Lecture Notes 2025W
104.694 VU Discrete Mathematics
(Lecture by Gittenberger)

October 6, 2025

Preface

I am indebted to Annemarie Borg and Reinhold Gschweicher who attended my lecture and wrote the original version of these lecture notes. As the course shrinked from 9 to 6 ECTS, I removed the parts that will not be taught anymore.

These lecture notes have to be read with care, as I have never found enough time for a thorough revision so far. They contain therefore still a lot of imprecisions in the presentation, mistakes and maybe even some serious errors.

Bernhard Gittenberger

Contents

Chapter 1

Graph Theory

1.1 Definition

1.1.1 Notation

First the used notations have to be defined.

Definition 1.1. *A mathematical structure $G = (V, E)$ is called a **graph**, which consists of the **vertex set** V and the **edge set** E.*

Definition 1.2. *A **directed graph** G is a graph in which all edges are directed. The **directed edges** $e \in E$ are pairs of the form $e = (v, w)$, for $v, w \in V$ and in particular $(v, w) \neq (w, v)$.*

Definition 1.3. *An **undirected graph** G is a graph in which all the edges $e \in E$ are of the form $e = \{v, w\}$. An edge e is a set and in particular $e = \{v, w\} = \{w, v\} = vw$. As a shorthand notation vw is used.*

There are some special edges: a **loop** is an edge (v, v) or $\{v, v\}$. If there are more edges between two nodes, it is a multi-set, with **multiple edges**.

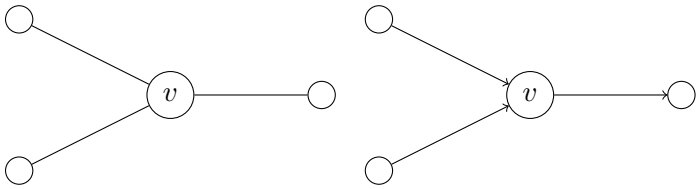
A graph without loops and without multiple edges is called a **simple graph**. Unless otherwise stated it can be assumed, that the graphs are simple and finite (there is a finite number of vertices).

(a) directed edge (b) undirected edge (c) loop (d) multiple edges

Figure 1.1: Different kind of edges

A graph corresponds to a **relation** R on V (i.e. $R \subseteq V \times V$), an undirected graph corresponds to a **symmetric relation**. The number of vertices are defined as $\alpha_0 = |V|$ and the number of edges are $\alpha_1 = |E|$.

$d(v)$	**degree**	number of edges which are incident to v
$d^+(v)$	**out-degree**	number of edges of the form (v, w)
$d^-(v)$	**in-degree**	number of edges of the form (w, v)
$\Gamma(v)$	**set of neighbors**	
$\Gamma^+(v)$	**set of successors**	set of vertices that are reachable from v
$\Gamma^-(v)$	**set of predecessors**	set of vertices from which v is reachable



(a) undirected graph, $d(v) = 3$ (b) directed graph, $d^+(v) = 1$, $d^-(v) = 2$

Figure 1.2: Examples for the degrees of vertex v

1.1.2 Some results and further concepts

Lemma 1.1 (Handshaking Lemma)**.** *Let $G = (V, E)$ be a simple graph. Then*

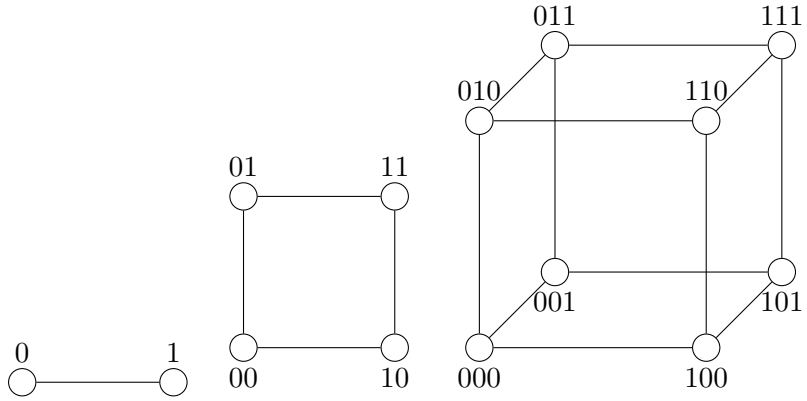
$$\sum_{v \in V} d(v) = 2|E| \qquad \text{if } G \text{ is undirected,}$$

$$\sum_{v \in V} d^+(v) = \sum_{v \in V} d^-(v) = |E| \qquad \text{if } G \text{ is directed.}$$

Proof.

- Undirected case:
  Count all the edges that are incident to v. If this is done for every $v \in V$, then every edge is counted twice.
- Directed case:
  Again count all the edges that are incident to v. However this time only the outgoing edges are counted.

□



(a) 1D-hypercube (b) 2D-hypercube (c) 3D-hypercube

Figure 1.3: n-Hypercubes

Example 1.1. *Let G be a graph, such that $G = (\{0,1\}^n, E)$ and $vw \in E \Leftrightarrow \sum_{i=1}^{n} |v_i - w_i| = 1$: if two vertices differ only in one coordinate, there is an edge between them. Now it is possible to compute the number of vertices (α_0) and the number of edges (α_1):*

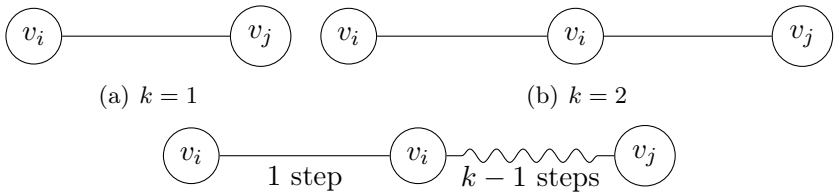
$$\alpha_0 = 2^n$$
$$\alpha_1 = \frac{1}{2} \sum_{v \in V} d(v) = 2^{n-1} \cdot n.$$

*If the degree of every vertex $v \in V$, is the same, it is said that G is a **regular graph**.*

Definition 1.4. *Let $e = vw \in E$. Then v and w are **adjacent**, this is denoted by $v \sim w$. Furthermore: e and v (or e and w) are said to be **incident**.*

Definition 1.5. *With the above definition, the **adjacency matrix** can be defined. Let $V = \{v_1, \ldots, v_n\}$ and $i, j = 1, 2, \ldots, n$, then the adjacency matrix $A = (a_{i,j})$ consists of the following entries:*

$$a_{i,j} = \begin{cases} 1 & v_i \sim v_j \text{ (v_i and v_j are adjacent)} \\ 0 & v_i \not\sim v_j \end{cases}$$



(a) $k = 1$ (b) $k = 2$

(c) induction-step

Figure 1.4: Adjacency via induction

Some remarks:

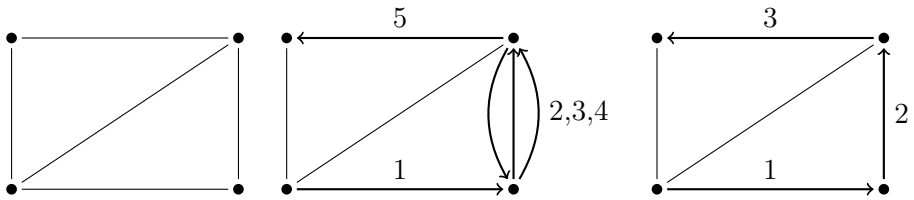
- *If G is undirected, A is symmetric.*
- *Consider the following adjacency matrix:*

$$A^k = (a_{ij}^{[k]})_{i,j=1,\dots,n} = A \cdot A^{k-1}$$

With $a_{ij}^{[k]} = \sum_{l=1}^{n} a_{il} \cdot a_{lj}^{[k-1]}$. In this matrix the entries $a_{ij}^{[k]}$ of A^k give the number of ways to get from v_i to v_j in exactly k steps.

Definition 1.6. *A **walk** in a graph G is a sequence of edges, where successive edges have a vertex in common. A walk may repeat an edge, but it does not make any jumps.*

*A **trail** is a walk, without repeating any edges. If a trail starts and ends in the same vertex, it is a **closed trail**, or a **circuit**.*



(a) Graph G (b) Walk over G (c) Trail over G

Figure 1.5: Walk and trail over G

Definition 1.7. *A graph $H = (V', E')$ of a graph $G = (V, E)$ is a **subgraph** of G ($H \leq G$) if:*

- *$V' \subseteq V$, and*
- *$E' \subseteq E$.*

E' contains only edges between vertices of V'. This is implied by the requirement that H is a graph.

Definition 1.8. *For undirected graphs, the **connectivity relation** R can be defined as follows:*

$$vRw \text{ (} v \text{ connected to } w\text{)} \iff \exists \text{ walk from } v \text{ to } w.$$

This relation can be described with a matrix C:

$$C = \sum_{k=0}^{L} A^k = (c_{i,j}).$$

With $L = \min(|E|, |V|-1)$ and $c_{i,j}$, which is the number of walks between v_i and v_j, the length has to be less than L.

The relation R has the following properties:

- $\forall v \in V : vRv$.
- $\forall v, w \in V,\ vRw \Rightarrow wRv$.
- $\forall u, v, w \in V,\ vRw \wedge wRu \Rightarrow vRu$.
- R is an equivalence relation!
- R induces a partition of V: $V = V_1 \cup V_2 \cup \ldots \cup V_n$ and if $i \neq j$ than $V_i \cap V_j = \varnothing$. The V_i's are the **connected components** of the graph.

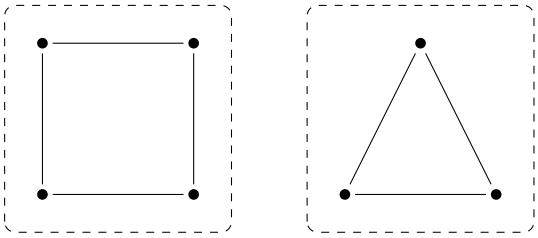


Figure 1.6: Graph with 2 components

Definition 1.9. *An undirected graph G is connected if $\forall v, w \in V : vRw$.*

Definition 1.10. *A subgraph H of G is a **connected component** of G if H is connected and H is maximal with regard to the subgraph relation. A graph H is maximal if: there exists no graph H' such that: $H \leq H' \leq G$ and H' is connected.*

Definition 1.11. *For directed graphs, the **connectivity relation** S is defined as follows:*

$$vSw \text{ (v connected to w)} \iff \exists \text{ walk from } v \text{ to } w \quad \text{and} \quad \exists \text{ walk from } w \text{ to } v.$$

Like R, S is an equivalence relation and S induces a partition on V.

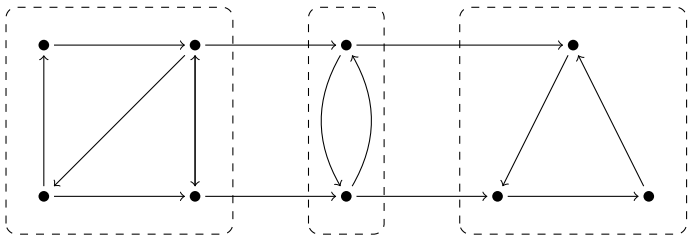


Figure 1.7: Graph with 3 strong connected components

Definition 1.12. *The directed graph G is **strongly connected** if and only if $\forall v, w \in V : vSw$.*

*Let $H \leq G$ and let H be maximal and strongly connected. Then H is a **strongly connected component** of G. The graph G is strongly connected if it has only one connected component.*

1.2 Trees and Forests

Definition 1.13. *An undirected acyclic graph $G = (V, E)$ is called a **forest**. A **tree** is a connected forest. If there is a node in a tree that can be designated as the **root**, it is a **rooted tree**.*

*A node which has degree 1 (there are no successors) is called a **leaf**. If removing an edge e increases the number of connected components, then e is called a **bridge**.*

*A **plane tree** is a tree embedded into the plane, i.e. the order of children (left and right) matters. Two trees may be isomorphic, but not equivalent when regarded as plane trees.*

An example for a plane, rooted tree is a binary search tree.

Definition 1.14. *Two graphs G and H are **isomorphic** ($G \cong H$) if there is a bijective function φ such that:*

$$\varphi : V(G) \mapsto V(H)$$

and: $vw \in E(G) \Leftrightarrow \varphi(v)\varphi(w) \in E(H)$.

Lemma 1.2. *Let T be a tree, with two ore more vertices: $|V(T)| \geq 2$, then T has at least two leaves.*

Proof.

- The tree with two nodes: in this case there is one edge, connecting the two leaves.
- A tree T, with at least three nodes: start at an arbitrary node, this node has to have a neighbor:
  - If the node has only one neighbor, remove the edge and this node, this gives a new tree: T'. The last part of the proof will be by induction: eventually the remaining tree has only two leaves.
  - If the node has more than one neighbor, see those neighbors as trees of their own and handle accordingly.

□

Theorem 1.1. *The following statements are equivalent:*

1. *T is a tree, it is a connected, acyclic, undirected graph.*
2. *$\forall v, w \in V(T)$ there is exactly one path from v to w.*
3. *T is connected and $|V| = |E| + 1$.*
4. *T is a minimal connected graph (every edge is a **bridge**).*
5. *T is a maximal acyclic graph.*

$1 \Rightarrow 3$. This will be proved by induction on $n = \alpha_0 = |V(T)|$. For $n = 1$ this is easy to see.

Take $n \to n + 1$ vertices. Choose a leaf v of T and create a new tree T' which is T without this leave: $T' = T \backslash \{v\}$. Apply the induction hypothesis: $|V(T')| = |E(T')| + 1 \Rightarrow |V(T)| = |V(T')| + 1 \wedge |E(T)| = |E(T')| + 1$, this proofs $1 \Rightarrow 3$, to prove the whole theorem, it would be necessary to prove equivalence for all five statements. □

1.2.1 Spanning subgraphs

Definition 1.15. *Let $G = (V, E)$ be an undirected graph. F is a **spanning forest** of G if and only if:*

1. *$V(F) = V(G)$ and $E(F) \subseteq E(G)$.*
2. *F is a forest*
3. *F has the same connected component as G.*

*If F is connected, it is a **spanning tree**.*

Example 1.2. *Take a square with nodes and edges:*

$$V = \{1, 2, 3, 4\}$$

$$E = \{\{1, 2\}, \{2, 4\}, \{3, 4\}, \{1, 3\}, \{1, 4\}\} = \{a, b, c, d, e\}.$$

There are eight spanning trees, all using only three edges.

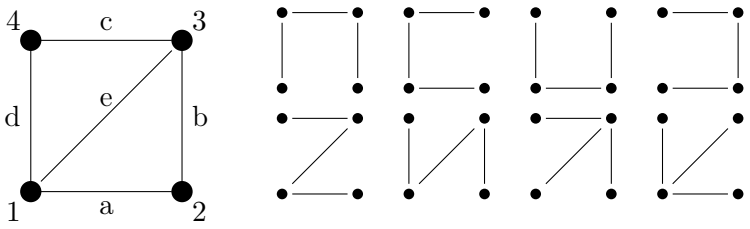


Figure 1.8: Graph G and all its spanning trees

It is possible to construct the adjacency matrix A and the degree matrix D from here. Taking nameweights into account the adjacency matrix $\widetilde{A}$ looks like:

$$\widetilde{A} = \begin{pmatrix} 0 & a & d & e \\ a & 0 & 0 & b \\ d & 0 & 0 & c \\ e & b & c & 0 \end{pmatrix}$$

The degree matrix with nameweights, $\widetilde{D}$, looks like:

$$\widetilde{D} = \begin{pmatrix} a+d+e & 0 & 0 & 0 \\ 0 & a+b & 0 & 0 \\ 0 & 0 & b+c+e & 0 \\ 0 & 0 & 0 & c+d \end{pmatrix}$$

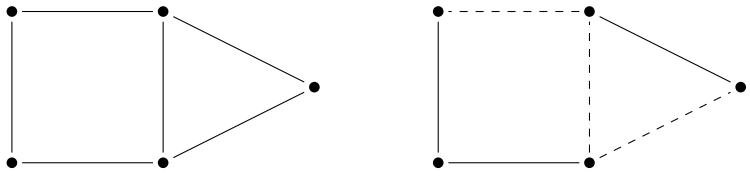
Resulting in:

$$\widetilde{D} - \widetilde{A} = \begin{pmatrix} a+d+e & -a & -e & -d \\ -a & a+b & -b & 0 \\ -e & -b & b+c+e & -c \\ -d & 0 & -c & c+d \end{pmatrix}$$

The determinant will give all the possible spanning subtrees:

$$\begin{vmatrix} a+b & -b & 0 \\ -b & b+c+e & -c \\ 0 & -c & c+d \end{vmatrix} = (a+b)(c+d)(b+c+e) - b^2(c+d) - c^2(a+b)$$
$$= bcd + abc + abd + acd + ace + ade + bce + bde.$$

If $a = b = c = d = e = 1$ then the determinant would be 8: the number of spanning subtrees.



(a) Graph G (b) maximal forest

Figure 1.9: Maximal spanning forest of graph G

Theorem 1.2 (Kirchhoff's Matrix-Tree Theorem)**.** *Let G be an undirected connected graph, A the adjacency matrix and D the degree matrix (with on its diagonal: $d(v_1), d(v_2), \ldots, d(v_n)$). The number of spanning trees is: $|\det((D-A)')|$, in which $(D-A)'$ is the matrix $D-A$ with one row and one column deleted.*

In the case that G is not connected, the same principle can be applied for every connected component. To count the number of possible spanning forests, you have to multiply.

Remark: *If you want to know which tree is cheapest, it is not efficient to generate them all. There are however some efficient algorithms that can do that.*

1.2.2 Minimum or maximum Spanning Trees

Given an undirected graph $G = (V, E)$, with a **weight function** $w : E \to \mathbb{R}$, every edge in E is assigned a weight: $e \mapsto w(e)$. Then G is called a **weighted graph** (sometimes also called a **network**).

The main interest lies in a subset of the edges. $F \subseteq E$ and $w(F) = \sum_{e \in F} w(e)$ are defined as the weight of the edge set F. The problem that arises is to find a set F, a spanning forest (with its vertices), with $w(F)$ (the weight) minimal/maximal. This problem is called the **MST problem**.

A greedy algorithm that gives the right set of edges **Kruskal's algorithm**.

Algorithm 1: Kruskal's algorithm

input : A undirected graph $G = (V, E)$, with a weight function w
output: A set $F \subseteq E$, with $G'(V, F)$ a spanning forest

```
1  Sort edges by weight; E' := ∅; j := 1;
2  if (V, E' ∪ {e_j}) is acyclic then
3  |  E' := E' ∪ {e_j};
4  end
5  if (j = |V| − 1 or j = m) then
6  |  END
7  else
8  |  j := j + 1;
9  |  goto 2;
10 end
```

1.2.3 Matroids and Greedy Algorithms

Kruskal's algorithm is a **greedy algorithm**. This algorithm only works on a local view of the graph and they use these local values to solve the maximization (or minimization) problem. Since it is greedy, it generally does not produce optimal maximal or minimal spanning trees. However it always works in the special case of **matroids**.

Using Kruskal's algorithm, the edges are stored in decreasing order of their weight. Every time the next best one is taken, with the restriction that it does not create a cycle. Let $G(V, E)$ be a graph on which Kruskal is used and define $S = \{F \subseteq E \mid F \text{ is a forest}\}$. The algorithm constructs a tree T, such that: $T := T \cup \{e\}$ if $T \cup \{e\} \in S$. In this case S is the set of all the possible forests with the edges in G. Note that, if an edge is used, the two vertices, that are connected by this edge, are also present in the generated tree.

Definition 1.16 (Independence systems)**.** *(E, S) is an **independence system** if $S \subseteq 2^E$ and S is closed under inclusion. If $A \in S$ and $B \subseteq A$ then $B \in S$. S is called the set of **independent sets**.*

This definition gives rise to a new optimization problem. Given the system (E, S) with $w : E \to \mathbb{R}_0^+$, $A \subseteq S$ and $w(A) = \sum_{e \in A} w(E)$. The problem is to search for an A such that $w(A)$ is maximal (or minimal) and A is in S. A should be maximal with respect to inclusion ($B \supseteq A$ implies $B \in S$). An example is the system (E, S) in which E is the edge set and S is the set of forests.

