8$ columns and this will be a check matrix for C_3.

Question 165. Find a check matrix such that the code it defines contains the words `1001` and `1100` but not `0110` and `1101`.

Solution. Let (a, b, c, d) be a row in the check matrix. We must have that $a + d = 0$ and $a + b = 0$ (in $\mathbb{Z}_2$), otherwise the first two code words are not in the code. But this is the same as $a = b = d$. We can then take one of the matrices

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad \text{or simply} \quad H' = \begin{bmatrix} 1 & 1 & 0 & 1 \end{bmatrix}$$

as a matrix for our linear code.

13.3. Exercises in Biggs

```
Read 24.1-24.4
24.1: 1, 2, 3
24.2: 1, 2, 3
24.3: 1, 2
24.4: 1, 2
```

Lecture 14: Graphs

Definition 166. We first have an overview of definitions.

- A graph is **r-regular** if every vertex has degree r.
- A **walk** (Sv. promenad) is a sequence of vertices $v_1, \ldots, v_n$ such that adjacent vertices are connected by an edge.
- A path is a walk where each vertex is visited only once.
- The **complete graph** K_n is the graph on n vertices where every pair of vertices is an edge.
- A graph is **bipartite** if we can partition the vertices into two sets, A and B such that edges are only between the two sets.
- A graph is **connected** if there is a path between any pair of vertices.
- A **cycle** is a path where the first and last vertex is connected by an edge.
- A **tree** is a connected graph without cycles.
- A **Hamilton path/cycle** is a path/cycle visiting every vertex in the graph exactly once.
- An **Euler walk/circuit** (Sv. promenad/krets) is a walk/circuit which uses every edge in the graph exactly once.
- Two graphs are **isomorphic** if there is a bijection between the vertices which sends edges to edges.
- A **proper graph coloring** of a graph is an assignment of colors to the vertices such that no two adjacent vertices have the same color.
- The **chromatic number** of a graph is the smallest number of colors needed in order to construct a proper graph coloring.

Theorem 167. *For any graph $G = (V, E)$ we have $\sum_{v \in V} \deg(v) = 2|E|$.*

14.1. Euler circuits

Theorem 168. *A connected graph has an Euler circuit if and only if the degree of each vertex is even.*

Proof. If we have an odd degree vertex, starting there will not allow us to end there, so all vertices must have even degree. We now show this is also sufficient.

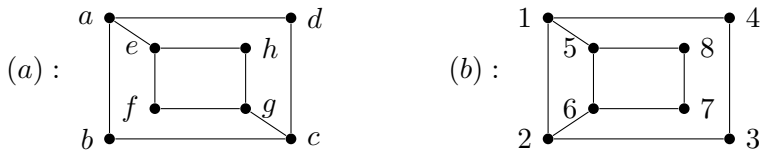
We prove this by induction on the number of edges. Base case is no edges, and here we have nothing to prove. We start at a vertex, and keep going until we have found a cycle (this will happen). Remove all these edges (all degrees are now still even). In each connected component, we can (by induction hypothesis) assume there is an Euler cycle.

So, we have one main cycle, and zero or more other cycles sharing vertices with the main cycle. But, we can then merge the main cycle with an auxiliary cycle, and in the end have one huge Euler cycle. □

(For the path statement, just add and remove the appropriate edge).

14.2. Graph isomorphism

Question 169. Are the following graphs isomorphic?



Solution. No, $1-5-6-2$ form a path in (b) where the degree of every vertex is 3, but such path does not exist in (a).

Question 170. Let G be a bipartite graph with an odd number of vertices. Show that G does not have a Hamiltonian cycle.

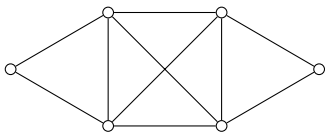
Solution. If G is bipartite, we can partition the vertices into two sets, say red and blue, such that every edge is between vertices of different colors. Every cycle in G must then have an even number of vertices, since the colors of the vertices must alternate. In particular, there cannot be a cycle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

Question 171. Solve the following problems.

(a) Draw a graph with chromatic number 4, and with the property that it has both an Euler circuit and a Hamilton cycle.

(b) Prove that a graph having exactly one cycle, has chromatic number at most 3.

Solution. (a) The graph



has four corners in the middle, which are all mutually connected, so the chromatic number is at least 4. It is then easy to see that 4 colors also suffices.

We can visit all corners by walking along the outer edge, so there is a Hamilton cycle. Finally, since the graph is connected and every vertex has even degree, it follows that it also has an Euler circuit.

(b) The graph has a cycle, so we start by coloring those vertices. Three colors suffices—we color one of the vertices blue, ant the remaining vertices on the cycle are colored white and black in an alternating fashion.

The remaining graph, which does not contain any more cycles, must consist of trees (which may or may not be connected to the cycle). Each such tree can be colored with two colors, and we may ensure that those two colors are different from the vertex where the tree connects to the cycle (if it does).

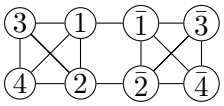
Question 172. Let G_n be the graph with vertex set $\{-n, -(n-1), \ldots, -1, 1, 2, 3, \ldots, n-1, n\}$, with $n \geq 2$. The edges of G are as follows: Every negative vertex has an edge with all other negative vertices. Every positive vertex has an edge with all other positive vertices. Finally, we also have the edges $\{-1, 1\}$ and $\{-2, 2\}$.

(a) Draw G_4.

(b) For what n does G_n have an Eulerian trail[1]?

(c) Show that G_n has a Hamiltonian cycle.

Solution. (a) G_4 is the following graph:



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

Question 173. Let $\Gamma = (V, E)$ be the graph where each vertex is a vectors (a, b, c) where $a, b, c \in \{0, 1, 2\}$. Two vectors (vertices) are connected by an edge if and only if the Euclidean distance between them is 1. Prove that Γ does not have a Hamiltonian cycle. Furthermore, prove that there is no Hamiltonian path starting at $(0, 0, 0)$ and ending at $(1, 1, 1)$.

Solution. We see that there are $3^3 = 27$ vertices in Γ. Let us now color each vertex black, if the sum of the entries is even, and white if the sum is odd. We then note that every edge connects vertices of different colors (we have an edge between v and w only if exactly one coordinate is different, and this difference is 1).

Thus, in a Hamiltonian cycle, the colors must alternate along the cycle. But this is not possible since the number of black vertices is 14, and the number of white vertices is 13. The best we can hope for is a Hamiltonian path, where the first and last vertex is colored black.

For the second question, the answer is therefore also negative, the vertex $(1, 1, 1)$ is white.

[1]May start and end in the same vertex

Question 174. Let[2] $G = (V, E)$ be the graph, where vertices are subsets of $\{1, 2, \ldots, 50\}$ of size 7. Two vertices are connected if they are disjoint. Show that the chromatic number for G is more than 7.

Solution. Suppose that it is possible to color the graph with 7 colors. We consider the subsets

$$\{1, \ldots, 7\},\ \{8, \ldots, 14\},\ \ldots\ \{42, \ldots, 49\}. \tag{14.1}$$

Since all these are disjoint, we must use 7 different colors to color these vertices; say colors $1, 2, \ldots, 7$. We now replace the largest number in each set with 50:

$$\{1, \ldots, 6, 50\},\ \{8, \ldots, 13, 50\},\ \ldots\ \{42, \ldots, 48, 50\}. \tag{14.2}$$

Now, the first set in (14.2) is disjoint from all but the first set in (14.1). With this argument, we can show that the kth set in (14.2) must have color k.

Now consider the set $\{7, 14, 21, \ldots, 49\}$. This is disjoint from all seven sets in (14.2), but all colors are already taken. Hence, $\chi(G) > 7$.

Question 175. A graph[3] $\Gamma = (V, E)$ is defined as follows. We have $V = \{S : S \subseteq \{1, 2, \ldots, 8\}\}$, i.e., the vertices are all possible subsets of $\{1, 2, \ldots, 8\}$. Two vertices S_1, S_2 are joined by an edge if S_1 can be obtained from S_2 by adding or removing exactly one number. For example, $\{1, 2, 5, 7\}$ and $\{1, 2, \mathbf{4}, 5, 7\}$ are joined by an edge.