A more generalized version of Kruskals algorithm is called **GREEDY**:

Algorithm 2: Generalized Kruskal: GREEDY

input : Sets E and S, a weight function w and the set T, which is the result of this algorithm

output: A spanning forest

```
1 Sort the elements of E according to weight: E = {e_1, ..., e_k | w(e_1) ≤ w(e_2) ≤ ...};
2 T = ∅;
3 for k = 1, ..., m do
4 |   if T ∪ {e_k} ∈ S (it does not create a cycle) then
5 |   |   T := T ∪ {e_k};
6 |   end
7 end
```

Definition 1.17 (Matroids)**.** *An independence system $M = (E, S)$ is called a* ***matroid*** *if for all $A, B \in S$ such that $|B| = |A| + 1$ there exists $v \in B \backslash A$ with $A \cup \{v\} \in S$.*

Remark: *This so called matroid property holds in general for $A, B \in S$ such that $|A| \leq |B|$ as well.*

Definition 1.18. *$A \in S$ is a* ***basis*** *of M if and only if A is a maximal independence set, with respect to inclusion. If A, B are bases of M, then the* ***rank of the matroid*** *M is defined as: $r(M) = |A| = |B|$.*

Theorem 1.3. *Let $G(V, E)$ be an undirected graph and $S = \{F \subseteq E \mid F \text{ is a forest}\}$, then (E, S) is a matroid.*

Proof. Suppose $F_1, F_2 \subseteq E$, such that $F_2 \in S$ and $|F_2| = |F_1|+1$. Suppose F_1 has m connected components (trees): $T_i = (V_i, A_i)$ for $i = 1, \ldots, m$.

Observe: $V = V_1 \cup V_2 \cup \ldots \cup V_m$, $F_1 = A_1 \cup A_2 \cup \ldots \cup A_m$ with $|A_i| = |V_i| - 1$ and F_2 is a forest.

Since F_2 is a forest it follows that there are at most $|V_i|-1$ edges in F_2 which connect $v, w \in V_i$, since $|F_2| > |F_1|$. This means that there exists an edge e, which connects two components of F_1, in F_2. Hence $F_1 \cup \{e\}$ is a forest.

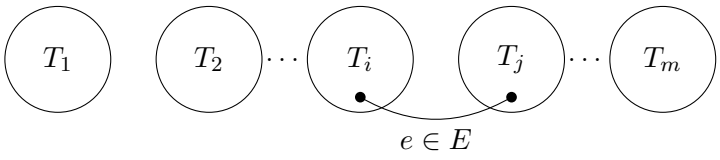


Figure 1.10: Forest F_2 and its trees

□

Example: Let $E = \{a_1, a_2, \ldots, a_n\}$ be a set of vectors in $\mathbb{R}^m$. Define the set S as follows: $S = \{A \subseteq E \mid A = \varnothing \text{ or } A = \text{linear independent}\}$. S is an independence system and it also a matroid.

Remark: A is a basis of S if and only if A is a basis of the span of E (denoted by $[E]$), a vector space. The rank of M is: $r(M) = \dim([E])$. If $A, B \in S$ and $|A| + 1 = |B|$ then $\exists x \in B \backslash A$ such that $A \cup \{x\} \in S$.

Theorem 1.4. *Let $M = (E, S)$ be a matroid with weight function $w : E \to \mathbb{R}$. Then **GREEDY** computes* "A is maximal with respect to inclusion such that $w(A)$ is minimal (or maximal)" *correctly. **GREEDY** computes the basis with minimal (or maximal) weight.*

Proof. Let A be the resulting set after running **GREEDY**, $A = \{a_1, a_2, \ldots, a_r\}$. The proof consists of three parts:

1. Start with proving that A is a basis, $A \in S$, by construction. Assume that A is not maximal, then $\exists e \in E$ such that $A \cup \{e\} \in S$. This is a contradiction, which means that A is maximal and hence a basis.

2. Now to prove that $w(a_1) \leq w(a_2) \leq \ldots \leq w(a_r)$. The elements are sorted in advance, **GREEDY** takes them in order, this property holds as well.

3. In this step it has to be proven that $w(A)$ is minimal. To to get a contradiction, assume that $w(A)$ is not minimal. Then $\exists B = \{b_1, \ldots, b_r\}$, which is a basis such that $w(B) < w(A)$, with $w(b_1) \leq w(b_2) \leq \ldots \leq w(b_r)$.

   Define $i := \min\{j \mid w(b_j) < w(a_j)\}$ and $A_{i-1} = \{a_1, \ldots, a_{i-1}\}$ as the status of A after $m \geq i - 1$ iterations of **GREEDY**. Now $B_i = \{b_1, \ldots, b_i\}$ and hence $|B_i| = |A_{i-1}| + 1$.

   Apply the matroid condition: $\exists b_j \in B_i \backslash A_{i-1}$ such that $A_{i-1} \cup \{b_j\} \in S$, but $w(b_j) \leq w(b_i) < w(a_i)$. This implies $\forall x \in B_i$: $w(x) < w(a_i)$. However, this is not how **GREEDY** works, the algorithm would have found b_j before a_i, which means that it would already have been added to the matroid. Since this is a contradiction, it follows that $w(A)$ is indeed minimal. □

With this, it has been proven that **GREEDY** works on matroids in a general setting. It is left to prove that matroids are exactly the structures on which **GREEDY** works correctly.

Theorem 1.5. *$M = (E, S)$ is an independence system. Assume **GREEDY** solves the optimization problem* "A is maximal such that $w(A)$ is maximal" *correctly for all weight functions on w, then M has to be a matroid.*

Proof. Assume M is not a matroid, then $\exists A, B \in S$ such that $|B| = |A| + 1$ and $\forall x \in B \backslash A$: $A \cup \{x\} \notin S$. What is $w(A)$ if $w(e)$ is set to:

$$w(e) = \begin{cases} |A| + 2 & \text{if } e \in A \\ |A| + 1 & \text{if } e \in B \backslash A \\ 0 & \text{otherwise} \end{cases}$$

To get a contradiction, present a weight function for which **GREEDY** does not work. By definition:

$$w(A) = |A| \cdot (|A| + 2) < (|A| + 1)^2 \leq w(B).$$

This implies that A is not a solution of the optimization problem and also not of *"$w(A)$ is maximal"*. **GREEDY** chooses $x \in A$ first (because $w(A) < w(B)$), then $w(A)$ cannot be increased anymore if $x \in B \backslash A$. This implies $A \cup \{x\} \notin S$ by assumption, so $x \notin A \cup B$. If all the weights would be zero, **GREEDY** arrives eventually at a set such that $w(N) = w(A)$ is not maximal. This is a contradiction: M has to be a matroid. □

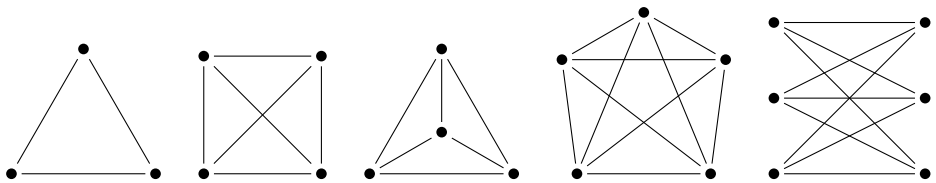
1.3 Special Graph Classes

There exists, besides trees and forest many other special graph classes. We will briefly discuss planar graphs and bipartite graphs.

1.3.1 Planar Graphs

Definition 1.19. *A graph G is **planar** if there is an isomorphic graph H embedded in the plane (vertices are points in the plane $= \mathbb{R}^2$) such that no two edges intersect.*

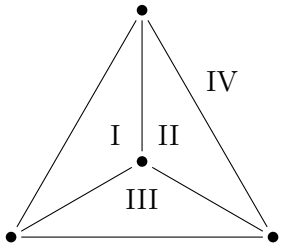
Example 1.3. *The graphs K_3 and K_4 (the complete graphs with three resp. four vertices) are planar. However, the graph K_5 is the smallest non-planar graph and the graph $K_{3,3}$ is the smallest non-planar complete bipartite graph.*



(a) K_3, planar (b) K_4, planar (c) K_4, planar, alternative (d) K_5, nonplanar (e) $K_{3,3}$, nonplanar, bipartite

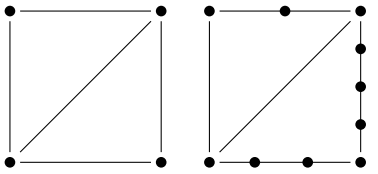
Figure 1.11: Examples for planar and non-planar graphs

Definition 1.20. *The edges of a graph (which have to be* Jordan curves*) divide the plane into regions. These regions are the **faces** of the graph, if the graph is planar. All the space outside the graph is a face as well. The number of faces will be denoted by α_2.*



$\alpha_0 = 4$
$\alpha_1 = 6$
$\alpha_2 = 4$

Figure 1.12: Faces of K_4



(a) Graph G (b) subdivision H of G

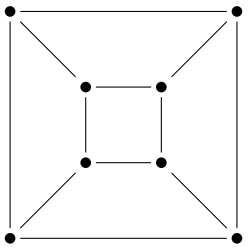
Figure 1.13: Graph G and a possible subdivision H

Definition 1.21. *A graph H is called a **subdivision** of G if H is obtained by replacing every edge of G by a path. This means: just adding some nodes on each edge, such that the edges become paths.*

Theorem 1.6. *A graph G is planar if and only if there exists no subgraph which is a subdivision of K_5 or of $K_{3,3}$.*

Proof. ("⇒") This side of the proof is to hard for this course. ("⇐") This side of the proof is trivial, since it is known that K_5 and $K_{3,3}$ are non-planar. □

Theorem 1.7 (Euler's polyhedron formula)**.** *If G is a connected and planar graph, then $\alpha_0 - \alpha_1 + \alpha_2 = 2$. Where $\alpha_0 - \alpha_1 + \alpha_2$ is also known as **the Euler characteristics**.*



$\alpha_0 = 8$
$\alpha_1 = 12$
$\alpha_2 = 6$
$\alpha_0 - \alpha_1 + \alpha_2 = 8 - 12 + 6 = 2$

Figure 1.14: Polyhedron of a dice

Proof. The proof is done by induction on α_2. Start with $\alpha_2 = 1$. This means that G must be a tree: there is only one face and the face outside of the graph is counted once, which means that there cannot be any cycles in a graph with $\alpha_2 = 1$. In a tree the following holds:

$$\alpha_0 - \alpha_1 + 1 = \alpha_0 - (\alpha_0 - 1) + 1 = 2.$$

Assume that this holds for all α_2 up to k faces. Apply induction $k \mapsto k + 1$. G has at least $k + 1 \geq 2$ faces. This implies that there exists an edge that separates two faces. Remove such an edge, which gives a new graph G', where $\alpha_2 = k$. This means:

$$\begin{aligned} \alpha_2(G') = k &\Rightarrow \alpha_0(G') - \alpha_1(G') + \alpha_2(G') = 2 \\ &\Rightarrow \alpha_0(G) - \alpha_1(G) + \alpha_2(G) = \alpha_0(G) - (\alpha_1(G') + 1) + (\alpha_2(G) + 1) = 2. \end{aligned}$$

□

Lemma 1.3. *If G is a simple, connected, planar graph, with no cycles of length 3 (this also means, no cycles of length ≤ 3), then*

$$\alpha_1(G) \leq 2\alpha_0(G) - 4.$$

Proof. Let f_j denote the number of faces with a boundary of length j. In this case: $f_3 = 0$. Then:

$$\begin{aligned} \sum_{j\geq 4} f_j &= \alpha_2 \\ \sum_{j\geq 4} j \cdot f_j &\leq 2 \cdot \alpha_1 \\ 4 \cdot \sum_{j\geq 4} f_j &= 4 \cdot \alpha_2 \leq 2 \cdot \alpha_1. \end{aligned}$$

From this it follows:

$$\begin{aligned} \alpha_0 - \alpha_1 + \alpha_2 &\geq 2 \\ 2\alpha_0 - 2\alpha_1 + 2\alpha_2 &\geq 4 \qquad \text{(where } 2\alpha_2 \leq \alpha_1\text{)} \\ 4 &\leq 2\alpha_0 - \alpha_1 \\ \alpha_1 &\leq 2\alpha_0 - 4. \end{aligned}$$

□

Remark: In a graph with k components, the Euler characteristic becomes: $\alpha_0 - \alpha_1 + \alpha_2 = 1 + k$.

Corollary 1.1. *The graph $K_{3,3}$ is not planar. Assume it is planar. Notice that $\alpha_0 = 6$ and $\alpha_1 = 9$, as it is a bipartite graph, there are no cycles of length 3: $f_3 = 0$. Therefore*

$$9 = \alpha_1 \leq 2\alpha_0 - 4 = 12 - 4 = 8$$

should hold, which is apparently not true. So, $K_{3,3}$ is not planar.

For K_5, the lemma does not apply, since this graph does have cycles of length 3.

Definition 1.22. *Let $G = (V, E)$ be a planar graph and let F be the set of its faces. Then $G^* = (V^*, E^*)$ is defined such that $V^* = F$ and for every edge $e \in E$, set $e^* = (f_1, f_2)$, if f_1 and f_2 are the faces left and right of e. G^* is called the **dual** of G.*

Remark Some remarks on the dual G^* of G:

- G^* is not unique.
- $|E| = |E^*|$.
- In general $|G^*|$ is a multigraph.
- Let G_1 and G_2 be duals of G, they might be different, but they are at least isomorphic: $G_1 \cong G_2$.

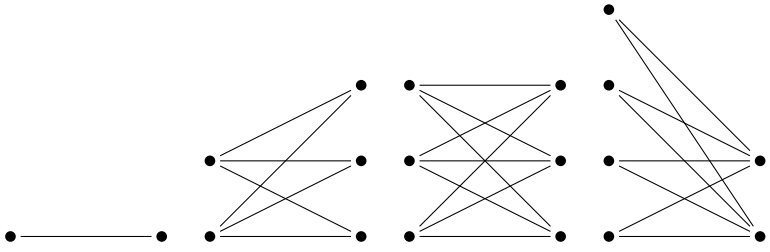
Theorem 1.8 (Whitney's Theorem)**.** *Let $A \subseteq E$, such that A is a cycle in G if and only if A^* is a minimum cut. Let G be a not necessarily planar graph, define G^{**} with this property such that: if G is planar, then $G^{**} \cong G^*$. If G is not planar, G^{**} does not exist.*

1.3.2 Bipartite Graphs and Matchings

Definition 1.23. *Let $G = (V, E)$ be a simple undirected graph. G is called **bipartite** if and only if:*

$$V = V_1 \cup V_2, V_1 \cap V_2 = \varnothing$$
$$vw \in E \Rightarrow v \in V_1, w \in V_2.$$

The complete bipartite graph is denoted by $K_{n,m}$.



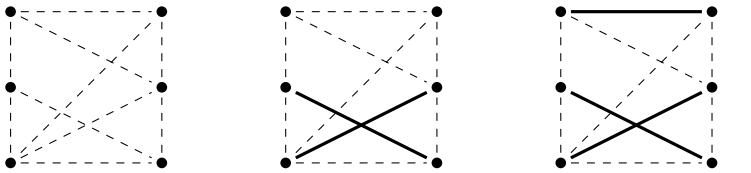
(a) $K_{1,1}$ (b) $K_{2,3}$ (c) $K_{3,3}$ (d) $K_{4,2}$

Figure 1.15: Examples for bipartite graphs

Definition 1.24. *A **matching** is a subset of edges $M \subseteq E$ such that*

$$\forall e, f \in M : e, f \text{ have no vertex in common.}$$

*A matching is a **perfect matching** if $\forall v \in V$, v is incident to some $e \in M$.*



(a) Graph G (b) Possible matching (c) Perfect matching

Figure 1.16: Graph with (perfect) matching

Theorem 1.9 (Hall's marriage theorem)**.** *Given a bipartite graph $G = (V, E)$, such that $V = W \cup M$, where W and M are finite and nonempty. Define the friendship relation: $F \subseteq W \times M$, with $wm \in E \Leftrightarrow wFm$.*

*A **feasible marriage** is a complete matching $F_1 \subseteq F$ (i.e. $\forall x \in W : \exists! y \in M$ such that xFy). Now the theorem states the following: there is a feasible marriage, if and only if:*

$$\forall W_0 \subseteq W : \underbrace{|\{y \in M \mid \exists x \in W_0 : x \,\mathrm{F}\, y\}|}_{\bigcup_{w \in W_0} \Gamma(w)} \geq |W_0|.$$

If there is a feasible marriage, every woman gets a partner.

Proof. ("⇒") This side of the proof is trivial. ("⇐") Consider a network given by a source with directed edges to all elements in W (each edge with weight $w = 1$). For each element in M, there is an edge to the sink (all of these edges also have weight $w = 1$). The edges between W and M all have weight $w = |W| + |M| + 1$. With this definition all the weights are integers, which means that there exists a maximal flow with integer weight.

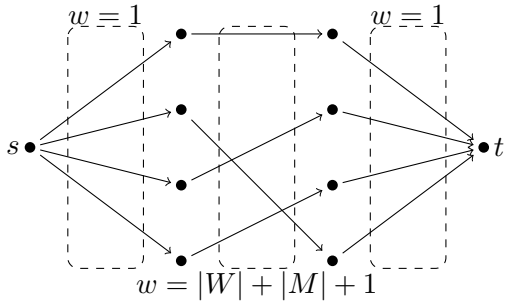


Figure 1.17: Feasable marriage, ∃ maximal flow with integer weights

Claim: $S = (\{s\}, V\backslash\{s\})$ is an minimum cut: $c(S) = |W|$.

Assume that there exists a S' such that $c(S') < c(S)$, this means: S' has no edge wm, with $w \in W$ and $m \in M$. Hence:

$$S' = (V_1, V_2) \hat{=} \{sw \mid w \in \widetilde{W} \subseteq W\} \cup \{mt \mid m \in \widetilde{M} \subset M\}.$$

The claim is that:

$$w \in W\backslash\widetilde{W}, m \in \Gamma^+(w) \Rightarrow m \in \widetilde{M}.$$

Assume that this does not hold, then there is a path such that $s \to w \to m \to t$, without using an edge of S'. But that would mean that $w, t \in V_1$, which is by construction not possible. This implies that:

$$\left| \bigcup_{w \in W\backslash\widetilde{W}} \Gamma^+(w) \right| \leq |\widetilde{M}|.$$

But

$$c(S') = |\widetilde{W}| + |\widetilde{M}| < c(S) = |W|.$$

This implies that:

$$|\widetilde{M}| < |W\backslash\widetilde{W}|.$$

But that is a contradiction which means that $c(S')$ cannot be a minimal cut: $c(S)$ is the minimal cut, which concludes the proof of the claim.

By the Ford and Fulkerson Algorithm, there exists a flow ϕ such that $v(\phi) = c(S) = |W|$. This flow defines the feasible marriage relation. □

1.4 Graph Colorings

A simple undirected graph $G = (V, E)$ can be used for graph colorings. Like coloring the countries on a map. A planar graph can be used to represent the coloring of the countries.

Definition 1.25. *Let $G = (V, E)$ be a simple undirected graph. A **vertex coloring** is a mapping $c : V \to C$ in which $C = \{c_1, \ldots, c_r\}$, a set of possible colors.*

*A coloring is **feasible** if $vw \in E \Rightarrow c(v) \neq c(w)$.*

Definition 1.26. *An **edge coloring** can be defined as: $\overline{c} : E \to C$, such that a coloring is feasible if edges that have a common vertex, have different colors. Then it follows that*

$$\overline{G} = (\overline{V}, \overline{E}), \overline{V} = E, \text{ and } e_1e_2 \in \overline{E} \Leftrightarrow e_1, e_2 \text{ share a common vertex.}$$

Based on this definition, everything that can be done with a vertex coloring, can also be done with an edge coloring.

Remark: Similarly, face colorings of a planar graph (think of the countries on a map) can be defined.

Definition 1.27. *Let $G = (V, E)$ be a graph. Then the **chromatic number** $\chi(G)$ is the minimum number of colors such that there is a feasible coloring.*

Some examples:

$$\begin{aligned} \chi(K_n) &= n \\ \chi(K_{n,m}) &= 2 \\ \chi(T) &= 2 \text{ if } T \text{ is a tree and } |V| > 1 \end{aligned}$$

Theorem 1.10. *Some theorems about graph coloring, with obvious proofs or proofs too hard for a normal human being:*

- *$\chi(G) = 1$ if $E(G) = \varnothing$.*
- *$\chi(G) = 2$ if and only if $E(G) \neq \varnothing$ and G is bipartite.*
- *$\chi(G) = 2$ if and only if $E(G) \neq \varnothing$ and all cycles have even length.*
- *If G is a planar graph: $\chi(G) \leq 4$. This is really hard to prove, in which many cases have to be considered.*
- *$\chi(G) \leq 1 + \max_{v \in V} d(v)$. This can be proved by induction on the number of vertices.*

Theorem 1.11. *If $G = (V, E)$ is a planar graph, then $\chi(G) \leq 5$.*

Proof. This proof is easier than the 4-color theorem. However, there are still some cases, which have to be considered. Start with a claim: the minimunm degree is less or equal to 5: $d_{\min} \leq 5$, this claim has to be proven first.