(a) Find all neighbors of $\{1, 2, 5, 7\}$.

(b) Show that Γ has an Euler cycle.

(c) Show that there is no Hamiltonian path starting in $\emptyset$ and ending in $\{1, 2, 3, 4, 5, 6, 7, 8\}$.

Solution. (a) The neighbors are $\{2, 5, 7\}$, $\{1, 5, 7\}$, $\{1, 2, 3, 5, 7\}$, $\{1, 2, 4, 5, 7\}$, $\{1, 2, 7\}$, $\{1, 2, 5, 6, 7\}$, $\{1, 2, 5\}$ and $\{1, 2, 5, 7, 8\}$.

(b) We can reach all vertices from $\emptyset$ by successively adding numbers. This shows that Γ is connected. Moreover, for any vertex S, there are exactly 8 neighbors since every member of $\{1, 2, \ldots, 8\}$ can either be added or removed from S in order to create a neighbor of S Since the degree of every vertex is even and the graph is connected, the graph must have an Euler cycle.

(c) If S_1 and S_2 are neighbors, then the size of S_1 and S_2 must differ by exactly 1. This shows that Γ is bipartite, where the vertices of odd size are only connected with vertices of even size. Since the graph has $2^8 = 256$ vertices, there can only be a Hamiltonian path between vertices of different parity of the sizes. But both $\emptyset$ and $\{1, 2, 3, 4, 5, 6, 7, 8\}$ have even sizes, so we cannot find a Hamiltonian path between these.

14.3. Exercises in Biggs

```
Read Chapter 15
15.1. 1-3
15.2. 1, 2
15.3. 1
```

[2] HMT final, 2022-03-26, Swedish national middle-school math competition. The original problem was not described in this technical manner, but had a much longer and convoluted description.

[3] MM5013, 2022-08-11 (only a and b)

15.4. 1, 4
15.5. 1, 2
15.6. 2, 3
15.8. 1

Lecture 15: Review

15.1. Overview

- Modular arithmetic,
- Euler's formula, $a^{\phi(n)} = 1$ in $\mathbb{Z}_n$, if $\gcd(a, n) = 1$.
- RSA
- Rings
- Fields, factorization, irreducible polynomials.
- Combinatorics, binomial, multinomial, Stirlingnumbers, ordered, unordered, inclusion-exclusion, mailbox.
- Equivalence relations (can be counted with Burnside's lemma sometimes).
- Permutations (sign, type, composition, inverse, order)
- Groups, multiplication table, Lagrange, isomorphisms, direct product
- Group action, Burnside's lemma
- Linear codes
- Graphs, degree, chromatic number, Eulerian circuit, Hamiltonian cycle.

15.2. Mixed questions

Question 176. Solve the system of equations

$$\begin{cases} x + 3y & = 2 \\ 5x + 13y & = 4 \end{cases}$$

in $\mathbb{Z}_{32}$.

Question 177. How many solutions are there to $x_1 + x_2 + x_3 \leq 10$, with all $x_i \geq 0$?

Question 178. How many non-negative integer solutions are there to the equation $(x_1 + x_2 + x_3)(y_1 + y_2 + y_3) = 15$?

Solution. Note that $15 = 3 \cdot 5$ so we have several cases to consider.

- $(x_1 + x_2 + x_3) = 1$ and $(y_1 + y_2 + y_3) = 15$,

- $(x_1 + x_2 + x_3) = 15$ and $(y_1 + y_2 + y_3) = 1$,
- $(x_1 + x_2 + x_3) = 3$ and $(y_1 + y_2 + y_3) = 5$,
- $(x_1 + x_2 + x_3) = 5$ and $(y_1 + y_2 + y_3) = 3$.

The first two cases give $3 \cdot \binom{15+2}{2}$ solutions each, while the last two cases give $\binom{3+2}{2} \cdot \binom{5+2}{2}$ each. Hence, the answer is

$$2 \cdot 3\binom{15+2}{2} + 2\binom{3+2}{2} \cdot \binom{5+2}{2} = 1236.$$

Question 179. Show that if $1 \leq k \leq n$, then $k\binom{n}{k} = n\binom{n-1}{k-1}$. Use either a combinatorial argument, or algebraic manipulation.

Question 180. Can $f(x) = x^{22} + 5x^{17} + ax^{12} + 8x^5 + 2$ be irreducible for all values of a, when considered as a polynomial in $\mathbb{Z}_{19}[x]$?

Solution. We have that $f(1) = 1 + 5 + a + 8 + 2 = 16 + a$. So, if we choose $a = 5$, we have that $f(1) = 0$, making it reducible.

Question 181. Suppose $f(x) \in K[x]$ is given by $f(x) = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0$ is palindromic, in the sense that $a_j = a_{k-j}$ for all $0 \leq j \leq k$. Prove that if $f(\alpha) = 0$ then $f(\alpha^{-1}) = 0$ also.

Solution. First note that f cannot have 0 as a root, since $a_0 = a_k \neq 0$. We now see that

$$\alpha^k f(\alpha^{-1}) = a_k + a_{k-1}\alpha + a_{k-2}\alpha^2 + a_1\alpha^{k-1} + a_0\alpha^k = f(\alpha)$$

where we in the last step used the fact that f is palindromic. Hence, $f(\alpha^{-1}) = 0$ if $f(\alpha) = 0$.

Question 182. Determine the inverse and order of the permutation $(1\ 5\ 2)(3\ 7\ 4)(6\ 8)$.

Question 183. Give an example of a non-commutative group G, and present two elements, $a, b \in G$ such that $ab \neq ba$.

Question 184. Write down all elements in $U(18)$ (that is, all invertible elements in $\mathbb{Z}_{18}$). This is a group under multiplication. Write down the multiplication table for this group, and determine if it is cyclic. If it is cyclic, describe an isomorphism from $U(18)$ to $(\mathbb{Z}_k, +)$ for an appropriate choice of k.

Solution. We have $U(18) = \{1, 5, 7, 11, 13, 17\} = \{1, 5, 7, -7, -5, -1\}$. The multiplication table is

·	**1**	**5**	**7**	**-7**	**-5**	**-1**
1	1	5	7	-7	-5	-1
5	5	7	-1	1	-7	-5
7	7	-1	-5	5	1	-7
-7	-7	1	5	-5	-1	7
-5	-5	-7	1	-1	7	5
-1	-1	-5	-7	7	5	1

We have that

$$\{5^0, 5^1, 5^2, 5^3, 5^4, 5^5\} = \{1, 5, 7, -1, -5, -7\}$$

so the group is cyclic with 7 as a generator. Hence, it must be isomorphic with $\mathbb{Z}_6$. An isomorphism must send generators to generators, so a possible isomorphism is then determined by having $\phi(5) = 1$, so that

$$\phi(1) = 0,\ \phi(5) = 1,\ \phi(7) = 2,\ \phi(-1) = 3,\ \phi(-5) = 4,\ \phi(-7) = 5.$$

15.2.1. Inclusion–exclusion

Question 185. Consider the integer equation

$$x_1 + x_2 + x_3 + x_4 + x_5 = 8, \qquad x_1, \dots x_5 \geq 0.$$

(a) Compute the total number of solutions to the equation.

(b) How many of these have that $x_1 + x_2 + x_3 = 6$?

(c) Compute the number of solutions satisfying the three conditions

$$x_1 + x_2 + x_3 \neq 6, \quad x_2 + x_3 + x_4 \neq 6, \quad x_3 + x_4 + x_5 \neq 6.$$

Solution. (a) We use stars and bars with 8 stars and 4 bars, so $\binom{8+4}{4}$ is the number of solutions.

(b) There are $\binom{6+2}{2} = 28$ ways for $x_1 + x_2 + x_3$ to be equal to 6, and there are 3 solutions to $x_4 + x_5 = 2$. Thus, we have $28 \cdot 3 = 84$ solutions in total.