Assume $d_{\min} \geq 6$, then

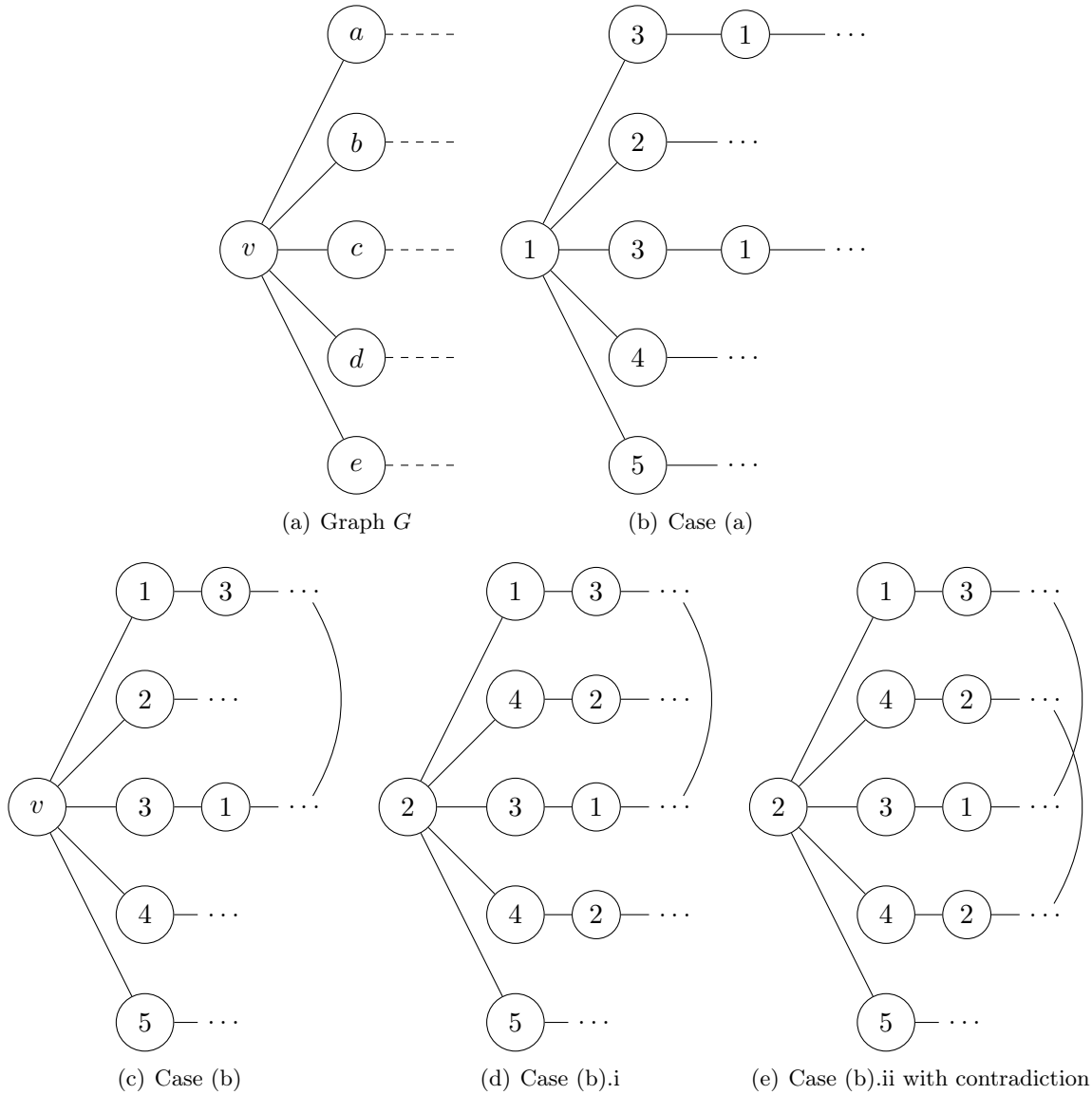
$$2\alpha_1 = \sum_{x \in V} d(x) \geq 6\alpha_0$$

which implies that $\alpha_1 \geq 3\alpha_0$. It is known that $2\alpha_1$ is the sum over all faces from the boundary edges, which is greater or equal to $3\alpha_2 = 3(2 - \alpha_0 + \alpha_1)$. Now: $\alpha_1 \leq 3\alpha_0 - 6$ but $\alpha_1 \geq 3\alpha_0$! This is a contradiction. Hence: there has to be a vertex with $d \leq 5$.

With this claim, the following cases can be proven, which will prove the whole theorem:

1. Suppose $d_{\min} \leq 4$ and suppose that x_0 is a vertex such that $d(x_0) \leq 4$. Define $G' = G \backslash \{x_0\}$ and assume $\chi(G') = 5$. Then, since x_0 has at most 4 neighbors, the vertex x_0 can be colored with the remaining color. Then, by induction: $\chi(G) = 5$.
2. There is vertex v, such that $d(v) = d_{\min} = 5$. Suppose the neighbors of v are $\{a, b, c, d, e\}$, such that $c(a) = 1, c(b) = 2, c(c) = 3, \ldots$. Define the following set: $G_a = \{x \in V \mid \exists 1 - 3 - 1 - 3 - \ldots \text{path a} \rightsquigarrow x\}$. And define a similar set for G_c.
   (a) If $G_a \cap G_c = \varnothing$, the vertices in G_a can be recolored, by switching colors 1 and 3. Then v can be colored with $c(v) = 1$.
   (b) If $G_a \cap G_c \neq \varnothing$, then it has to be the case that $G_a = G_c$. In the same way this can be done for G_b and G_d:
      i. If $G_b \cap G_d = \varnothing$, then recolor G_b by switching 2 and 4, and let $c(v) = 2$.
      ii. If $G_b \cap G_d \neq \varnothing$, then $G_b = G_d$. However, this is a contradiction: the graph G is a planar graph, which means that the paths $G_a = G_c$ and $G_b = G_d$ cannot cross each other.

□



(a) Graph G (b) Case (a)

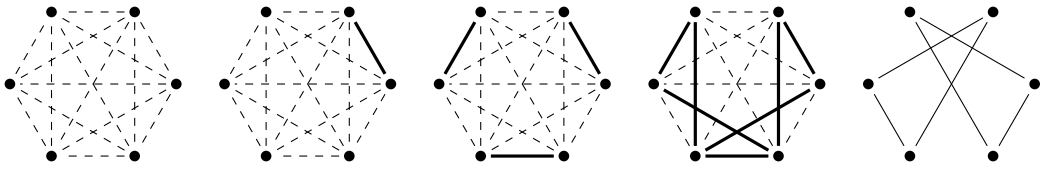
(c) Case (b) (d) Case (b).i (e) Case (b).ii with contradiction

Figure 1.18: Planar graph coloring

1.4.1 Ramsey Theory

Example 1.4. *Every 2-edge coloring of K_6 has a monochromatic K_3.*

Proving this can be done by drawing such a graph. A monochromatic triangle will always be found!



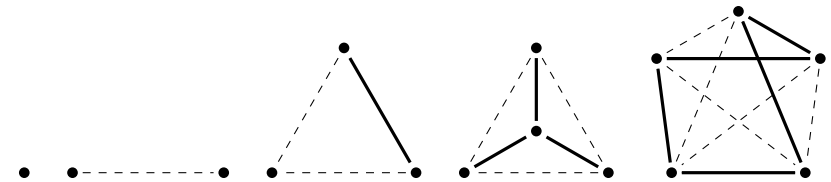
(a) K_6 (b) Start coloring edges (c) Continue (d) Stuck (e) Thin triangles

Figure 1.19: Attempt to color a K_6 without producing a monochromatic triangle.

*The idea of those monochromatic subgraphs can be generalized: take K_n instead of K_6 and K_r and K_s instead of K_3. This is exactly what the **Ramsey Theory** does.*

Definition 1.28. *The **Ramsey number** $R(r, s)$ is the minimum n such that every red-blue coloring of K_n contains either a red K_r or a blue K_s.*

In the given example: $R(3, 3) \leq 6$. It can even be shown that $R(3, 3) = 6$.



(a) K_1 (b) K_2 (c) K_3 (d) K_4 (e) K_5

Figure 1.20: Examples for Ramsey number

Lemma 1.4. $R(r, s) \leq R(r-1, s) + R(r, s-1)$.

Proof. Let $n = R(r-1, s) + R(r, s-1)$ and partition K_n. Take a vertex v, let M be the set of all the neighbors of v connected with a red edge and let N be the set of all neighbors of v connected with a blue edge.

Claim: $|M| \geq R(r-1, s)$ or $|N| \geq R(r, s-1)$ and $n = |M| + |N| + 1$. Now there are two possibilities:

- There exists a blue K_s in M or a red K_{r-1} in N.
- There exists a blue K_{s-1} in M or a red K_r in N.

To show that there exists a blue K_s or a red K_r. In both cases, together with v, it is always possible to find a blue K_s or a red K_r. □

Corollary 1.2. $R(r, s) \leq \binom{r+s-2}{r-1} \leq 2^{r+s-2}$.

Proof. Start with $R(2,n) = R(n,2) = n \leq \binom{n}{1}$. From there, apply induction, use Pascal's triangle and the above lemma. This will give the whole proof. □

Definition 1.29.

$$R(n_1, n_2, \ldots, n_r) = \min\{n \mid \textit{all } r\textit{-edge colorings of } K_n \textit{ (colors } c_1, \ldots, c_r\textit{)} \\ \textit{have a } c_j\textit{-colored } K_j \textit{ for some } j\}$$

Chapter 2

Advanced Combinatorics

2.1 Enumerative Combinatorics

The first part of this chapter will be about enumerative combinatorics: Let A be a finite set, the goal is to find the cardinality of A: $|A|$. More general: Given a collection/system/family of sets $(A_n)_{n\geq 0}$, let $a_n = |A_n|$, what is the **counting sequence** $(a_n)_{n\geq 0}$?

- In the best case, it is possible to find a closed formula.
- Otherwise a recursion or a generating function is also alright (e.g. $\sum_{n\geq 0}[a_n z^n]$).
- If all those options fail an asymptotic estimate can be used:

$$a_n \sim b_n \Leftrightarrow \lim_{n\to\infty} \frac{a_n}{b_n} = 1.$$

Example 2.1. *Let $A_n = \{$permutations of $1, 2, \ldots, n\}$, then $|A_n| = n!$. Now let $a_1 = 1$ and $a_n = na_{n-1}$. Then $a_n \sim \left(\frac{n}{e}\right)^n \sqrt{2\pi n}$.*

2.1.1 Counting Principles

The elementary counting principles are:

- Sum principle: $A \cap B = \varnothing \Rightarrow |A \cup B| = |A| + |B|$.
- Product principle: $|A \times B| = |A| * |B|$.
- Bijection principle: A bijective mapping $f : A \mapsto B \Rightarrow |A| = |B|$.

Example 2.2. What is the number of two-digit positive integers? *This problem looks at the set $\{10, \ldots, 99\}$. It is easy to see that its cardinality is 90. But this can also be done with the given product principle, let xy be such an integer, then:*

$$x \in X = \{1, 2, \ldots, 9\}$$
$$y \in Y = \{0, 1, \ldots, 9\}$$
$$|X \times Y| = |X| * |Y| = 9 * 10 = 90.$$

Example 2.3. How many passwords are there that have 4 up to 10 digits? *Let A_i denote the set of passwords with i digits. Let $Y = \{0, 1, \ldots, 9\}$, then:*

$$\begin{aligned} A_i &= Y^i \\ |Y| &= 10 \\ |A_i| &= 10^i \\ \textit{Total number} &= 10^4 + 10^5 + \ldots + 10^{10}. \end{aligned}$$

Example 2.4. There is a thief, who saw someone using his bankcard and afterwards stole this card. The thief has seen that the code starts with 0 and contains an 8. How many possibilities are left for the thief to check?

Since one of the four digits is already known, we know by the product principle, that there are 10^3 possibilities left, including codes without the integer 8. With the sum principle, the codes without the integer 8, there are 9^3 such codes, can be subtracted, this gives a total of:

$$\textit{Total number} = 10^3 - 9^3 = 271.$$

Example 2.5. Given a set $A = \{a_1, a_2, \ldots, a_n\}$ and its power set: $2^A = \{X \mid X \subseteq A\}$, what is the cardinality of this powerset, what is: $|2^A|$?

Define the set: $B \subseteq A$; $B = \{a_{i_1}, \ldots, a_{i_k}\}$, where $k \leq n$, such that $1 \leq i_i \leq i_2 \leq \ldots \leq i_k \leq n$. Map B to a new set: $B \mapsto (b_1, b_2, \ldots, b_n) \in \{0, 1\}^n$, such that:

$$b_i = \begin{cases} 1 & a_i \in B \\ 0 & a_i \notin B \end{cases}$$

The mapping $f : 2^A \mapsto \{0, 1\}^n$ is bijective, by the bijection principle it follows that $|2^A| = |\{0, 1\}^n| = 2^n$.

Double counting: Given two sets $A = \{a_1, a_2, \ldots, a_m\}$ and $B = \{b_1, b_2, \ldots, b_n\}$ and a relation $R \subseteq A \times B$, such that $aRb \Leftrightarrow (a, b) \in R$. Define two other sets: $R_{i,0} = \{b \in B \mid a_i R b\}$ and $R_{0,i} = \{a \in A \mid aRb_i\}$, where the subscript 0 just means that this part is fixed. Then:

$$|R| = \sum_{i=1}^{m} |R_{i,0}| = \sum_{j=1}^{n} |R_{0,j}|.$$

Proof. Define a matrix (x_{ij}) in which $i = 1, \ldots, m$ and $j = 1, \ldots, n$, with:

$$x_{ij} = \begin{cases} 1 & \text{if } a_i R b_j \\ 0 & \text{otherwise} \end{cases}$$

The first sum is the row-wise sum (count row by row). The second sum is the column-wise sum (count column by column). Both give the cardinality. Of course, summing up all the elements of the matrix gives the same result. □

Example 2.6. *Define the following:*

$$\begin{aligned}
\tau(n) &= \text{ average number of divisors of an integer } k,\ 1 \leq k \leq n.\\
d(n) &= \text{ number of divisors of } n. \text{ Then:}\\
\tau(n) &= \frac{d(1) + \ldots + d(n)}{n}\\
&= \frac{1}{n}\sum_{i=1}^{n} d(i)\\
A = B &= \{1, \ldots, n\}\\
R &\subseteq A \times B : aRb \Rightarrow a|b.
\end{aligned}$$

The example for the integers 1 to 9 is shown in table 2.1. From this table it can be concluded that for $n = 6$, $\tau(n) = \tau(6) = \frac{7}{3}$.

n	1	2	3	4	5	6	7	8	9
$d(n)$	1	2	2	3	2	4	2	4	3

Table 2.1: The number of divisors of integers 1 to 9

Based on the definitions, the given example can be extended into the following more general rules:

$$\begin{aligned}
n \text{ prime} &\Rightarrow d(n) = 1\\
n = p^e, p \in \mathbb{P}, e \in \mathbb{N}^+ &\Rightarrow d(n) = e + 1\\
n = \prod_{i=1}^{k} p_i^{e_i} &\Rightarrow d(n) = \prod i = 1^k(e_1 + 1).
\end{aligned}$$

From here it follows that $l|n$ *if and only if* $l = \prod_{i=1}^{n} p_i^{f_i}, f_i \leq e_i$, *for some* $f_i \leq e_i$, *where* l *is defined by* $(f_1, \ldots, f_k)$. *Now it follows that:*

$$\begin{aligned}
\tau(n) &= \frac{1}{n}\sum_{i=1}^{n} d(i)\\
&= \frac{1}{n}\sum_{j=1}^{n} |R_{0,j}| && \text{sum of the columns}\\
&= \frac{1}{n}\sum_{i=1}^{n} |R_{i,0}| && \text{sum of the rows. Where:}\\
R_{0,j} &= \{a \mid aRj\} = d(j)\\
R_{i,0} &= \{b \mid iRb\} && \text{sum of the number of multiples of } i \text{ in } b.
\end{aligned}$$

With this, $\tau(n)$ can be calculated as follows:

$$\begin{aligned}\tau(n) = \ldots &= \frac{1}{n}\sum_{i=1}^{n}\left\lfloor\frac{n}{i}\right\rfloor \\ &= \frac{1}{n}\sum_{i=1}^{n}\left(\frac{n}{i} - \underbrace{\left\{\frac{n}{i}\right\}}_{\textit{fractional part}}\right) \\ &= \sum_{i=1}^{n}\frac{1}{i} - \frac{1}{n}\sum_{i=1}^{n}\underbrace{\left\{\frac{n}{i}\right\}}_{\leq 1} \\ &= \mathcal{H}_n + \mathcal{O}(1) \sim \ln(n).\end{aligned}$$

Where $\mathcal{H}$ are the ***harmonic numbers****.*

Pigeon hole principle: Let $A_1, \ldots, A_k$ be finite pairwise disjoint sets, $|A_1 \cup \ldots \cup A_k| > k \cdot r$, for $r \in \mathbb{N}$, this implies: $\exists i : |A_i| > r$. If $r = 1$, then it follows that:

$$f : A \mapsto B, |A| > |B| \Rightarrow \exists b \in B : |f^{-1}(b)| \geq 2.$$

Where $|f^{-1}(b)|$ is the set of pre-images and f is not injective.

Example 2.7. Claim: there are two people, living in Austria, who are born in the same hour, of the same day, in the same year.

Take as the maximal age 200 (in that case everyone in Austria is counted), there are 365 days, with each 24 hours. Then it follows:

$$365 \cdot 24 \cdot 200 < 2 \cdot 10^6.$$

The Austrian population is bigger than that!

Example 2.8. For all odd numbers q: $\exists i : q|2^i = 1 =: a_i$.

If $\exists i : a_i \equiv 0 \mod q$, the proof is done. Consider $a_1, a_2, \ldots a_q \mod q$. Either $\exists i : a_i \equiv 0 \mod q$ or $\exists i, j : i < j, a_i \equiv a_j \mod q$. By the pigeon hole principle, without 0, there are only $q - 1$ residue classes left. Assume that $i < j$:

$$\begin{aligned} a_i - a_j &= q \cdot a && a \in \mathbb{Z} \\ 2^i(1 - 2^{j-i}) &= q \cdot a. \end{aligned}$$

Since q is odd: $gcd(2^i, q) = 1$, which implies that $q|2^{j-i} - 1$ and $2^{j-i} - 1 = a(j - i)$. But then $a_{j-i} \equiv 0$, which is what is needed.

Example 2.9 (Interpreting the pigeon hole principle as a coloring)**.** Let A be a set with $|A| = n$. Define: $l_1, l_2, \ldots, l_k \geq 1$ and $n > l_1 + l_2 + \ldots + l_k - k$. Then, by the pigeon hole principle, for each coloring of the elements of A with colors $1, 2, \ldots, k$, there is an i such that l_i elements have the color i.

Let $f : A \mapsto \{1, 2, \ldots, k\}$ be a mapping. Assume $|f^{-1}|$ is the number of elements having the color $i < l_i$, $\forall i = 1, 2, \ldots, k$. Then:

$$n = |A| = \sum_{i=1}^{k} |f^{-1}(i)| \leq l_1 + \ldots + l_k - k.$$

However, this is a contradiction and hence proofs this example.

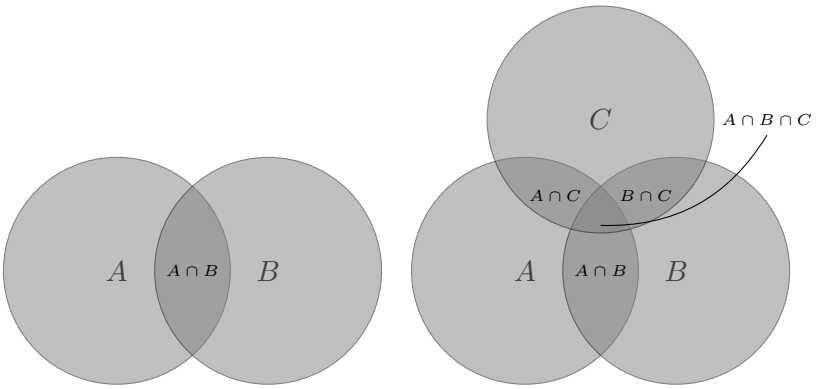
Principle of inclusion and exclusion: Given two non-disjoint sets A and B, it might be interesting to know the cardinality of $|A \cup B|$. Since the sets are non-disjoint, just adding the cardinalities of both sets, counts the elements of $A \cap B$ twice. In order to calculate the cardinality of $|A \cup B|$ correctly, $|A \cap B|$ has to be subtracted from $|A| + |B|$ once:

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Now consider three sets, that are all overlapping: A, B and C. Again, just adding the cardinalities of those three sets will count some elements twice or even three times!

This time it is not enough to subtract just the intersections of each two sets, because then $A \cap B \cap C$ is not counted at all. This gives the following:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$



(a) 2 sets (b) 3 sets

Figure 2.1: Principle of inclusion and exclusion

What about the general case? For pairwise disjoint sets it is known that:

$$\begin{aligned} |A_1 \cup \ldots \cup A_n| &= |A_1| + \ldots |A_n| \\ &= \sum_{\varnothing \neq I \subseteq \{1,\ldots,n\}} (-1)^{|I|+1} \left| \bigcap_{i \in I} A_i \right|. \end{aligned}$$

If there is a universe A, such that: $A_1, \ldots, A_n \subseteq A$, where the sets are not necessarily pairwise

disjoint, then:

$$A_1, \ldots, A_n \subseteq \left| A \backslash \bigcap_{i=1}^{n} A_i \right| = |A| + \sum_{\varnothing \neq I \subseteq \{1,\ldots,n\}} (-1)^{|I|} \left| \bigcap_{i \in I} A_i \right|$$
$$= \sum_{I \subseteq \{1,\ldots,n\}} (-1)^{|I|} \left| \bigcap_{i \in I} A_i \right|.$$

2.1.2 Counting Sets

Given a finite set $A = \{a_1, \ldots, a_n\}$. A counting set is a set A such that: $A = \{1, 2, \ldots, n\}$. There are six basic problems:

1. The number of permutations: $n!$
2. The number of k subsets: $\binom{n}{k}$
3. The number of ordered k-subsets: $k \cdot \binom{n}{k}$
4. The number of k-multisets, (in which the arguments can be used more than once): $\binom{n+k-1}{k}$. *Proof:* $b_1, \ldots, b_k \in A$, the order does not matter. There is a mapping f, that maps the k-multiset $\subseteq A$: $b_1, \leq \ldots \leq b_k$ to the k-multiset$\subseteq \{1, 2, \ldots, n+k-1\} : b_1 < b_2 + 1 < \ldots < b_k + k - 1$.
5. The number of arrangements of the multiset $\{b_1, \ldots, b_1, b_2, \ldots, b_2, \ldots, b_m, \ldots, b_m\}$, where b_1 appears k_1 times and k_i are all the elements b_i. Then there are $\frac{n!}{k_1! k_2 \ldots k_m!}$ permutations of this multiset.
6. The number of ordered k-multisets over A: n^k. (Take a fixed number of positions k and for each position choose any element from A).

The total number of subsets of the set A is: $\sum_{k=0}^{n} \binom{n}{k} = 2^n$. There are some important identities that are used often when counting sets:

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$
$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$$
$$\sum_{m=0}^{n} \binom{m}{k} = \binom{n+1}{k+1}$$
$$\binom{n}{k} = \binom{n}{n-k}$$
$$\sum_{k=0}^{n} \binom{m+k}{k} = \binom{m+n+1}{n}$$
$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \qquad \forall n \in \mathbb{N}, \forall x, y \in \mathbb{C}$$
$$\binom{n}{k} = \frac{n(n-1)\ldots(n-k+1)}{k!} \qquad \text{This also holds if } n \in \mathbb{C}.$$

Lemma 2.1. $\forall k \in \mathbb{N}$, $\forall x \in \mathbb{C}$: $\binom{x}{k} = \binom{x-1}{k-1} + \binom{x-1}{k}$. *If* $k < 0$ *then* $\binom{x}{k} = 0$.

Theorem 2.1 (Vandermonde)**.** $\forall n \in \mathbb{N}$, $\forall x, y \in \mathbb{C}$ *and* $\forall k \in Z$*:*

$$\binom{x+y}{n} = \sum_{k=0}^{n} \binom{x}{k}\binom{y}{n-k}.$$

If $k < 0$ *then again:* $\binom{x}{k} := 0$*.*

Proof. Assume that $x, y \in \mathbb{N}$. Let X, Y be sets, such that $X \cap Y = \varnothing$, $|X| = x$ and $|Y| = y$. The left-hand side of the theorem is $\binom{x+y}{n}$, this is the number of n-subsets of $x + y$ elements, of $X \cup Y$. Choose any n-subset $A \subseteq X \cup Y$. Then $A = (A \cap X) \cup (A \cap Y)$. Where $|A \cap X| = k$ and $|A \cap Y| = n - k$.

The number of unions of the shape of the right-hand side of A is $\binom{x}{k}\binom{y}{n-k}$. For all possible k it is $\sum_{k=0}^{n}\binom{x}{k}\binom{y}{n-k}$. Let I be a finite set. Then for the left-hand side it follows:

$$\sum_{i \in I} p_i(x)y^i = \sum_{i \in I} \widetilde{p_i}(x) \cdot y^i.$$

Assume $x \in \mathbb{N}$ and assume it is fixed. Let Q_i denote a polynomial. Then: $Q_1(y) = Q_2(y)$, $\forall y \in \mathbb{C}$. It follows: $p_i(x) = \widetilde{p_i}(x)$, $\forall x \in \mathbb{N}$. □

2.1.3 Stirling Numbers

Let $A = \{1, 2, 3, \ldots, n\}$ be a set and let $\pi \in S_n$ be a permutation, where S_n is the symmetric group, such that: $|S_n| = n!$. This permutation π can be represented as follows:

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \pi(1) & \pi(2) & \pi(3) & \cdots & \pi(n) \end{pmatrix}$$

Example 2.10. Permutations on symmetric groups. *Take the set of the first seven positive integers and a possible permutation. A possible permutation is the following, 2-line representation:*

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 6 & 3 & 1 & 7 & 5 & 2 \end{pmatrix}$$

The second line is also called the word representation. Another way to represent the same permutation is the cycle representation: $(14)(3)(2657)$*. Fixpoints can be omitted, which means that the permutation is:* $(14)(2657)$*. With this permutations calculations can be carried out.*

More examples of permutations are:

- $(12) \in S_7$*, this is the same as:* $(12)(3)(4)(5)(6)(7)$*.*
- *A transposition is a permutation of just 2 elements.*
- *Take two cycles:* (12) *and* (13)*, both from* S_7*. Then this can also be written as:* $(12) \circ (13) = (132)$*.*

Every $\pi \in S_n$ is a product of cycles, even a product of transpositions, however, not unique. For example: $(14)(2657) = (14)(27)(25)(26)$.

The order within the cycle does not matter: $(2657) = (5726)$. Notice that for S_4: $(12)(3)(4) = (12) = (12)(12)(12) = (12)(34)(34)$.

The **canonical representation** is generated from the 2-line representation, the smallest element comes first. If additionally the representation is started with the largest last element first, the parentheses can be omitted.

Definition 2.1. *Let $s_{n,k}$ be the number of permutations of an n-set A, which has k cycles (a fixpoint counts as a cycle as well). Then $s_{n,k}$ are the* ***Stirling numbers of the first kind****.*

Remark:

$$\begin{aligned} s_{n,1} &= (n-1)! \\ s_{n,n-1} &= \binom{n}{2} \\ s_{n,n} &= 1 \\ s_{0,0} &= 1 \\ s_{n,0} = s_{0,k} &= 0 \qquad\qquad n,k \geq 1 \\ \sum_{k=0}^{n} s_{n,k} &= k!. \end{aligned}$$

It does not matter where in the cycle the permutation is started. However, the order of the cycle should always be the same.

Theorem 2.2. $\forall n,k > 0 : s_{n,k} = s_{n-1,k-1} + (n-1)s_{n-1,k}$.

Proof. Take a permutation $\pi(1\ldots)(\ldots)\ldots(\ldots) \in S_n$, with k cycles. The question is: how many such permutations are there? There are two options:

1. 1 is a fixed point (it is always mapped to itself). In this case this cycle can be removed, which leaves: $s_{n-1,k-1}$.
2. 1 is not a fixed point. Start with a permutation of $n-1$ elements and add the element 1 to one of the cycles. This can be inserted before any of the $n-1$ elements. Then there are $(n-1)s_{n-1,k}$ possibilities.

□

Remark: Let $c_{n,k} = (-1)^{n+k}s_{n,k}$. These are the **signed Stirling numbers of the first kind**, $s_{n,k}$ are the **signless Stirling numbers**.

Definition 2.2. *Let $A = \{1,2,\ldots,n\}$ and $A = A_1 \cup A_2 \cup \ldots \cup A_k$ such that $\forall i,j : A_i \cap A_j = \varnothing$. The number of set partitions of A, with k blocks (a k-partition) is denoted by: $S_{n,k}$. These numbers are called the* ***Stirling numbers of the second kind****.*

Remark:

$$\begin{aligned} S_{n,1} = S_{n,n} &= 1 \\ S_{n,2} &= 2^{n-1} - 1 \\ S_{n,n-1} &= \binom{n}{2} \\ S_{0,0} &= 1 \\ S_{n,0} = S_{0,k} &= 0 \qquad\qquad \forall n, k \geq 1 \end{aligned}$$

Example 2.11. *Let $A = \{1, 2, 3, 4\}$, then:*

$$\begin{aligned} S_{4,1} &= 1 \\ S_{4,2} &= 7 \\ S_{4,3} &= 6 \\ S_{4,4} &= 1 \end{aligned}$$

Theorem 2.3. $S_{n,k} = S_{n-1,k-1} + k \cdot S_{n-1,k}$.

Proof. This proof will be similar to the proof with the Stirling numbers of the first kind. The proof exists of two parts.

1. If $\{1\}$ is a block, then it follows: $S_{n-1,k-1}$.
2. If $\{1\}$ is not a block, then 1 is part of one of the k blocks, with at least one other element in the same block. This means: $k \cdot S_{n-1,k}$.

□

Theorem 2.4. $\forall x \in \mathbb{C}$, $\forall n \geq 0$*:*

$$\begin{aligned} x_0 &:= 1 \\ (x)_n &:= x(x-1)(x-2)\dots(x-n+1) = \sum_{k=0}^{n} (-1)^{n+k} s_{n,k} x^k \\ x^n &= \sum_{k=0}^{n} S_{n,k} (x)_k. \end{aligned}$$

Remark: Let $V_n = \{a_0 + a_1 x + \ldots + a_n x^n \mid a_i \in \mathbb{C}\}$. Then $(V_n, +, \mathbb{C})$ is a vectorspace with dimension: $n + 1$. Now: $\{1, x, x^2, \ldots, x^n\}$ and $\{1, (x)_1, (x)_2, \ldots, (x)_n\}$ are bases of V_n.

Proof.

$$\begin{aligned}
(x)_n &= (x)_{n-1}(x-n+1) \\
&= (x-n+1)\cdot\sum_{k=0}^{n-1}(-1)^{n-1+k}s_{n-1,k}x^k \\
&= \sum_{k=0} n-1(-1)^{n-1+k}s_{n-1,k}x^{k+1} + (n-1)\sum_{k=0}^{n}(-1)^{n+k}s_{n-1,k}x^k \\
&= \sum_{k=0}^{n}(-1)^{n+k}s_{n-1,k-1}x^k + (n-1)\sum_{k=0}^{n}(-1)^{n+k}s_{n-1,k}x^k \\
&= \sum_{k=0}^{n}(-1)^{n+k}(s_{n-1,k-1} + (n-1)s_{n-1,k})x^k \\
&= \sum_{k=0}^{n}(-1)^{n+k}s_{n,k}x^k. \qquad \square
\end{aligned}$$

2.2 Generating Functions

Generating functions provide a tool for coping with combinatorial enumeration problems. The ordinary generating function defines the sum of a sequence:

$$(a_n)_{n\geq 0} = \sum_{n\geq 0} a_n z^n.$$

Such a sequence is in most cases defined on $\mathbb{R}$ or even $\mathbb{N}$. The definition above is the decoding of the sequence, as a formal power series. Some operations:

- **Addition:** $\sum_{n\geq 0}(a_n + b_n)z^n$.
- **Multiplication:** $\sum_{n\geq 0}\sum_{k=0}^{n} a_k b_{n-k} z^n$, the **Cauchy product**.
- **Division:** If $b_0 \neq 0$, then:
$$\frac{\sum a_n z^n}{\sum b_n z^n} = \sum c_n z^n.$$
- **Limit:** If it is given that:
$$(*) = \sum_{n\geq 0} a_n z^n = \lim_{n\to\infty}\sum_{k=0}^{n} a_k z^k$$
and $(*)$ is convergent ($(*) < \infty$), then the domain of the convergence is a disk with its center (0,0), the origin. The **radius of the convergence** is R:
$$R = \frac{1}{\overline{\lim}\sqrt[n]{|a_n|}} \in [0,\infty].$$

Theorem 2.5. *Let $f(x) = \sum a_n(z-z_0)^n, a_i \in \mathbb{C}$ and $R = \frac{1}{\overline{\lim}\sqrt[n]{|a_n|}}$. Then:*

1. *$|z-z_0| < R$ implies $f(x)$ is absolutely convergent, i.e., $\sum |a_n|(z-z_0)^n$ converges.*
2. *$|z-z_0| > R$ implies $f(z)$ is divergent.*

Example 2.12.

$$\sum_{n\geq 0} z^n = \frac{1}{1-z} \qquad \text{for } |z|<1, R=1, \text{ only in disk of convergence}$$

$$\sum_{n\geq 0} \frac{z^n}{n!} = e^z \qquad R=\infty$$

$$\sum_{n\geq 0} n! z^n \qquad R=0$$

The first example shows a function description everywhere on the plain, the second one nowhere on the plain.

Inside the disk of convergence the ***uniform convergence*** *allows the interchange of limits. It is also possible to differentiate and integrate with these functions:*

$$\frac{1}{(1-z)^2} = \left(\frac{1}{1-z}\right)' = \left(\sum_{n\geq 0} z^n\right)' = \sum_{n\geq 1} n z^{n-1}$$

Theorem 2.6 (Identity theorem for power series)**.** *Let $f(z) = \sum_{n\geq 0} a_n$, where $f(z)$ converges for $|z-z_0|<\epsilon$. The coefficients a_n are unique and satisfy $a_n \frac{f^{(n)}(z_0)}{n!}$. Notice that $f(z)$ is a Taylor series!*

Corollary 2.1.

$$\sum a_n (z-z_0)^n = \sum b_n (z-z_0)^n \text{ for } |z-z_0|<\epsilon \text{ implies: } a_n = b_n.$$

Since $f(z)$ generates the sequence (a_n) by continued differentiation and evaluation, $f(z)$ is called the ***generating function****. In particular:*

$$\sum a_n z^n \text{ is an } \textbf{\textit{ordinary generating function}}$$

$$\sum a_n \frac{z^n}{n!} \text{ is an } \textbf{\textit{exponential generating function}}$$

2.2.1 Operations on Generating Functions

Let sequence $(a_n)_{n\geq 0}$ correspond to the function: $\sum_{n\geq 0} a_n z^n = A(z)$ and $(b_n)_{n\geq 0}$ correspond to $B(z)$, observe that this is a linear process. Define the following operations:

1. **Addition:**
$$(\alpha a_n + \beta b_n)_{n\geq 0} \leftrightarrow \alpha A(z) + \beta B(z), \forall \alpha, \beta \in \mathbb{C}.$$
2. **Multiplication:**

$$\left(\sum_{k=0}^{n} a_k b_{n-k}\right) \leftrightarrow A(z)B(z) \text{ in particular: } \left(\sum_{k=0}^{n} a_k\right)_{n\geq 0} \leftrightarrow \frac{1}{1-z} A(z).$$

Remark:

$$\hat{A}(z) = \sum_{n\geq 0} a_n \frac{z^n}{n!}$$

$$\hat{B}(z) = \sum_{n\geq 0} b_n \frac{z^n}{n!}$$

$$\left(\sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k}\right)_{n\geq 0} \leftrightarrow \hat{A}(z)\hat{B}(z).$$

3. $(a_n\gamma^n)_{n\geq 0} \leftrightarrow A(\gamma z)$.
4. $(a_{n-1})_{n\geq 1} \leftrightarrow zA(z)$,

$$(a_{n+1})_{n\geq 0} \leftrightarrow \frac{A(z)-a_0}{z}$$

and for exponential generating functions (EFG):

$$(a_{n+1})_{n\geq 0} \leftrightarrow \hat{A}'(z).$$

5. $(na_n)_{n\geq 0} \leftrightarrow zA'(z)$.

Example 2.13.

$$\sum_{n\geq 0}(-1)^n z^n = \frac{1}{1+z} \quad \textit{for } |z|<1$$

$$\sum_{n\geq 0} n z^n = \frac{z}{(1-z)^2} = z\left(\frac{1}{1-z}\right)'$$

$$\sum_{n\geq 0}\binom{\alpha}{n} z^n = (1+z)^\alpha \quad \forall \alpha \in \mathbb{C}$$

$$a_n = \sum_{k\geq 0}^{n} k \textit{ then:}$$

$$\sum_{n\geq 0} a_n z^n = \sum_{n\geq 0}\left(\sum_{k=0}^{n} k\right) z^n = \sum_{n\geq 0}\left(\sum_{k=0}^{n} k\cdot 1\right) z^n = \left(\sum_{n\geq 0} n z^n\right)\left(\sum_{n\geq 0} 1\cdot z^n\right)$$

$$= \frac{z}{(1-z)^3} = \frac{1}{2}\cdot z\left(\frac{1}{1-z}\right)''$$

$$= \frac{z}{2}\sum_{n\geq 0} n(n-1)z^{n-2} = \sum_{n\geq 0}\frac{(n+1)n}{2} z^n = \sum_{n\geq 0}\binom{n+1}{2} z^n$$

$$a_n = \binom{n+1}{2}.$$

Lemma 2.2.

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

This can be proven using $(1+z)^\alpha = \sum \binom{a}{n} z^n$ *and then using Taylor series:*

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

2.2.2 Recurrence Relations

Many problems, like the *Towers of Hanoi* and the *Fibonacci sequence* can be described with recurrence relations.

Example 2.14. *Consider the* Towers of Hanoi *problem with n disks. How many steps are needed to move the disks? Notice that $a_0 = 0$ and $a_1 = 1$. For the $n+1$-th step, put n disks to a temporary location, then move the $n+1$-th disk and then move the n disks again. So in general it holds:*

$$\begin{aligned} a_{n+1} &= 2a_n + 1 \\ a_n &= 2^n - 1 \\ A(z) &= \sum_{n\geq 0} a_n z^n. \end{aligned}$$

Now multiply both sides with z^{n+1} and sum up over n. This results in the following:

$$\begin{aligned} \sum_{n\geq 0} a_{n+1} z^{n+1} &= 2\sum_{n\geq 0} a_n z^{n+1} + \sum_{n\geq 0} z^{n+1} \\ A(z) - a_0 &= 2zA(z) + \frac{z}{1-z} \\ A(z) &= 2zA(z) + \frac{z}{1-z} \\ &= \frac{z}{(1-z)(1-2z)} \\ &= \frac{\alpha}{1-z} + \frac{\beta}{1-2z} \\ &= \frac{-1}{1-z} + \frac{1}{1-2z} \\ &= -\sum_{n\geq 0} z^n + \sum_{n\geq 0} 2^n z^n \\ &= \sum_{n\geq 0} (2^n - 1) z^n \end{aligned}$$

Example 2.15. *From the* Fibonacci sequence *it is known that: $F_0 = 0$, $F_1 = 1$ and that $F_{n+2} = F_{n+1} + F_n$. From this, the following can be derived:*

$$\begin{aligned} F(z) &= \sum_{n\geq 0} F_n z^n \\ F(z) - F_0 - F_1 z &= z\left(F(z) - F_0\right) + z^2 F(z) \\ \textit{This implies: } F(z) &= \frac{z}{1-z-z^2} \\ &= \frac{-z}{(z-z_1)(z-z_2)} \qquad\qquad z_{1,2}\frac{-1\pm\sqrt{5}}{2} \\ &= \frac{1}{\sqrt{5}} \cdot \frac{1}{1-\frac{1+\sqrt{5}}{2}\cdot z} - \frac{1}{\sqrt{5}} \cdot \frac{1}{1-\frac{1-\sqrt{5}}{2}\cdot z} \\ \textit{This implies: } F(z) &= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right). \end{aligned}$$

In the more general case: take the sequence $a_{n+k} + q_1 a_{n+k-1} + \ldots + q_k a_n = 0$ and call it $(*)$, for $n \geq 0$. The sequence $(*)$ is unique if the first k elements: $a_0, a_1, \ldots, a_{k-1}$ are known. The q_i are given constants (independent of n). Then:

$$\begin{aligned}
A(z) &= \sum_{n\geq 0} a_n z^n \\
&\quad \sum_{n\geq 0} a_{n+k} z^{n+k} + q_1 \sum_{n\geq 0} a_{n+k-1} z^{n+k} + \ldots + q_k \sum_{n\geq 0} a_k z^{n+k} = 0 \\
A(z) &= a_0 - a_1 \cdot z - \ldots - a_{k-1} z^{k-1} + q_1 z \left(A(z) - \sum_{i=0}^{k-2} a_i z^i \right) + \ldots + q_z^k A(z) = 0 \\
A(z) &= \frac{p(z)}{1 + q_1 z + q_2 z^2 + \ldots + q_k z^k} \frac{p(z)}{q(z)} = \frac{p(z)}{\prod_{i=1}^{r} (z - z_i)^{\lambda_i}}.
\end{aligned}$$

Observe that $\deg(p) < \deg(q)$. Use the ansatz to solve the equation:

$$\begin{aligned}
\frac{p(z)}{q(z)} &= \sum_{i=1}^{r} \sum_{j=1}^{\lambda_i} \frac{A_{ij}}{(z - z_j)^j} \\
&= \frac{A_{11}}{z - z_1} + \frac{A_{12}}{(z - z_1)^2} + \ldots + \frac{A_{1\lambda_i}}{(z - z_1)^{\lambda_i}} + \ldots
\end{aligned}$$

Notice that

$$\frac{A}{(z - z_i)^i} = \frac{A}{(-z_i)^i} \cdot \frac{1}{(1 - \frac{z}{z_i})^i}.$$

And hence, by looking at the coefficient of z^n the following can be computed:

$$\begin{aligned}
\sum_i \sum_j \frac{B_{ij}}{\left(1 - \frac{z}{z_i}\right)^j} &= \sum_i \sum_j B_{ij} \cdot \binom{n + j - 1}{j - 1} \cdot z_i^{-n} \\
&= \frac{\alpha}{1 - z} + \frac{\beta}{1 - 2z} + \frac{\gamma}{(1 - 2z)^2} + \frac{\delta}{(1 - 2z)^3}.
\end{aligned}$$

Now it follows that $[z^n]$ is a polynomial in n, with degree $j - 1$. From here it can be concluded that:

$$A(z) = \sum_{n\geq 0} \left(p_1(n) \left(\frac{1}{z_1} \right)^n + p_2(n) \left(\frac{1}{z_2} \right)^n + \ldots + p_i(n) \left(\frac{1}{z_i} \right)^n \right) z^n.$$

With the degree of: $p_i \leq \lambda_i + 1$.