(c) We do inclusion-exclusion and let A_k (for $k = 1, 2, 3$) be the sets of solutions where $x_k + x_{k+1} + x_{k+2} = 6$. As we saw in (b), we have that $|A_1| = |A_2| = |A_3| = 84$. We must now consider the intersections of these sets

- $|A_1 \cap A_2|$. We must here have $x_1 + x_2 + x_3 = 6$, $x_4 = x_1$ as well as $x_4 + x_5 = 2$. There are then three sub-cases $x_4 = 0, 1, 2$. Every such number determines x_5 and x_1. For each such case, we can choose $x_2 + x_3 = 6 - x_1$ in 7, 6 and 5 ways, respectively, so there are 18 solutions in total.
- $|A_2 \cap A_3|$, same as $|A_1 \cap A_2|$ by symmetry.
- $|A_1 \cap A_3|$. We now have $x_1 + x_2 + x_3 = 6$ and $x_3 + x_4 + x_5 = 6$. The first equation forces $x_4 + x_5 = 2$, so $x_3 = 4$. This leads to $x_1 + x_2 = 2$ and $x_4 + x_5 = 2$. There are 3 choices in every case, so 9 ways in total.
- $|A_1 \cap A_2 \cap A_3|$. Same analysis as in the previous case but with the additional requirement that $x_2 + x_3 + x_4 = 6$. Since $x_3 = 4$, we must have $x_2 + x_4 = 2$. Together with the equations $x_1 + x_2 = 2$ and $x_4 + x_5 = 2$, we only have 3 solutions, since $x_1 \in \{0, 1, 2\}$ determine all the other values of the variables.

Inclusion–exclusion now gives that the number of solutions we seek is

$$\binom{12}{4} - 3 \cdot 84 + (18 + 18 + 9) - 3 = 285.$$

15.2.2. Groups

Question 186. Let G be the group consisting of all 2×2-matrices of the form

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix}$$

where $a, b \in \{-1, 1, i, -i\}$, and the group-operation is matrix multiplication.

(a) Compute $|G|$ and determine if G is commutative or not.

(b) Find the order of the matrix $A = \begin{pmatrix} 0 & i \\ -1 & 0 \end{pmatrix}$.

(c) Is there a subgroup of G of size 8?

Solution. (a) The multiplication principle tells us that $|G| = 32$. The group is not commutative, since

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ och } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

do not commute.

(b) By Lagrange's theorem, the order must be a divisor of 32. By repeated squaring, we can find that the order of A is 8.

(c) Since A has order 8, it generates a cyclic group of size 8, so the answer is yes.

Question 187. Let $n \geq 2$. Suppose that $\eta : \mathrm{S}_n \to \mathbb{Z}_3$ is a homomorphism. Show that η cannot be surjective.

Solution. Every permutation $\pi = \tau_1 \cdots \tau_k$ can be expressed as a product of transpositions. If $\eta(\tau_j) = 0$ for every transposition, then η is not surjective as it sends everything to 0. So assume $\eta(\tau) \neq 0$ for some transposition. But then $\eta(\tau^2) = \eta(\mathrm{id}) = 0$, so $\eta(\tau)^2 = 0$. In particular, $\eta(\tau)$ is an element of order 2. However, this is impossible as there is no element in $\mathbb{Z}_3$ with order 2. It follows that $\eta(\tau) = 0$ for all transpositions, and therefore for all permutations as well.

15.2.3. Group action

Question 188. Let X be all possible ways to partition the elements in $\mathbb{Z}_6$ into 3 disjoint subsets of size 2. For example, $\{\{0,4\},\{1,5\},\{2,3\}\}$ is an element in X. The group $\mathbb{Z}_6$ act on X as follows:

$$a \cdot \{\{y_0, y_1\}, \{y_2, y_3\}, \{y_4, y_5\}\} = \{\{y_0 + a, y_1 + a\}, \{y_2 + a, y_3 + a\}, \{y_4 + a, y_5 + a\}\}.$$

(a) Determine $|X|$.

(b) Determine the orbit of $\{\{0,3\},\{1,5\},\{2,4\}\}$ under $\mathbb{Z}_6$.

(c) Determine the stabilizer of this element.

Solution. (a) We have that $|X| = \frac{1}{3!}\binom{6}{2,2,2} = 15$.