Example 2.16. *Let $a_{n+2} - 4a_{n+1} - 4a_n = 0$, such that $n \geq 0$ and a_0 and a_1 are given and*

let $A(z) = \sum a_n z^n$. The goal is to compute $A(z)$, this can be done as follows:

$$\begin{aligned}
A(z) - a_0 - a_1 z - 4z(A(z) - a_0) - 4z^2 A(z) &= 0 && = (*)\\
(1 - 4z + 4z^2)A(z) &= a_0 + a_1 z - 4a_0 z\\
A(z) &= \frac{a_0 + (a_1 - 4a_0)z}{1 - 4z + 4z^2}\\
&= \frac{a_0 + (a_1 - 4a_0)z}{(1-2z)^2}\\
&= \frac{C}{1-2z} + \frac{D}{(1-2z)^2} && = (\circ)\\
a_0 + (a_1 - 4a_0)z &= C(1-2z) + D\\
[z^0] : a_0 &= C + D\\
[z^1] : a_1 - 4a_0 &= -2C.
\end{aligned}$$

Since a_0 and a_1 are known, it is possible to compute C and D and from there $A(z)$ can be calculated. With the found values of C and D, equation $(\circ)$ can be calculated:

$$\begin{aligned}
(\circ) &= C \cdot \sum_{n\geq 0} 2^n z^n + D \cdot \sum_{n\geq 0} (n+1) 2^n z^n\\
&= \sum_{n\geq 0} (2^n \cdot C + (n+1) \cdot 2^n D) z^n\\
&= \sum_{n\geq 0} (a_n) z^n\\
a_n &= 2^n \cdot C + (n+1) \cdot 2^n \cdot D.
\end{aligned}$$

If the right-hand side of the equation $(*)$ is not zero, but a function $f(n)$, it is called a ***inhomogeneous recurrence****. In that case, the equation $(*)$ becomes:*

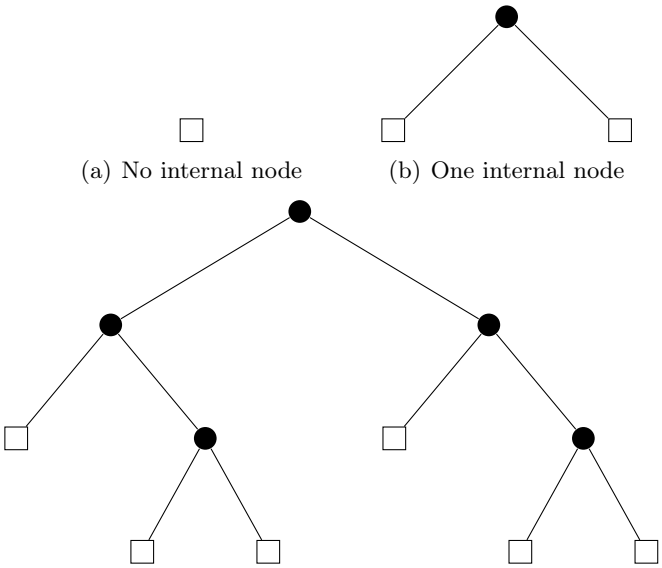
$$\sum f(n) z^{n+2} = F(z).$$

2.2.3 Unlabeled Combinatorial Structures

Example 2.17. *Take a complete binary tree. This means: without cycles, plane, rooted and every node has either no further children (external nodes, leaves) or two children (internal nodes). The internal nodes are denoted by $\circ$, the external nodes by $\square$. Assume this is a plain tree, which means: the left and right ordering does matter.*

Let a_n denote the number of binary trees with n internal nodes. If there are n internal nodes, then there are $n+1$ leaves. Notice that with that, it can be concluded that the number of vertices in a binary tree is always odd: $(n + (n+1))$.

A binary tree can be described recursively. The root node has two binary trees as its children: B and B'. Assume the tree has size $n+1$ and that the left child, binary tree B, has size k. Then the right child, binary tree B' has size $n-k$. A binary tree can also be described with



(a) No internal node (b) One internal node

(c) 5 internal nodes

Figure 2.2: Binary trees

generating functions:

$$
\begin{aligned}
a_0 &= 1 \\
a_{n+1} &= \sum_{k=0}^{n} a_k a_{n-k} \\
A(z) &= \sum a_n z^n \\
A(z) - 1 &= zA(z)^2 && \textit{(Cauchy Product)} \\
A(z) &= \frac{1 \pm \sqrt{1-4z}}{2z} \\
&= \frac{1 \pm (1-2z)^{\frac{1}{2}}}{2z} && \textit{Use "-", "+" is no option here.}
\end{aligned}
$$

Since $(1+z)^\alpha = \sum_n \binom{\alpha}{n} z^n$ *it follows that:*

$$
\begin{aligned}
(1-4z)^{\frac{1}{2}} &= \sum_{n\geq 0} \binom{\frac{1}{2}}{n} (-4)^n z^n \\
&= -\sum_{n\geq 0} \frac{\frac{1}{2}(-\frac{1}{2})(-\frac{3}{2})\dots(\frac{1}{2}-n+1)}{n!} \cdot (-4)^n z^n \\
&= \sum_{n\geq 0} \underbrace{\frac{1}{n+1}\binom{2n}{n}}_{\textbf{\textit{Catalan numbers}}} z^n.
\end{aligned}
$$

In a binary tree, the number of internal nodes is: $a_n = \frac{1}{n+1}\binom{2n}{n}$. *Then* $A(z) = 1 + zA(z)^2$, *which can be solved. A tree, from the set of binary trees* B *exists of either a leaf, with size 0 (only one node:* $\square$*) or a root node* $\circ$ *and two binary trees as its children.*

Example 2.18. Given a bin with red, blue and yellow balls. The following is known: there are 2 or 3 red balls, at least one blue ball and not more than one yellow ball. What is the number of combinations of n balls?

Introduce variable names for each color: r, b and y respectively. The following holds: $r^2 + r^3$ for the red balls, $1 + y$ for the yellow balls and $b + b^2 + \ldots = \frac{b}{1-b}$ for the blue balls. There are 2 configurations:

$$\begin{aligned} A(z) &= \sum a_n z^n \\ B(z) &= \sum b_n z^n \\ \textit{General: } &= \sum_{k=0}^{n} a_k b_{n-k}. \end{aligned}$$

Let z be the total number, then the generating function of these configurations is:

$$(r^2z^2 + r^3z^3)(1 + zy)\left(\frac{bz}{1 - bz}\right) = \sum a_{lmkn} r^l b^m y^k z^n.$$

Here the coefficient a_{lmkn} is the number of configurations $l \cdot r$, $m \cdot b$, $k \cdot y$ and n balls in total. Since the question is not about the number of balls with a specific color, but about the total number of used balls, set $r = b = y = 1$. This results in the function:

$$(z^2 + z^3)(1 + z)\frac{z}{1 - z}.$$

The number of combinations is:

$$\begin{aligned} [z^n]\frac{z^3(1+z)^2}{1-z} &= [z^{n-3}]\frac{(1+z)^3}{1-z} \\ &= [z^{n-3}]\frac{1}{1-z} + 2[z^{n-4}]\frac{1}{1-z} + [z^{n-5}]\frac{1}{1-z}. \end{aligned}$$

For $n \geq 5$ it follows that $a_n = 4$, since $\frac{1}{1-z} = \sum_{m \geq 0} z^m$. Notice that $a_3 = 1$ and $a_4 = 3$.

Example 2.19. Given a set $M = \{1, 2, \ldots, N\}$. What is the number of combinations of size $k = \binom{N}{k}$?

Derive this number by the following generating functions:

$$a_1, a_2, \ldots, a_n \hat{=} \textit{ different balls } \hat{=} \textit{ elements of } M.$$

For all the elements holds: the element is taken, or it is not taken. This gives the following formula:

$$(1 + a_1)(1 + a_2)\ldots(1 + a_N).$$

Like with the balls, the element does not matter, it is about the number of elements, replace all a_i by x. This gives the following:

$$(1 + x)(1 + x)\ldots(1 + x) = (1 + x)^N = \sum \binom{N}{k} x^k.$$

If repetitions are allowed it follows that:

$$\prod_{i=1}^{N}(1+a_i+a_i^2+\ldots)=\prod_{i=1}^{N}\frac{1}{1-a_i}.$$

Set again $a_i = x$, the generating function is:

$$\begin{aligned} f(x) &= \prod_{i=1}^{N}\frac{1}{1-x}=\frac{1}{(1-x)^N}=(1-x)^{-N} \\ &= \sum_{k\geq 0}\binom{-N}{k}(-1)^k x^k \\ &= \sum_{k\geq 0}\binom{N+k-1}{k}x^k. \end{aligned}$$

2.2.4 Combinatorial Construction

Let $\mathcal{A}$ be a **combinatorial class**, a set of object. Define the size of such a class by the size function: $w : \mathcal{A} \to \mathbb{N}$. Let a_n denote the number of objects $x \in \mathcal{A}$, such that $w(x) = n < \infty$, $\forall n \in \mathbb{N}$. The generating function of $(\mathcal{A}, w)$ is the following:

$$A(z)=\sum_{n\geq 0}a_n z^n.$$

Two combinatorial classes, from combinatorial classes, with weight function are created: $(\mathcal{A}, w_{\mathcal{A}})$ and $(\mathcal{B}, w_{\mathcal{B}})$. Define the following operations:

1. **Combinatorial sum, $\mathcal{A}+\mathcal{B}$:** Assume that $\mathcal{A}\cap\mathcal{B}=\varnothing$. Then:

$$\begin{aligned} \mathcal{A}+\mathcal{B} &= (\mathcal{A}\cup\mathcal{B}, w) \\ w(x) &= \begin{cases} w_{\mathcal{A}}(x) & x\in\mathcal{A} \\ w_{\mathcal{B}}(x) & x\in\mathcal{B} \end{cases} \\ c_n &= a_n+b_n \text{ this implies:} \\ C(z) &= A(z)+B(z). \end{aligned}$$

2. **Combinatorial product, $\mathcal{A}\times\mathcal{B}$:** Define $\mathcal{C}=\mathcal{A}\times\mathcal{B}=(\mathcal{A}\times\mathcal{B}, w)$, with:

$$w((x,y))=w_{\mathcal{A}}(x)+w_{\mathcal{B}}(y), x\in\mathcal{A}, y\in\mathcal{B}.$$

   Then:

$$c_n=\sum_{k=0}^{n}a_k b_{n-k}$$

   and $C(z)=A(z)B(z)$.

3. **Sequence of $\mathcal{A}$:** Define

$$seq(\mathcal{A})=\{(x_1,x_2,\ldots,x_k)\mid k\in\mathbb{N}, x_i\in\mathcal{A}\}$$

If $k = 0 \hat{=} \epsilon$ then it is the empty sequence. Define the size as:

$$w((x_1, \ldots, x_k)) = \sum_{i=1}^{k} w_{\mathcal{A}}(x_i).$$

Then:

$$\mathcal{C} = seq(\mathcal{A}) = \{\epsilon\} \cup \mathcal{A} \cup \mathcal{A} \times \mathcal{A} \cup \ldots$$
$$C(z) = 1 + A(z) + A(z)^2 + \ldots = \frac{1}{1 - A(z)}.$$

With the assumption that $a_0 = 0$.

Example 2.20 (Integer partitions)**.** *An integer can be decomposed into the sum of smaller integers. The order does not matter. If the order would matter, it would be a composition of integers. For example:*

$$5 = 3 + 1 + 1 = 1 + 3 + 1 = 2 + 2 + 1 = 1 + 1 + 1 + 1 + 1$$
$$5 = 4 + 1 = 3 + 2 = 3 + 1 + 1 = 2 + 2 + 1 = +2 + 1 + 1 + 1 = 1 + 1 + 1 + 1 + 1.$$

Let $\mathcal{C}$ define the compositions of an integer in $\mathbb{N}^+$. Then $\mathcal{C}$ is a sequence:

$$\mathcal{C} = seq(\mathcal{A})$$
$$\mathcal{A} = \mathbb{N}^+$$
$$w_{\mathcal{A}} = x$$
$$\underline{x} = (x_1, x_2, \ldots, x_k) \in \mathcal{C}$$
$$\underline{x} \hat{=} x_1 + x_2 + \ldots + x_k$$
$$w(\underline{x}) = x_1 + \ldots + x_k.$$

Let $\mathcal{A} = seq((\{0\}) \backslash \{\epsilon\})$, where $\{0\} \leftrightarrow z$, from this it follows:

$$A(z) = \frac{1}{1 - z} - 1 = \frac{z}{1 - z}$$
$$C(z) = \frac{1}{1 - A(z)} = \frac{1 - z}{1 - 2z} = 1 + \sum_{n \geq 1} 2^{n-1} z^n.$$

For integer partitions it follows:

$$P(z) = \prod_{i \geq 1} \frac{1}{1 - x^i}$$
$$\mathcal{P} = seq(\{1\}) \times seq(\{2\}) \times \ldots$$

Example 2.21 (Strings composed of $\circ$ and $-$)**.** Suppose there is a string, composed with two signs: $\circ$ and $-$, where $\circ$ has length 1 and $-$ has length 2. What is the number of strings of length n?

Take the class $\mathcal{A} = \{\circ\}$ and $\mathcal{B} = \{-\} \hat{=} \mathcal{A} \times \mathcal{A}$. With generating functions z and z^2 respectively. Now:

$$\mathcal{C} = seq(A \cup A \times A)$$
$$C(z) = \frac{1}{1 - z - z^2} = \sum_{n \geq 0} F_n z^n.$$

Notice that this is the Fibonacci sequence again.

Example 2.22 (Binary trees)**.** *Let $\mathcal{B}$ be a binary tree, as defined above. Then this can also be written as:*

$$\mathcal{B} = \{\square\} + \{\circ\} \times \mathcal{B} \times \mathcal{B}$$
$$B(z) = 1 + z \cdot B(z) \cdot B(z).$$

2.2.5 Labeled Constructions

Example 2.23 (Permutations)**.** *Let $a_n = n!$, then*

$$A(z) = \sum_{n \geq 0} n! z^n.$$

A cyclic permutation, exists of exactly one cycle: $(p_1 p_2 \dots p_n) \hat{=} (p_3 p_4 \dots p_n p_1 p_2)$. Such that p_1 maps on p_2, p_2 on p_3 and so on, until p_n maps on p_1. The number of such cyclic permutations is therefore $(n-1)!$, with corresponding generating function:

$$B(z) = \sum (n-1)! z^n.$$

If there are two cycles in the permutation, the total number of permutations will be

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

The Cartesian product alone is not enough.

Definition 2.3. *Let $\mathcal{A}$ be a **labeled structure**. This means: each object of size n is composed of n atomic objects. The atoms are numbered with integers from 1 to n. The generating function is defined as follows:*

$$\hat{A}(z) = \sum_{n \geq 0} a_n \frac{z^n}{n!}$$

Define the following operations on these labeled structures:

1. **Sum, $\mathcal{A} + \mathcal{B}$:** Let $C = \mathcal{A} + \mathcal{B}$, with $\mathcal{A} \cap \mathcal{B} = \varnothing$. Then the weight function is defined as:

$$w(x) = \begin{cases} w_{\mathcal{A}}(x) & x \in \mathcal{A} \\ w_{\mathcal{B}}(x) & x \in \mathcal{B}. \end{cases}$$

   From there it follows that:

$$\hat{C}(z) = \sum_{n \geq 0} (a_n + b_n) \frac{z^n}{n!} = \hat{A}(z) + \hat{B}(z).$$

2. **Partitional product, $\mathcal{A} * \mathcal{B}$:** Let $\mathcal{C} = \mathcal{A} * \mathcal{B}$ then:

$$\mathcal{C} = \{(x, y) \mid x \in \mathcal{A}, y \in \mathcal{B}, \text{ atoms are labeled in order preserving way} \\ \text{s.t. the labels are } 1, 2, \dots, w_{\mathcal{A}}(x) + w_{\mathcal{B}}(x)\}$$

The question is: what is the number of objects of size n? This can be calculated as follows:

$$\begin{aligned} c_n &= \sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k} \\ \frac{c_n}{n!} &= \sum_{k=0}^{n} \frac{1}{k!(n-k)!} a_k b_{n-k} \\ &= \sum_{k=0}^{n} \frac{a_k}{k!} \cdot \frac{b_{n-k}}{(n-k)!} \\ &= \sum_{k=0}^{n} [z^k]\hat{A}(z)[z^{n-k}]\hat{B}(z) \\ \Rightarrow\ \hat{C}(z) &= \hat{A}(z)\hat{B}(z). \end{aligned}$$

3. **Sequence construction:** Let $seq(\mathcal{A}) = \{\epsilon\} \times \mathcal{A} \times (\mathcal{A} * \mathcal{A}) \times \ldots$. Then

$$\hat{C}(z) = \frac{1}{1 - \hat{A}(z)}.$$

4. **Set construction:** Let

$$set(\mathcal{A}) = \{\varnothing\} \times \mathcal{A} \times \frac{1}{2}\mathcal{A} * \mathcal{A} \times \frac{1}{3!}\mathcal{A} * \mathcal{A} * \mathcal{A}.$$

This implies: $\hat{C}(z) = e^{\hat{A}(z)}$. In the unlabeled case, for $set(\mathcal{A})$, $C(z)$ is defined as:

$$C(z) = \exp(\hat{A}(z)) = \exp\left(A(z) - \frac{A(z^2)}{2} + \frac{A(z^3)}{3} + \ldots\right).$$

5. **Cycles of objects of $\mathcal{A}$:** This is defined as:

$$cyc(\mathcal{A}) \cong \mathcal{A} + \frac{1}{2}\mathcal{A} * \mathcal{A} + \frac{1}{3}\mathcal{A} * \mathcal{A} * \mathcal{A} + \ldots.$$

With generating function:

$$\hat{C}(z) = \log\left(\frac{1}{1 - \hat{A}(z)}\right).$$

Example 2.24. *Let $\mathcal{P} = set(cyc(\{\circ\}))$, in $\mathcal{P}$ the order does not matter and $\circ$ is a labeled atom. Then it follows:*

$$\begin{aligned} \hat{P}(z) &= e^{\log\left(\frac{1}{1-z}\right)} = \frac{1}{1-z} \\ &= \sum_{n \geq 0} n! \frac{z^n}{n!}. \end{aligned}$$

Example 2.25. *Let $\mathcal{P}$ be a permutation, then $\mathcal{P} = set(cyc(\mathcal{A}))$ and $\mathcal{A} = \{1\}$, in which 1 is a labeled atom. Then it follows:*

$$\hat{P}(z) = exp\left(\log\left(\frac{1}{1-z}\right)\right) = \sum_{n \geq 0} n! \frac{z^n}{n!}.$$

Example 2.26. *Given a set partition: $\mathcal{M} = M_1 \cup \dots M_k$, such that $M_i \neq \varnothing$ and if $i \neq j$ then $M_i \cap M_j = \varnothing$. For the class of set partitions $\mathcal{P}$ it follows:*

$$\begin{aligned} \mathcal{P} &= set(set(\mathcal{A})\backslash\{\varnothing\}) \\ \hat{P}(z) &= exp(exp(z) - 1) \\ \textit{Which implies:} \quad [z^n]e^{e^z-1} &= \sum_{k\geq 0} S_{n,k}. \end{aligned}$$

2.2.6 Exponential Generating Functions and Ordered Structures

Take a look at ordered n-tuples: $(q_1, \dots, q_n)$, where $q_i \in \{1, 2, \dots, N\}$, with no repetitions. Then a_n is the number of n-tuples. Define:

$$Q = \underbrace{\{\epsilon, 1\}}_{1+z} * \underbrace{\{\epsilon, 2\}}_{1+z} * \dots * \underbrace{\{\epsilon, N\}}_{1+z}.$$

For the generating function it follows:

$$\begin{aligned} \sum_{n\geq 0} a_n \frac{z^n}{n!} = (1+z)^N &= \sum_{n=0}^{N} \binom{N}{n} z^n \\ a_n &= \frac{N!}{(N-n)!}. \end{aligned}$$

If repetitions were allowed it follows that:

$$\left(1 + z + \frac{z^2}{2!} + \frac{z^3}{3!} + \dots\right)^N = e^{zN} = \sum_{n\geq 0} N^n \frac{z^n}{n!}.$$

Chapter 3

Number Theory

3.1 Divisibility and Factorization

Definition 3.1. *Let $a, b \in \mathbb{Z}$, then $a|b$ if and only if $\exists c \in \mathbb{Z}$ such that $a \cdot c = b$. In general, let $a, b \in R$ in which R is a **ring** (e.g. polynomials $R = \mathbb{Z}[x]$), then $a|b$ if and only if $\exists c \in R$ such that $a \cdot c = b$.*

Definition 3.2. *Let $a, b \in \mathbb{Z}$, then $d = gcd(a, b)$ if and only if:*

- *$d|a$ and $d|b$.*
- *$t|a$ and $t|b$ implies: $t|d$.*

Notice that the greatest common divisor is not unique. For example: $gcd(2, 4) = \{2, -2\}$. In this definition as well: it is possible to replace $\mathbb{Z}$ by any ring R.

Definition 3.3. *Let $a, b \in \mathbb{Z}$, such that $b > 0$. Then $\exists q, r$ such that $a = b \cdot q + r$, with $0 \leq r < b$.*

Theorem 3.1 (Euclidean algorithm)**.** *Given a and b, what is the greatest common divisor of those two integers? The **Euclidean algorithm** is an algorithm that calculates the gdc of two integers. Look at the following sequence of equations:*

$$\begin{aligned} a &= bq_0 + r_0 \\ b &= r_0 q_1 + r_1 \\ r_0 &= r_1 q_2 + r_2 \\ &\vdots \\ r_{k-2} &= r_{k-1} q_k + r_k \\ r_{k-1} &= r_l q_{k_1} + 0. \end{aligned}$$

It follows, from the previous formulas, that $b > r_0 > r_1 > r_2 > \ldots > r_k > 0$. Hence: $r_k = gdc(a, b)$.

Proof. The proof consists of two parts:

1. Start with proving that r_k is indeed a common divisor of a and b:

$$r_k|r_{k-1} \Rightarrow r_k|\underbrace{r_{k-1}q_k + r_k}_{r_{k-2}} \Rightarrow \ldots \Rightarrow r_k|a \wedge r_k|b.$$

2. The second part is to show that this is the greatest common divisor. Does $t|a \wedge t|b$ imply $t|r_k$? Suppose that $t|a$ and $t|b$ it follows that $\Rightarrow t|\underbrace{a - bq_0}_{r_0} \Rightarrow t|r_1 \Rightarrow \ldots \Rightarrow t|r_k$.

□

Remark: If

$$r_j = r_{j+1} \cdot \underbrace{q_{j+2}}_{\geq 1} + r_{j+2} \geq \underbrace{r_{j+1}}_{> r_{j+2}} + r_{j+2} > 2r_{j+2}$$

then it follows that

$$\forall j : r_{j+2} < \frac{r_j}{2}.$$

Theorem 3.2. *Let $a, b \in \mathbb{Z}$ and suppose that $d = gcd(a, b)$. Then $\exists e, f \in \mathbb{Z}$ such that $d = ae + bf$.*

Proof. To prove the theorem: just reverse the Euclidean algorithm. □

Definition 3.4. *Let R be a **commutative ring**, with a 1-element. Then:*

- *$(R, +)$ is an **Abelian group**, which means: there is a 0-element and $\forall a$ there is an inverse $-a$.*
- *$(R, \cdot)$ is a **semigroup**, which means, there exists an neutral element 1 and the distributive laws hold.*
- *R is an **integral domain** if and only if $\nexists a, b \in R\backslash\{0\}$, such that $a \cdot b = 0$.*

Example 3.1. *$(\mathbb{R}, +, \cdot)$, $(\mathbb{Z}_m, +, \cdot)$, for $m \in \mathbb{P}$. Where $\mathbb{P}$ are the prime numbers and $\mathbb{Z}_m$ are the integers, modulo m.*

If $m \notin \mathbb{P}$ then $m = n \cdot k$ and $\overline{n} \cdot \overline{k} = \overline{m} = \overline{0}$. Take $m = 6$, then: $\mathbb{Z}_6 : \overline{2} \cdot \overline{3} = \overline{0}$. Furthermore:

$$\mathbb{Z}[x] = (\{a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \mid a_i \in \mathbb{Z}, n \in \mathbb{N}\}, +, \cdot).$$

Definition 3.5. *A ring R is called a **Euclidean ring** if R is an integral domain and there is a Euclidean function n: $n : R \to \mathbb{N}$ such that $\forall a, b \in R$ with $b \neq 0$ there exists $q, r \in R$:*

1. *$a = b \cdot q + r$ with $r = 0$ or $n(r) < n(b)$.*
2. *$\forall a, b \in R\backslash\{0\}$: $n(a) \leq n(a \cdot b)$.*

Definition 3.6. *A **field** $(K, +, \cdot)$ is a commutative group, with two operations: addition and multiplication, such that:*

- *$(K, +)$ is an Abelian group (it is associative, there is a 0-element and $\forall a$, $\exists -a$).*
- *$(K\backslash\{0\}, \cdot)$ is an Abelian group.*
- *The distributive laws hold.*

Example 3.2. *Take a look at the integers $\mathbb{Z}$, with $n(a) = |a|$. K is a field, such that*

$$K[x] = (\{a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \mid a_i \in K, n \in \mathbb{N}\}, +, \cdot).$$

Where n is the degree of the whole polynomial over ring K.

If $K[x]$ is a Euclidean ring, then for $p(x) \in K[x]$: $n(p(x)) = \deg(p(x))$.

Example 3.3.

$$\begin{array}{rrrrr|l}
x^4 & +3x^3 & -3x^2 & -7x & +6 & : (x^3 + x^2 - x + 15) = x + 2 \\
\cline{6-6}
-x^4 & -x^3 & +x^2 & -15x & & \\
\cline{1-4}
 & 2x^3 & -2x^2 & -22x & +6 & \\
 & -2x^3 & -2x^2 & +2x & -30 & \\
\cline{2-5}
 & & -4x^2 & -20x & -24 &
\end{array}$$

$$p(x) = (x+2) \cdot q + \underbrace{(-4x^2 - 20x - 24)}_{r(x)}$$

If $p(x), q(x) \in K[x]$, then $gcd(p(x), q(x)) = a \cdot d(x)$, for $a \in K[x] \backslash \{0\}$.

Definition 3.7. *Let $p \in \mathbb{Z}$ and $p > 1$. Now p is called a **prime number** if and only if ± 1 and $\pm p$ are the only divisors of p. The set of all prime numbers is denoted by $\mathbb{P}$.*

Theorem 3.3. *Let $p \in \mathbb{P}$. If $p|(a \cdot b)$ then $p|a \vee p|b$.*

Proof.

Case 1: $p|a$, then the proof is done.

Case 2: $p \nmid a$, then $gcd(p, a) = 1$, which means: $\exists e, f \in \mathbb{Z}$ such that $ep + fa = 1$. Now it follows that: $b = b \cdot 1 = \underbrace{bep}_{\text{multiple of } p} + \underbrace{bfa}_{\text{multiple of } p}$ from which it follows that $p|b$. □

Theorem 3.4. *Let $n \in \mathbb{N}^+$, then $\exists p_1, \ldots, p_r \in \mathbb{P}$ such that $n = p_1 \cdot \ldots \cdot p_r$, for $r \geq 0$. $\left(\prod_{i \in \varnothing} a_1 = 1\right)$.*

Proof. The proof will be by induction, with base case: $n \in \mathbb{P}$, in which case the proof follows immediately.

Now suppose $n \notin \mathbb{P}$. This means, $\exists n_1, n_2 \in \mathbb{Z}$ such that $n = n_1 \cdot n_2$, where $n_1, n_2 < n$. By induction hypothesis it follows that: $n_1 = p_1 \cdot \ldots \cdot p_r$ and $n_2 = q_1 \cdot \ldots \cdot q_s$. From which the proof follows. □

Definition 3.8. *$\nu_p(n)$ is the **multiplicity of p in the factorization of** n. From this the following follows:*

$$\begin{aligned}
p^{\nu_p(n)} &| n \\
p^{\nu_p(n)+1} &\nmid n \\
gcd(a, b) &= \prod_{p \in \mathbb{P}} p^{\min(\nu_p(a), \nu_p(b))} \\
lcm(a, b) &= \prod_{p \in \mathbb{P}} p^{\max(\nu_p(a), \nu_p(b))} \\
a|b &\Leftrightarrow \forall p \in \mathbb{P} : \nu_p(a) \leq \nu_p(b).
\end{aligned}$$

Notice that $\nu_p(x)$ might also be zero: not every prime number has to be a factor of an integer.

Remark: Factorization is unique up to the order of the factors. This implies:

$$n = \prod_{p \in \mathbb{P}} p^{\nu_p(n)}.$$

Theorem 3.5. *There are infinitely many prime numbers: $|\mathbb{P}| = \infty$.*

Proof. To get a contradiction, assume there are only finitely many prime numbers:

$$\mathbb{P} = \{p_1, \ldots, p_r\}.$$

Construct, from these prime numbers a new prime number: N, such that:

$$N = p_1 \cdot \ldots \cdot p_r + 1.$$

There are two possible cases:

1. N is a not yet known prime number, but that is a contradiction, since it is not part of the defined set $\mathbb{P}$.
2. It is possible to factor N into prime numbers. However, by construction of N, this is not possible: every element of $\mathbb{P}$ is certainly not a prime factor of N. But then should N be a new prime number. Which is again a contradiction.

Since in both cases a contradiction is derived, it follows that $\mathbb{P}$ contains not all the prime numbers: it is always possible to find a new prime number. □

3.2 Congruence Relations and Residue Classes

Definition 3.9. *Let $m \in \mathbb{N}^+$ be the modulus. Then a **residue class** is defined as: $a+m\cdot\mathbb{Z} = \overline{a}$. Where $a + m \cdot \mathbb{Z} = \{a + k \cdot m \mid k \in \mathbb{Z}\}$ notice: $\overline{a} \subseteq \mathbb{Z}$ and $\overline{a} = \overline{a+m}$.*

Remark:

$$a \in \overline{a}, \overline{a} \equiv \overline{b} \Leftrightarrow m|a-b$$
$$a \equiv b \mod m \Leftrightarrow m|a-b$$
$$a \equiv b(m) \Leftrightarrow \overline{a} = \overline{b}.$$

Furthermore:

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\} \Rightarrow \overline{0} \cup \overline{1} \cup \overline{2} \cup \ldots \cup \overline{m-1} = \mathbb{Z}.$$

Definition 3.10. *Let $\overline{a}$ and $\overline{b}$ be two residue classes then define the following two equivalences:*

$$\overline{a} + \overline{b} := \overline{a+b}$$
$$\overline{a} \cdot \overline{b} := \overline{a \cdot b}.$$

Remark: Let $a \equiv c(m)$ and $b \equiv d(m)$ then it follows that:

$$a + b \equiv c + d(m)$$
$$ab \equiv cd(m).$$

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

Figure 3.1: Definition of addition and multiplication in the binary residue classes

Example 3.4. *Take a look at the binary residue classes, the definition of addition and multiplication in those classes is defined as shown in figure 3.1.*

Theorem 3.6. *The structure $(\mathbb{Z}_m, +, \cdot)$ is a commutative ring, with a 1-element.*

Definition 3.11. *Let $\overline{a} \in \mathbb{Z}_m$. The inverse element is defined as follows: let $\overline{x} \in \mathbb{Z}_m$ such that: $\overline{x} \cdot \overline{a} = \overline{1}$. Then $\overline{x} = \overline{a}^{-1}$.*

Example 3.5. *Take $m = 5$, then $\overline{2}^{-1} = \overline{3}$. Now take $m = 6$, then $\overline{2} \cdot \overline{3} = \overline{0}$, which implies that $(\overline{x} \cdot \overline{2}) \cdot \overline{3} = \overline{0}$ and if: $\overline{x} \cdot \overline{2} \neq \overline{1}$ then $\nexists \overline{2}^{-1}$.*

Theorem 3.7. *Let $\overline{a} \in \mathbb{Z}_m$, then there exists an inverse element $\overline{a}^{-1}$ if and only if a and m are co-prime, which means: $gcd(a, m) = 1$.*

Proof. " $\Rightarrow$ " Let $\overline{a} \cdot \overline{x} = \overline{1}$ then $\exists k \in \mathbb{Z}$ such that $ax = 1 + km$, from which follows that: $ax - km = 1$. Let $d = gcd(a, m)$ then:

$$d | \underbrace{ax - km}_{1} \Rightarrow d = 1.$$

" $\Leftarrow$ " Now assume that $gcd(a, m) = 1$, then $\exists e, f \in \mathbb{Z}_m$ such that $ae + mf = 1$. From here it follows that: $ae = 1 + (-f)m$ and hence:

$$\overline{a} \cdot \overline{e} = \overline{1} \Rightarrow \overline{e} = \overline{a}^{-1}.$$ □

Definition 3.12. *Define the set of prime residue classes, modulo m as follows:*

$$\mathbb{Z}_m^* = \{\overline{a} \in \mathbb{Z}_m \mid gcd(a, m) = 1\}.$$

This set contains all invertible elements of $\mathbb{Z}_m$, which means it can also be defined as:

$$\mathbb{Z}_m^* = \{x \in \mathbb{Z}_m \mid \exists x^{-1} : x \cdot x^{-1} = 1\}.$$

*The set is sometimes also called the **group of units**.*

Example 3.6. *Start with $m = 5$ and $m = 6$ again. Then the prime residue classes are:*

$$\mathbb{Z}_5^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$$
$$\mathbb{Z}_6^* = \{\overline{1}, \overline{5}\}.$$

Example 3.7. *Look at the case where $m = 17$, the question is: what is the inverse element of 13? Start with $13x \equiv 1(17)$. Using the Euclidean algorithm it follows:*

$$17 = 13 \cdot 1 + 4$$
$$13 = 4 \cdot 3 + 1 \text{ then:}$$
$$\begin{aligned} 1 &= 13 - 4 \cdot 3 \\ &= 13 - (17 - 13) \cdot 3 \\ &= 17 \cdot 3 + 4 \cdot 13 \end{aligned}$$
$$x \equiv 4(17).$$

The solution to this problem is: $x \equiv 4(17)$ *which means that* $\overline{13}^{-1} = 4$.

Example 3.8. *Take a look at* $3b \equiv 3c(5)$*, to solve this: multiply both sides with 2, then divide by three. Since* $\overline{2}^{-1} = 3$ *it follows that the system becomes* $b \equiv c(5)$*, which can be solved.*

Example 3.9. *Now look at the system* $3b \equiv 3c(6)$*. Then* $\exists k \in \mathbb{Z}$ *such that:* $3b = 3c + k \cdot 6$*, divide both sides by three. This gives* $b = c + k \cdot 2$*, from which it follows that* $b \equiv c(2)$*, which can be solved.*

Some rules:

$$ab \equiv ac(am) \Rightarrow b \equiv c(m)$$
$$ab \equiv ac(m) \Rightarrow b \equiv c(m) \text{ if } ax \equiv 1(m) \text{ has a solution} \Leftrightarrow gcd(a, m) = 1.$$

3.3 Systems of congruences

Theorem 3.8. *Suppose* $m = m_1 \cdot m_2$ *and* $gcd(m_1, m_2) = 1$*. Then:*

$$x \equiv y(m) \Leftrightarrow \begin{cases} x \equiv y(m_1) \\ x \equiv y(m_2) \end{cases}$$

Proof. " $\Rightarrow$ " Since $x \equiv y(m) \Leftrightarrow x = y + k \cdot m$ it follows that $x = y + k \cdot m_1 \cdot m_2$ and hence

$$\begin{cases} x \equiv y(m_1) \\ x \equiv y(m_2) \end{cases}$$

" $\Leftarrow$ " Now assume that

$$\begin{cases} x \equiv y(m_1) \\ x \equiv y(m_2) \end{cases}$$

then $\exists l$ such that $x - y = l \cdot m_1 \equiv 0(m_2)$. From here it follows that if $l \equiv 0(m_2)$ then $x - y = l' \cdot m_1 \cdot m_2$ which implies: $x \equiv y(m)$. □

Corollary 3.1. *Let* $m = \prod_{i=1}^{r} m_i$ *such that* $\forall i \neq j : gcd(m_i, m_j) = 1$*. Then* $x \equiv y(m)$ *if and only if* $\forall i = 1, \ldots, r$*:* $x \equiv y(m_i)$*.*

Theorem 3.9 (Chinese remainder theorem)**.** *Given a system of congruence equations*

$$x \equiv a_i(m_i)$$

where $1 \leq i \leq r(*)$ *and if* $i \neq j$ *then* $gcd(m_i, m_j) = 1$*, then the system has a unique solution, modulo* $m = \prod_{i=1}^{r} m_i$*. The solution is given by:*

$$x \equiv \sum_{j=1}^{r} \frac{m}{m_j} \cdot b_j \cdot a_j(m).$$

Where $b_j = \left(\frac{m}{m_j}\right)^{-1} \mod m_j$.

Example 3.10. *Given the following system of congruence equations:*

$$3x \equiv 2(5)$$
$$2x \equiv 7(11).$$

It can be shown that this system is equivalent to:

$$x \equiv 4(5)$$
$$x \equiv 9(11).$$

From this system the following can be calculated:

$$m_1 = 5, m_2 = 11 \Rightarrow m = 55 \qquad b_1 \cdot 11 = 1(5) \Rightarrow b_1 = 1$$
$$a_1 = 4, a_2 = 9 \qquad b_2 \cdot 5 = 1 \Rightarrow b_2 = 9.$$

Then the solution to the whole system can be calculated as follows:

$$x \equiv 11 \cdot 1 \cdot 4 + 5 \cdot 9 \cdot 9(55)$$
$$x \equiv 449(55)$$
$$x \equiv 9(55)$$

The set of solutions is then:

$$\{\ldots, -46, 9, 64, 119, \ldots\}.$$

Proof. The proof exists of two parts: proving that x is indeed a solution and then proving that x is the unique solution modulo m:

1. x **is a solution:** It is known that the $m_i's$, for $i = 1, 2, \ldots, r$ are pairwise co-prime. This implies that $gcd\left(\frac{m}{m_j}, m_j\right) = 1$ which guarantees that $\exists b_j$ and $\forall i \neq j$: $\frac{m}{m_j} \equiv 0(m_i)$. This implies:

$$\sum_{j=1}^{r} \frac{m}{m_j} b_j \cdot a_j \equiv \frac{m}{m_j} \cdot \underbrace{\left(\frac{m}{m_j}\right)^{-1}}_{b_i} \cdot a_i(m_i) \mod m_i$$
$$\equiv a_i(m_i).$$

   This proves the existence of x.

2. x **is the unique solution, modulo** m**:** For all $i = 1, \ldots, r$ it holds that:

$$x \equiv a_i(m_i)$$
$$y \equiv a_i(m_i)$$
$$x \equiv y(m_i).$$

   Then it follows that $x \equiv y(m)$. This proves the whole theorem.

□

3.4 Euler-Fermat Theorem and RSA-Algorithm

Theorem 3.10. *Take a look at the group $(\mathbb{Z}_m^*)$, where $|\mathbb{Z}_m| = m$ and $\mathbb{Z}_m^* = \varphi(m)$. The function $\varphi(m)$ is **Euler's totient function**. E.g.: $\varphi(5) = 4$ and $\varphi(6) = 2$. Consider two cases for this function:*

1. *Suppose $m \in \mathbb{P}$ then $\varphi(m) = m - 1$.*
2. *Let $m = p^e$, for $p \in \mathbb{P}$ and $e \geq 1$. Now it holds that:*

$$\overline{a} \in \mathbb{Z}_m \Rightarrow gcd(a, p^e) = \begin{cases} 1 & \text{if } \overline{a} \in \mathbb{Z}_m^* \\ p^f & 1 \leq f < e \end{cases}$$
$$\overline{a} \in \mathbb{Z}_m^* \Leftrightarrow p \nmid a.$$

Now look at the first p^e natural numbers: $0, 1, 2, \ldots, p^e - 1$. Then

$$p^e - p^{e-1} = \varphi(p^e) = p^{e-1}(p-1) = \varphi(m).$$

And: $\varphi(m) = m\left(1 - \frac{1}{p}\right)$.