(b) The orbit is

$$\{03, 15, 24\},\ \{14, 02, 35\},\ \{25, 13, 04\}.$$

(c) The stabilizer is $\{0, 3\} \subseteq \mathbb{Z}_6$.

Question 189. Let X be the set of non-negative integer solutions $(x_0, x_1, \ldots, x_5)$ to

$$x_0 + x_1 + x_2 + x_3 + x_4 + x_5 = 12.$$

The group $\mathbb{Z}_6$ acts on X, by

$$a \cdot (x_0, x_1, \ldots, x_5) = (x_{0+a}, x_{1+a}, \ldots, x_{5+a})$$

where the index is computed modulo 6. Find the number of orbits under this group action.

Solution. We must find the number of fixed points for every element in $\mathbb{Z}_6$.

- 0: Every element is fixed, and we have $\binom{12+5}{5}$, as this is the total number of solutions.
- 1: Here, we need $x_0 = x_1 = \cdots = x_5$, and there is one solution, all variables equal to 2.
- 2: A solution must be of the form (a, b, a, b, a, b) so we need to count the number of solutions to $3a + 3b = 12$, that is, $a + b = 4$. This equation has 5 solutions.
- 3, A solution here is of the form (a, b, c, a, b, c) and this reduces to counting solutions to $2a + 2b + 2c = 12$, or $a + b + c = 6$. There are $\binom{6+2}{2}$ solutions.
- 4: Same number as for 2.
- 5: Same number as for 1.

Using Burnside's lemma, we have

$$\frac{1}{6}\left(\binom{17}{5} + 1 + 5 + \binom{8}{2} + 5 + 1\right) = 1038.$$

15.2.4. Graphs

Question 190. Suppose that a 5-regular graph G admits two disjoint Hamiltonian cycles (they do not share any edges). Show that G has a proper edge coloring *(In a proper edge coloring, any two edges that share a vertex must have different colors.)* using 5 colors.

Solution. Recall that in any graph (V, E), we have that $\sum_{v \in V} \deg(v) = 2|E|$. In our case, we have $\deg(v) = 5$, so $5|V| = 2|E|$. Since the right-hand side is even, we find that $|V|$ is even. Hence, each Hamiltonian cycle has an even number of edges.

We can then color the edges in the first Hamiltonian cycle alternating using `red` and `blue` color, and the edges in the second Hamiltonian cycle are colored `green` and `yellow`. The remaining edges are colored `orange`.

Since every vertex is visited by the two (edge-disjoint) Hamiltonian paths, its five connecting edges must all have different colors, and we are done.

Question 191. Given a graph G, we define the **line graph** $L(G)$ as follows. For every edge in G, there is a vertex in $L(G)$, and two vertices in $L(G)$ share an edge if and only if the corresponding edges in G share a vertex.

Show that $L(G)$ has an Euler circuit if G has an Euler circuit.

Solution. A graph G has an Euler circuit precisely when it is connected and every vertex has even degree.

Let $\{u, v\}$ be any edge in G. We know that $\deg(u) = 2a$, $\deg(v) = 2b$ for some integers $a, b \geq 1$, since the degree of every vertex in G is even. Now, uv is a *vertex* in $L(G)$, and it is connected to all the other edges connected to either u or v in G. Hence, uv (as a vertex in $L(G)$) has $(2a - 1) + (2b - 1) = 2a + 2b - 2$ neighbors in total, so $\deg(uv)$ is even.

Moreover, it is easy to see that $L(G)$ is connected if G is, so it follows that $L(G)$ must have an Euler circuit also.

Question 192. Let $\Gamma = (V, E)$ be a graph. For an integer $m \geq 1$, we construct a new graph Γ_m, with vertex set

$$\{(v, i) : v \in \Gamma, \quad 1 \leq i \leq m\}$$

and (v_1, i_1) is connected to (v_2, i_2) by an edge if and only if $v_1 = v_2$ and $|i_1 - i_2| = 1$.

(a) If $\Gamma = K_3$, draw Γ_2 and Γ_3.

(b) Prove that Γ and Γ_m have the same chromatic number.