Theorem 3.11. *Let $m = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$ then:*

$$\varphi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_r}\right).$$

Proof. Let $r = 2$ and $M = \{1, 2, \ldots, m\}$, define two sets A and B as:

$$A = \{n \in M \mid p_1 | n\} = \{p_1, 2p_1, 3p_1, \ldots, m - p_1, m\}$$
$$B = \{n \in M \mid p_2 | n\} = \{p_2, 2p_2, 3p_2, \ldots, m - p_2, m\}.$$

Notice that $|M| = m$, $|A| = \frac{m}{p_1}$, $|B| = \frac{m}{p_2}$ and $|A \cap B| = \frac{m}{p_1 p_2}$. Then the totient function of m will be:

$$\begin{aligned} \varphi(m) &= |M \backslash (A \cup B)| \\ &= |M| - |A| - |B| + |A \cap B| \\ &= m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right). \end{aligned}$$

For the case that $r > 2$ the principle of inclusion and exclusion has to be applied. □

Theorem 3.12 (Theorem of Euler-Fermat)**.** *If $gcd(a, m) = 1$ then $a^{\varphi(m)} \equiv 1(m)$. In particular:*

$$p \in \mathbb{P}, p \nmid a \Rightarrow a^{p-1} \equiv 1(p).$$

*This is **Fermat's Little Theorem**.*

Proof. Let $\mathbb{Z}_m^* = \{\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_k\}$ and $k = \varphi(m)$. Multiply everything by $\overline{a}$, then the claim is that this gives the following set:

$$\mathbb{Z}_m^* \{\overline{a}\overline{a}_1, \overline{a}\overline{a}_2, \ldots, \overline{a}\overline{a}_k\}.$$

Since $\overline{a}\overline{a}_i = \overline{a}\overline{a}_j \Rightarrow \overline{a}_i = \overline{a}_j \Rightarrow i = j$ it follows that:

$$\underbrace{\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_k}_{\in \mathbb{Z}_m^*} = \overline{a}^k \cdot \underbrace{\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_k}_{\in \mathbb{Z}_m^*}.$$

Which implies that: $\overline{a}^k = \overline{1} = \overline{a}^{\varphi(m)}$. □

Theorem 3.13. *Let $p, q \in \mathbb{P}$ such that $p \neq q$ and both are odd. Let $m = p \cdot q$ and $v = lcm(p-1, q-1)$, then:*

$$\forall a, k \in \mathbb{Z} : a^{kv+1} \equiv a(m).$$

Proof. It has to be shown that $pq | a^{kv+1} - a$. This is the case, if and only if:

$$p \mid a^{kv+1} - a$$
$$q \mid a^{kv+1} - a.$$

There are two possible cases:

1. $p \mid a$, in this case the proof is done.
2. $p \nmid a$, then it follows that: $a^{p-1} \equiv 1(p)$ which implies $a^{kv} \equiv 1(p)$. Multiply both sides with a gives: $a^{kv+1} \equiv a(p)$. Do the same for q, then it follows that $a^{kv+1} \equiv a(m)$.

□

3.4.1 RSA-algorithm

Let $p, q \in \mathbb{P}$ such that $m = p \cdot q$ and $v = lcm(p-1, q-1)$ then

$$gcd(e, v) = 1 \Rightarrow \exists d : d \cdot e \equiv 1(v).$$

Suppose there is a message $a_1, a_2, a_3, \ldots$, with $0 \leq a_i < m$, that can be encrypted and decrypted as follows:

- **Encryption:** $E(a_j) = b_j := a_j^e \mod m$.
- **Decryption:** $D(b_j) = a_j := b_j^d \mod m$.

It can be shown that this really works:

$$\begin{aligned} b_j^d &\equiv (a_j^e)^d \mod m \\ &\equiv a_j^{e \cdot d} \mod m \\ &\equiv a_j^{kv+1} \mod m \\ &\equiv a_j \mod m. \end{aligned}$$

A public key (m, e) can be provided, this means: everyone can do the encryption. However a private key d is needed to decrypt the message. If someone, who does not have the private key, wants to decrypt the message, the right factorization of $m = p \cdot q$ has to be found. The time needed to find the factorization grows exponentially with the number of digits of m.

e-Signature: Let (e_j, d_j) be given, where e_j are public: e_j is public $\hat{=} E_j, D_j$. User i sends a message to user j as follows:

$$E_j(D_i(x)) = x^{d_i e_j}(m).$$

User j has the private key and can decrypt the message:

$$D_j(E_j(D_i(x))) = D_i(x).$$

Then for E_i holds afterward: $E_i(D_i(x)) = x$.

Caveat: (warning), (x) may have many fixed points. If the order is low, it is possible to find x.

Recall of some group-theory:

- **Group:** Let G be a group and $x \in G$, then $ord_G(x) = \min\{i \in \mathbb{N}^+ \mid x^i = e\}$. If e is the neutral element, then: $ord_G(e) = 1$, since $e^1 = e$. If $a \neq e$ it follows that $ord_G(a) > 1$.
- **Cyclic group:** Let $\langle x \rangle$ denote the group generated by x. For example:

  $$\langle e \rangle = \{e\} \text{ this is the trivial group}$$
  $$\langle x \rangle = \{e, x, x^2, x^3, \ldots\}.$$

  Suppose G is finite and let U be a subgroup of G: $U \leq G$, then $|U| \mid |G|$, where $|G|$ is the order of the group G. If$\langle x \rangle = \{e, x, \ldots, x^{ord_G(x)-1}\}$ then $|\langle x \rangle| = ord_G$, which implies: $ord_G(x) \mid |G|$.
  The group G is a cyclic group if and only if $\exists x \in G$ such that $\langle x \rangle = G$ if and only if $\exists x \in G : ord_G(x) = |G|$.
  Notice that a group is always a subgroup of itself: $G \leq G$.

Definition 3.13. *Let $\overline{a} \in \mathbb{Z}_m^*$, then $\langle \overline{a} \rangle = \mathbb{Z}_m^*$ is called a **primitive root mod** m. If $\overline{a}$ is a primitive root mod m, then*

$$\mathbb{Z}_m^* = \{\overline{a}, \overline{a}^2, \overline{a}^3, \ldots, \underbrace{\overline{a}^{\varphi(m)}}_{=1}\}.$$

Example 3.11.

$$\mathbb{Z}_2^* = \{\bar{1}\} = \langle \bar{1} \rangle$$
$$\mathbb{Z}_3^* = \{\bar{1}, \bar{2}\} = \langle \bar{2} \rangle = \{\bar{2}, \bar{2}^2\} = \{\bar{2}, \bar{1}\}$$
$$\mathbb{Z}_4^* = \{\bar{1}, \bar{3}\} = \langle \bar{3} \rangle$$
$$\mathbb{Z}_5^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\} = \langle \bar{2} \rangle = \langle \bar{3} \rangle \neq \langle \bar{4} \rangle = \{\bar{1}, \bar{4}\}$$
$$\mathbb{Z}_8^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\} \textit{ has no primitive roots } \Longrightarrow \mathbb{Z}_8^* \textit{ is not a cyclic group}$$
$$\langle \bar{1} \rangle = \{\bar{1}\} \quad \langle \bar{3} \rangle = \{\bar{3}, \bar{3}^2\} = \{\bar{3}, \bar{1}\}$$
$$\langle \bar{5} \rangle = \{\bar{5}, \bar{5}^2\} = \{\bar{5}, \bar{1}\}$$
$$\langle \bar{7} \rangle = \{\bar{7}, \bar{7}^2\} = \{\bar{7}, \bar{1}\}$$

Theorem 3.14. *$\mathbb{Z}_m^*$ is cyclic:*

$$\Leftrightarrow \exists \textit{ primitive root mod } m$$
$$\Leftrightarrow m \in \{2, 4\} \cup \{p^e \mid p \in \mathbb{P} \backslash \{2\}, e \geq\} \cup \{2p^e \mid p \in \mathbb{P}, e \geq 1\}.$$

Proof. Define: $\mathbb{Z}_p^* = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}$. Assume g is a primitive root mod p. Then:

$$\langle g \rangle = \mathbb{Z}_p^* \Leftrightarrow g^{p-1} \equiv 1(p) \wedge \forall 1 < r < p-1 : g^r \not\equiv 1(p).$$

This is an equivalent formulation for being a primitive root. Now define: $s : ord_{\mathbb{Z}^*_{p^2}}(g)$ which implies: $g^s \equiv 1(p^2)$. In particular this implies:

$$g^s \equiv 1(p) \Rightarrow s \geq p-1.$$

Claim: $g^{p-1} \equiv 1(p^2)$ or $(g+p)^{p-1} \not\equiv 1(p^2)$.

Proof of the claim: If $g^{p=1} \equiv 1(p^2)$ then $(g+p)^{p-1} \equiv g^{p-1} + p \cdot g^{p-2}(p^2)$, because all the other terms contain a factor p^2. It is known that $g^{p-1} = 1$. Now from $p \cdot g^{p-1}$ follows that $gcd(g,p) = 1$ which means $p \cdot g^{p-2} \neq 0(p^2)$ and hence $g^{p-1} + p \cdot g^{p-2} \neq 1$.

If $(g+p)^{p-1} \equiv 1(p^2)$ then $g^{p-1} + p \cdot g^{p-2} \equiv 1(p^2)$ and $g^{p-1} + p \cdot g^{p-2} \not\equiv 0$. Which implies that $g^{p-1} \not\equiv 1(p^2)$. This proves the claim. □

To complete the proof of the theorem both cases of the claim have to be considered:

1. Suppose $g^{p-1} \not\equiv 1(p^2)$ then $s \geq p$, where s denotes the order of gp^2. Note: $\varphi(p^2) = p(p-1)$ which implies that $s|p(p-1)$. Now $s = p-l$, where $p-1 = k \cdot l$ for $(k, l < p-1)$. Then $g^{p \cdot l} \equiv 1(p^2)$ and $g^{p \cdot l} = (g^p)^l \equiv g^l \equiv 1(p)$. This is a contradiction for $l < p-1$. From this contradiction it follows that $s = p(p-1)$ and hence: the order of g in $\mathbb{Z}^*_{p^2}$ is a generator of this group, with g a primitive root $\mod p^2$.
2. The proof of the case where $(g+p)^{p-1} \not\equiv 1(p^2)$ is similar to the first case. Again: $s = p(p-1)$. □

Lemma 3.1. *Let g be a primitive root mod p, for $p \in \mathbb{P}\backslash\{2\}$. Then either g or $g+p$ is a primitive root* $\mod p^e$*, for $e \geq 2$.*

Lemma 3.2. *Let h be a primitive root* $\mod p^e$*. Then h or $h + p^e$ is a primitive root mod $2p^e$.*

3.4.2 The Order of Elements of an Abelian Group G With Neutral Element e

Theorem 3.15. *If $ord(a) = r$, $ord(b) = s$ and $gcd(r,s) = 1$ then $ord(ab) = rs$.*

Proof. Take $(ab)^{rs}$, since this is an Abelian group, it is allowed to change the order. Then:

$$ab^{rs} = (\underbrace{a^r}_{e})^s(\underbrace{b^s}_{e}) = e.$$

Which implies that: $\underbrace{ord(ab)}_{n}|rs$. From here it follows that $e = (ab)^n = a^n b^n$ and then of course: $a^n = (b^{-1})^n$. Call the following equation $(*)$: $e = a^{r \cdot n} = (b^{-1})^{n \cdot r}$. But then: $(b^{-1})^k = e \Leftrightarrow b^k = e$, by $(*)$ it follows that $b^{n \cdot r} = e$. Since $n \cdot r$ is a multiple of $ord(b) = s$, $s|n \cdot r$ and hence $s|n$.

To prove that $r|n$, both a and b have to be changed. The proof is similar to the proof above. □

Corollary 3.2. *The following follows directly from the theorem above:*

$$ord(a^k) - ord(a) \Leftrightarrow gcd(k, ord(a)) = 1.$$

Theorem 3.16. *If $a, b \in G$, $ord(a) = r$ and $ord(b) = s$, then $\exists c \in G : ord(c) = lcm(r, s)$.*

Proof. Assume that for $e_i, f_i \geq 0$ the following holds:

$$r = \prod_{i \in I} p_i^{e_i}$$
$$s = \prod_{i \in I} p_i^{f_i}.$$

With these prime factorizations the lcm and the gdc of r and s can be expressed as:

$$lcm(r, s) = \prod_{i \in I} p_i^{\max(e_i, f_i)}$$
$$gcd(r, s) = \prod_{i \in I} p_i^{\min(e_i, f_i)}$$

A consequence of this is: $lcm(r, s) \cdot gcd(r, s) = r \cdot s$.

Define : $I_1 = \{i \in I \mid e_i \leq f_i\}$ and $I_2 = I \backslash I_1$. Then for r and s it holds:

$$r = \prod_{i \in I_1} p_i^{e_i} \cdot \prod_{i \in I_2} p_i^{e_i}$$
$$s = \prod_{i \in I_1} p_i^{f_i} \cdot \prod_{i \in I_2} p_i^{f_i}.$$

Define the integers d_1 and d_2 as:

$$d_1 = \prod_{i \in I_1} p_i^{e_i}$$
$$d_2 = \prod_{i \in I_2} p_i^{f_i}$$
$$d_1 \cdot d_2 = gcd(r, s).$$

Notice that in all cases the smaller component is taken. From these d_1 and d_2 it follows that:

$$ord(a^{d_1}) = \frac{r}{gcd(r, d_1)} = \frac{r}{d_1}$$
$$ord(b^{d_2}) = \frac{s}{gcd(s, d_2)} = \frac{s}{d_2}.$$

Observe that $gcd(\frac{r}{d_1}, \frac{s}{d_2}) = 1$, this follows from the definition of r and s with I_1 and I_2. Using this observation and the above theorem it follows that:

$$ord(a^{d_1} b^{d_2}) = \frac{rs}{d_1 d_2} = lcm(r, s).$$ □

Corollary 3.3. *Let $a_1, \ldots, a_r$ such that $ord(a_i) = k_i$. Then $\exists a \in G$ such that*

$$ord(a) = lcm(k_1, k_2, \ldots, k_r).$$

3.4.3 Carmichael Function

Definition 3.14. *The **Carmichael function** is defined as:*

$$\lambda(m) = \max\{\overline{a} \mid \overline{a} \in \mathbb{Z}_m^*\} \cdot ord_{\mathbb{Z}_m^*}(\overline{a}).$$

Remark

a) $\lambda(m) \mid \varphi(m)$

b) $p \in \mathbb{P}\backslash\{2\} \implies \lambda(p^e) = \varphi(p^e) = p^{e-1}(p-1)$
$\lambda(1) := \varphi(1) = 1$
$\lambda(2) = \varphi(2) = 1$
$\lambda(4) = \varphi(4) = 2$

c) $\lambda(2^e) = 2^{e-2}$ for $e \geq 3$
$\lambda(2^e) = ord_{\mathbb{Z}_{2^e}^*}(5)$

Take a look at the function $\lambda(n)$ for $n = \prod_{i=1}^{r} p_i^{e_i}$ with $e_i > 0$, these are the real prime factors of n. Let $a_i \in \mathbb{Z}_{p_i^{e_i}}^*$ such that there exists an element of maximal possible order:

$$ord(a_i) = \varphi(p_i^{e_i}) = \lambda(p_i^{e_i}).$$

Let $b_i \in \mathbb{Z}_n$ such that $b_i \equiv 1(p_j^{e_j})$, $\forall j \neq i$ and $b_i \equiv a_i(p_i^{e_i})$. Does such a b_i exist? The answer to this question follows from the *Chinese remainder theorem*: it exists.

Claim:

$$ord_{\mathbb{Z}_n^*}(b_i) = ord_{\mathbb{Z}_{p_i^{e_i}}^*}(b_i) = \lambda(p_i^{e_i})$$

Proof. For $b_i^k \equiv 1(n)$ it must be the case that, $\forall j = 1, \ldots, r$: $b_i^k \equiv 1(p_j^{e_j})$. Then:

$$b_i = c \cdot n + 1 = c \cdot c_1 \cdot p_j^{e_j} + 1.$$

For $j = i$ it holds that: $b_i^k \equiv a_i^k \equiv 1(p_i^{e_i})$. Take a look at the following:

$$k_{\min} = \lambda(p_i^{e_i}) \implies ord_{\mathbb{Z}_n^*}(b_i) \geq \lambda(p_i^{e_i})$$
$$b_i^{k_{\min}} \equiv 1(p_j^{e_j}) \quad \forall j \implies b_i^{k_{\min}} \equiv 1(n).$$

From here it can be concluded that both equations are true. Up until now the following has been found: $b_1, b_2, \ldots, b_r \in \mathbb{Z}_n$ such that $ord_{\mathbb{Z}_n^*}(b_i) = \lambda(p_i^{e_i})$, $\forall i = 1, \ldots, r$. This implies:

$$\exists b \in \mathbb{Z}_n^* : ord_{\mathbb{Z}_n^*}(b) = lcm(\lambda(p_1^{e_1}), \lambda(p_2^{e_2}), \ldots, \lambda(p_r^{e_r})).$$

Call this number K. It is known that $\lambda(n) \geq K$, it is left to show that $\lambda(n) = K$.

Let $a \in \mathbb{Z}_n : a^k \equiv 1(n) \Leftrightarrow a^k \equiv 1(p_i)^{e_i}, \forall i = 1, \ldots, r$. That means: $\lambda(p_i^{e_i})$ is the maximal order in $\mathbb{Z}_{p_i^{e_i}}^*$. By the theorem above it follows that: $ord_{\mathbb{Z}_{p_i^{e_i}}^*}(a) | \lambda(p_i^{e_i})$. Therefore $ord_{\mathbb{Z}_{p_i^{e_i}}^*}(a) | K$, by transitivity of $|$.

This means that: $a^k \equiv 1(p_i^{e_i})$ $\forall i$ if and only if $a^k \equiv 1(n)$ and therefore $ord_{\mathbb{Z}_n^*}(a) | K$.

It was already shown that $\exists b$ that has order K, now it is also shown that every element has order K. From there it follows that $\lambda(n) = K$. □

Theorem 3.17. *Let G be an Abelian group, if $a \in G$, such that $ord_G(a)$ is maximal, then $\forall b \in G : ord_G(b) | ord_G(a)$. This is also true for non-cyclic groups.*

Proof. That $ord_G(a)$ is maximal means: $ord_G(a) = \max\{ord_G(a_i) \mid \forall a_i \in G\}$, it has to be shown that $\forall b \in G : ord_G(b) | ord_G(a)$. This can be proven by contradiction. Assume that $\exists x \in G : ord_G(x) \nmid ord_G(a)$. By definition of the order of a group it follows that:

$$\exists y \in G : ord_G(y) = lcm(ord_G(x), ord_G(a)).$$

Since $ord_G(x) \nmid ord_G(a)$ it follows that $lcm(ord_G(x), ord_G(a)) > ord_G(a)$. But that is not possible, since this would meand that $ord_G(y) > ord_G(a)$, from which it follows that $ord_G(a)$ is not the maximal order. Hence: such an x cannot exist. □

Theorem 3.18. *The Carmichael function $\lambda(n)$ obeys the following values and rules:*

- $\lambda(1) = 1, \lambda(2) = 1, \lambda(4) = 2$
- $\lambda(2^e) = 2^{e-2}$ *for* $e \geq 3$
- $\lambda(p^e) = p^{e-1}(p-1)$ *for* $p \in \mathbb{P} \backslash \{2\}$
- $\lambda\left(\prod_{i=1}^{r} p_i^{e_i}\right) = lcm(\lambda(p_1^{e_1}), \ldots, \lambda(p_r^{e_r}))$

Example 3.12.

$$\lambda(100) = \lambda(2^2 \cdot 5^2) = lcm(\lambda(4), \lambda 25) = lcm(2, 20) = 20.$$

The Carmichael function and RSA: Attack by encryption iteration. Let $n = p \cdot q$, with public key (n, e) and private key (n, d). Suppose x is the message. Define:

$$\begin{aligned} y_0 &= x \\ y_1 &= x^e(n) \\ y_i &= y_{i-1}^e(n). \end{aligned}$$

To search for k, do the following:

$$\begin{aligned} y_k &= x \\ y_i &= x^{(e^i)}(n) \\ ed &\equiv 1(v) \\ v &= lcm(p-1, q-1) = \lambda(n) \\ x^{v+1} &\equiv x(n). \end{aligned}$$

The minimal k such that $y_k = x$ is $k_0 = ord_{\mathbb{Z}_v^\star}(e) = ord_{\mathbb{Z}^\star_{\lambda(n)}}(e)$, this means $k_0 | \lambda(\lambda(n))$. Look for p, q such that $\lambda(\lambda(n))$ is large. It can be shown that if p and q are such that $\frac{p-1}{2}$, $\frac{p-3}{4}$, $\frac{q-1}{2}$, $\frac{q-3}{4}$ are primes tho, then:

$$\begin{aligned} \lambda(pq) &= lcm(p-1, q-1) = 2 \cdot \frac{p-1}{2}\frac{q-1}{2} = \frac{(p-1)(q-1)}{2} \\ \lambda\left(\lambda(pq)\right) &= lcm\left(\lambda(2), \lambda\left(\frac{p-1}{2}\right), \lambda\left(\frac{q-1}{2}\right)\right) = \frac{(p-3)(q-3)}{8}. \end{aligned}$$

From which it follows that $\lambda(\lambda(pq))$ is of the same order of n. Which implies $\Theta(n) \sim \frac{n}{8}$.

Chapter 4

Polynomial over Finite Fields

4.1 Rings

Definition 4.1. *A structure $(R, +, \cdot)$ is called a **ring** if:*

- $(R, +)$ *is an Abelian group, with neutral element 0.*
- $(R, \cdot)$ *is a semigroup, where only associativity holds.*
- *The distributive laws hold:* $\forall a, b, c \in R$:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(a + b) \cdot c = a \cdot c + b \cdot c.$$

Definition 4.2. *An **integral domain** is a commutative ring, with a 1-element (the neutral element) and no zero divisors: if $a \cdot b = 0$ then $a = 0$ or $b = 0$.*

Definition 4.3. *A **Euclidean ring** is an integral domain with $n : R\backslash\{0\} \to \mathbb{N}$, a Euclidean function such that, $\forall a, b \in R, b \neq 0 : \exists q, r \in R$:*

$$a = b \cdot q + r$$
$$n(r) < n(b) \text{ or } r = 0$$
$$n(a) \leq n(ab).$$

Notice that there are rings on which such a function cannot be defined.

Example 4.1. *Some valid functions n in the respective fields are:*

$$n(x) = |x| \qquad x \in \mathbb{Z}$$
$$n(p(x)) = \deg(p(x)) \qquad x \in K[x]$$

Definition 4.4. *Assume there is an integral domain $(R, +, \cdot)$ such that $t|a \Leftrightarrow c : a = t \cdot c = c \cdot t$. Define the greatest common divisor (gcd) as:*

$$d = gcd(a, b) \text{ if } d|a \wedge d|b$$
$$t|a \wedge t|b \Rightarrow t|d.$$

Remember: in $\mathbb{Z}$: $d = gcd(a, b) \Rightarrow -d = gcd(a, b)$.

Definition 4.5. *Let R be an integral domain and suppose $a, b \in R$. Then a and b are called* ***associated****, denoted by $a \sim b$ if and only if, there exists a unit $r \in R^*$, such that $a = r \cdot b$.*

Recall the set (group) of units: $R^* = \{x \in R \mid \exists x^{-1} : x \cdot x^{-1} = 1\}$. Notice that $(R^*, \cdot)$ is a group, since:

- *There is a neutral element: $1^{-1} = 1$ which implies: $1 \in R^*$.*
- *For every element there is an inverse: $x \in R^*$ implies: $x^{-1} \in R^*$.*

Theorem 4.1. *Let R be an Euclidean ring, with $a, b \in R$. Then:*

$$a|b \Rightarrow n(a) \leq n(b).$$

Proof. There exists a c such that: $b = ac$ with $n(a) \leq n(ac) = n(b)$. □

Corollary 4.1. *Given two gcd's of a and b: d and d' then $n(d) = n(d')$.*

Proof. $d|d'$ and $d'|d$. □

Remark: Suppose $x = a \cdot b$ and $a, b \notin R^* \cup \{0\}$ then $n(a) < n(x)$, $n(b) < n(x)$, this follows by symmetry.

Remark: In general, for integral domains it holds:

$$d = gcd(a, b), d' = gcd(a, b) \Rightarrow d \sim d'.$$

It is known that $d'|d$ and $d|d'$, this implies: $d = c_1 \cdot d'$ and $d' = c_2 \cdot d$. Then: $d = c_1 \cdot c_2 \cdot d$ which means that $d(1 - c_1 \cdot c_2) = 0$ from which it follows that $c_1 \cdot c_2 = 1$. Therefore: $c_1, c_2 \in R^*$, they are units.

4.1.1 Generalization of prime numbers

Definition 4.6. *Let R be an integral domain and let $a \in R \backslash (\{0\} \cup R^*)$, i.e. $\nexists a^{-1}$, then a is* ***irreducible*** *if and only if $a = b \cdot c$ always implies that either $b \in R^*$ or $c \in R^*$.*

For $\mathbb{Z}$ it holds that $\mathbb{Z}^* = \{-1, 1\}$ and $p = p \cdot 1 = (-p) \cdot (-1)$.

The element a is called a ***prime element*** *if and only if $a|b \cdot c$ implies that $a|b$ or $a|c$. In general these are two different concepts.*

Example 4.2. *Let $R = \mathbb{Z}$, then $x \in R$ is irreducible if and only if $x \in \mathbb{P}$ or $-x \in \mathbb{P}$ if and only if x is a prime element.*

Theorem 4.2.

1. *Every prime element is irreducible.*
2. *In Euclidean rings, the converse is true as well.*

Proof.

1. Suppose a is a prime element and $a = b \cdot c$, this implies $a|b$ or $a|c$. To show that b or c is a unit. Assume that $a|b$ then $a|b$ and $b|a$ implies that $a = b \cdot c$ and $b = a \cdot \overline{c} = b \cdot c \cdot \overline{c}$. Now use the distributive laws:

$$b(1 - c \cdot \overline{c}) = 0 \Rightarrow c \cdot \overline{c} = 1.$$

   From which it follows that $c, \overline{c} \in R^*$ hence $a \sim b$ and it follows that a is irreducible. Since a is irreducible it follows that $b \in R^*$ ($a \sim c$) or $c \in R^*$ ($a \sim b$).
2. Suppose a is irreducible, $a|b \cdot c$ and $a \nmid b$. Let $d = gcd(a, b)$ this means: $a = d \cdot c_1$ and $b = d \cdot c_2$. Since a is irreducible it has to hold that either d or c_1 is a unit. This gives two options:
   - $c_1 \in R^*$ then it follows that $\exists c_1^{-1}$ for which it holds that $d = a \cdot c_1^{-1}$ but then $b = a \cdot c_1^{-1} \cdot c_2$ which suggests that $a|b$, but that is a contradiction!
   - Let $c_1 \notin R^*$ then it has to hold that $d \in R^*$. Suppose, without loss of generality, that $d = 1$. Since R is an Euclidean ring, it follows that $\exists x, y \in R$ such that $1 = a \cdot x + b \cdot y$. Multiplying by c gives:

$$c = a \cdot c \cdot x + b \cdot c \cdot y = a \cdot c \cdot x + a \cdot y = a(c \cdot x + y)$$

   From this it follows that $a|c$.

In the same way it is possible to prove that $a|b$ if it is assumed that $a \nmid c$.

□

Example 4.3. Let $R = \mathbb{Z}[i\sqrt{5}] = \{a + b \cdot i \cdot \sqrt{5} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$, where $i = \sqrt{-1}$. Is $R = \mathbb{Z}[i\sqrt{5}]$ an Euclidean ring?

Notice that $(R, +, \cdot) \leq (\mathbb{C}, +, \cdot)$ where $\leq$ denotes the subring relation. Since R is an Abelian group, multiplication is defined as follows:

$$(a + bi\sqrt{5})(c + di\sqrt{5}) = \underbrace{ac - 5bd}_{\in\mathbb{Z}} + \underbrace{(ad + bc)}_{\in\mathbb{Z}} i\sqrt{5} \quad \in \mathbb{Z}[i\sqrt{5}].$$

The ring is closed with respect to multiplication. There is also a neutral element:

$$1 + 0 \cdot i\sqrt{5} \in R.$$

There is however no unique decomposition in R, take for example the integer 6:

$$\begin{aligned} 6 = 2 \cdot 3 = &(1 + i\sqrt{5})(1 - i\sqrt{5}) \\ 2|6 \wedge 2 \nmid (1 + i\sqrt{5}): \quad &1 + i\sqrt{5} = 2 \cdot c = 2 \cdot (a + bi\sqrt{5}) \\ &2a = 1 \wedge 2b = 1 \\ &a \notin \mathbb{Z}. \end{aligned}$$

In the same way $2 \nmid (1 - i\sqrt{5})$. However $2|(1 + i\sqrt{5})(1 - i\sqrt{5})$, which implies that 2 is not a prime element of R. This means:

$$\begin{aligned} 2 &= \underbrace{(a + bi\sqrt{5})}_{r}\underbrace{(c + di\sqrt{5})}_{s} \\ &\Rightarrow \frac{2}{a + bi\sqrt{5}} \cdot \frac{a - bi\sqrt{5}}{a - bi\sqrt{5}} = c + di\sqrt{5} = \underbrace{\frac{2a}{a^2 + 5b^2}}_{\in\mathbb{Z}} - i\sqrt{5}\underbrace{\frac{2b}{a^2 + 5b^2}}_{\in\mathbb{Z}}. \end{aligned}$$

But $a^2 + 5b^2 > 4b^2 > 2|b|$, except if $b = 0$. Which implies that $d \notin \mathbb{Z}$ except if $b = 0$. Because, if $b = 0$ then:

$$c = \frac{2a}{a^2} = \frac{2}{a} \Rightarrow a \in \{\pm 1, \pm 2\}.$$

And hence $r = \pm 1$. Which implies $r \in R^*$ or $r = \pm 2$ and furthermore implies $s \in R^*$. But then 2 is irreducible, which means that $\mathbb{Z}[i\sqrt{5}]$ is not an Euclidean ring.

Example 4.4. *Let K be a field, then $(K, +)$ is an Abelian group, $(K\backslash\{0\}, \cdot)$ also is an Abelian group and the distributive law $a \cdot (b + c) = a \cdot b + a \cdot c$ apply: this means $\forall x \in K : 0 \cdot x = 0$, then $K[x]$ is an Euclidean ring.*

Recall that $n(p(x)) = \deg(p(x))$ and $\deg(p(x)) \leq \deg(p(x) \cdot q(x))$, this implies that the prime elements are the irreducible elements, irreducible polynomials: $a(x) = b(x) \cdot c(x)$, with $\deg(b(x)) = 0$ or $\deg(c(x)) = 0$. With as a side remark:

$$r(x) \in K[x]^*, 1 = 1 \cdot x^0 + 0 \cdot x^1 + \dots$$
$$r(x) \in K[x]^* \Leftrightarrow r(x) \neq 0, \deg(r(x)) = 0.$$

In $\mathbb{C}[x]$ it holds that $\deg(p(x)) = n$ which implies that $\exists n$ not necessarily different zeros $a_1, a_2, \dots, a_n$ and $p(x) = (x - a_1)(x - a_2)\dots(x - a_n)$ which is a fundamental theorem of algebra. It follows that $p(x)$ is irreducible if and only if $p(x) = ax + b$ is a linear polynomial.

In $\mathbb{R}[x]$: $x^4 = (x^2 + \sqrt{2} + 1)(x^2 - \sqrt{2} + 1)$ it can be shown that without zeros the only irreducible polynomials are: $ax + b$ and $ax^2 + bx + c$. If $p(a) = 0$ then $p(\overline{a}) = 0$. Which implies that:

$$(x - a)(x - \overline{a}) = x^2 - \underbrace{a + \overline{a}}_{Re(a)} x + \underbrace{a\overline{a}}_{|a|^2}.$$

A factor like this always exists in a polynomial.

Definition 4.7. *Let R be an integral domain, such that $\forall a \in R\backslash(\{0\} \cup R^*)$ there exists an unique representation $a = \epsilon p_1 p_2 \dots p_k$, where $\epsilon \in R^*$ and $p_1, \dots, p_k$ are prime elements. Here uniqueness means that if:*

$$\epsilon p_1 \dots p_k = \eta q_1 \dots q_k$$

then $k = l$ and there is a permutation pi such that $p_i \sim q_{\pi(i)}$ $\forall i = 1, \dots, k$ where $p_i = \epsilon_i q_{\pi(i)}$ and $\epsilon_i \in R^*$. For example:

$$15 = 1 \cdot 3 \cdot 5 = (-1) \cdot (-5) \cdot 3$$
$$3 \sim 3, 5 \sim (-5) : 5 = \underbrace{(-1)}_{\in \mathbb{Z}^*}(-5).$$

*Then R is called a **factorial ring** (Also called a ZPE-Ring).*

Theorem 4.3. *Every Euclidean ring is a factorial ring.*

Proof. To prove this theorem existence and uniqueness have to be proven.

- **Existence:** There are two cases: a is irreducible, or it is not irreducible.

1. Suppose that a is irreducible, this is the case if and only if a is a prime element. From which it follows that $a = 1 \cdot a$. This is a representation as desired.
2. Now suppose that $a = bc$, with $b, c \notin R^*$, then $n(b) < n(a)$ and $n(c) < n(a)$. Suppose that a does not have a representation of the form $a = \epsilon p_1 \dots p_k$ and that $a(n)$ is minimal. This suggests that b and c have a prime representation as follows:

$$b = \epsilon_1 p_1 \dots p_k$$
$$c = \epsilon_2 q_1 \dots q_l.$$

But then $a = \epsilon_1\epsilon_2 p_1 \dots p_k q_1 \dots q_l$ with $\epsilon_1\epsilon_2 \in R^*$. This is a contradiction.
With this the existence if proven.

- **Uniqueness:** Suppose $a = \epsilon p_1 \dots p_k = \eta q_1 \dots q_l$ for $k \geq 2$. This suggests that $p_1 | \eta q_1 \dots q_l$ and since $p_1 \notin R^*$ it follows that $p_1 \nmid \eta$ and hence $p_1 | q_1 \dots q_l$. This means: $\exists i : p_1 | q_i$.
Without loss of generality suppose $i = 1$, then $p_1 | q_1$, from which it follows that $p_1 \sim q_1$ and $p_1 = \epsilon_1 q_1$, with $\epsilon_1 \in R^*$. Then it follows that:

$$\epsilon p_2 \dots p_k = \eta\epsilon_1 q_2 \dots q_l.$$

Where $\eta\epsilon_1 \in R^*$. Now, without loss of generality, suppose that $p_2 | q_2$. If $l > k$ at the end it is found that $\epsilon = \widetilde{\epsilon} q_{k+1} \dots q_l$ but this is a contradiction: $l = k$ follows from this. Which proves the uniqueness. □

4.1.2 Ideals in Rings

Recall: $(G, *)$ is a group, let U be a subgroup: $U \leq G$: $a * U = \{a * x \mid x \in U\}$. These sets form a partition of the group. If $a \neq a'$ then either $a * U = a' * I$ or $(a * U) \cap (a' * U) = \varnothing$. Define the **left cosets** to be the elements $a * U$, with $a \in G$ and the **right cosets** to be the elements $U * a$, with also $a \in G$.

If $U \leq G$, such that $\forall a \in G : a * U = U * a$, then U is called a **normal subgroup**, denoted by $U \trianglelefteq G$. If $U \trianglelefteq G$ then:

$$(a * U) * (b * U) = (a * b) * U$$
$$(a * U) = (a' * U) \wedge (b * U) = (b' * U) \Rightarrow (a' * b') * U.$$

The group $(G/U, *)$ is called the **quotient group**. Where G/U, read as "G modulo U", is defined as: $G/U = \{a * U \mid a \in G\}$.

Definition 4.8. *Let R and S be rings, with a mapping $\varphi : R \to S$. The mapping φ is called a (ring) homomorphism if φ is compatible with the ring operations:*

$$\varphi(a + b) = \varphi(a) + \varphi(b)$$
$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b).$$

The kernel of φ is defined as: $kern\varphi = \{x \in R \mid \varphi(x) = 0\}$.

Theorem 4.4.

$$(kern\varphi, +) \trianglelefteq (R, +) \text{ and } a \cdot kern\varphi \subseteq kern\varphi$$
$$(kern\varphi) \cdot a \subseteq \varphi.$$

Proof. This theorem can easily be proven:

$$x \in kern\varphi \Rightarrow \varphi(ax) = \varphi(a) \cdot \underbrace{\varphi(x)}_{=0} = 0$$
$$\Rightarrow ax \in kern\varphi, xa \in kern\varphi.$$

□

Definition 4.9. *Let R be a ring, $I \subseteq R$ is an **ideal** if:*

1. *$(I, +)$ is a (normal) subgroup of $(R, +)$ (it is then also an Abelian group).*
2. *$a \cdot I \subseteq I$, $I \cdot a \subseteq I$.*

Since every subgroup of an Abelian group is a normal subgroup, the (normal) is not necessary.

Remark: *Let $\varphi : R \to S$ be a homomorphism, then $kern\varphi$ is an ideal of R.*

Theorem 4.5. *Let R be a ring and $I \subseteq R$ an ideal. Define $+$ and $\cdot$ on $R/I = (R, +)/(I, +)$, R modulo I, as follows:*

$$(a + I) + (b + I) := (a + b) + I$$
$$(a + I) \cdot (b + I) := (a \cdot b) + I.$$

*With this definition $(R/I, +, \cdot)$ is a ring, called the **quotient ring** R modulo I.*

Example 4.5. Let $R = \mathbb{Z}$, $I = n * \mathbb{Z} = \{n \cdot z \mid z \in \mathbb{Z}\}$, is this set an ideal?

Define $U \subseteq G$ as follows:

$$U \subseteq G \Rightarrow 1)\ U \neq \varnothing$$
$$2)\ a, b \in U \Rightarrow a * b^{-1} \in U.$$

It has to be verified. If $x, y \in n \cdot \mathbb{Z}$, such that $x = k \cdot n$ and $y = l \cdot n$ then $x - y = (k - l) \cdot n \in n \cdot \mathbb{Z}$. Now $n \cdot \mathbb{Z} \trianglelefteq \mathbb{Z}$, what are the cosets? Take $a \in \mathbb{Z}$ and the group operation $+$. Then $a + n \cdot \mathbb{Z} = \{a + nz \mid z \in \mathbb{Z}\}$. And furthermore:

$$a + n\mathbb{Z} = \overline{a} \text{ in } \mathbb{Z}_n$$
$$a \cdot n \cdot \mathbb{Z} \subseteq n \cdot \mathbb{Z}.$$

From this it follows that it is indeed an ideal. Look at the quotient: $\mathbb{Z}/n \cdot \mathbb{Z} = \mathbb{Z}_n$ here it holds that:

$$\overline{a} + \overline{b} = \overline{a + b}$$
$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

Furthermore: $a + b \equiv a + b(n)$ and $a \cdot b \equiv a \cdot b(n)$.

Remark: Let R be a ring, then there are two trivial ideals: $\{0\}$ and R.

Definition 4.10. *Let R be a ring and $I \subseteq R$ an ideal. Define an equivalence relation $\sim$ on R, i.e. $\sim \subseteq R \times R$. The relation $\sim$ is compatible with $+$ and $\cdot$ if:*

$$\begin{aligned} a \sim b \wedge c \sim d &\Rightarrow a + c \sim b + d \\ &\Rightarrow a \cdot c \sim b \cdot d. \end{aligned}$$

*An equivalence relation $\sim$ that is compatible with $+$ and $\cdot$ is called a **congruence relation**, e.g. $\equiv \mod n$. In particular $a \sim b$ if and only if $a + I = b + I$ which suggests that $\sim$ is a congruence relation.*

Theorem 4.6. *Let R be a ring with a 1 element, let $I \subseteq R$ be an ideal and $\epsilon \in R^* \cap I$. Then $R = I$.*

Proof. Since $\epsilon \in I \cap R^*$ it follows that $\exists \epsilon^{-1}$. By definition of an ideal it is known that $\forall r \in R : r \cdot I \subseteq I$. In particular: $\epsilon^{-1} \cdot I \subseteq I$, from which it follows that $1 \in I$.

$r \cdot I \subseteq I$ implies that $r \cdot 1 = r \in I$ from which it follows that $R \subseteq I$. Since also $I \subseteq R$ it has to be that $R = I$. □

Corollary 4.2. *A field K has only the trivial ideals $\{0\}$ and K.*

Remark: Let R be a ring, let $(I_j)_{j \in J}$ denote the **family of ideals**. Then $\bigcap_{j \in J} I_j$ is an ideal as well.

Definition 4.11. *Let R be a ring and $M \subseteq R$, such that:*

$$(M) := \bigcap_{I \subseteq R, I \text{ ideal}, M \subseteq I} I.$$

*This is the **ideal generated by** M. It is the smallest ideal, which contains M, with respect to $\subseteq$.*

Definition 4.12. *An ideal generated by only one element a $(-(a))$ is called a **principal ideal**.*

Theorem 4.7. *Let R be an Euclidean ring. Then every ideal is a principal ideal, i.e. R is a **principal ideal domain**.*

Remark: Euclidean ring $\subsetneq$ principal ideal domain $\subsetneq$ factorial ring $\subsetneq$ integral domain.

Example 4.6. Let $R = \mathbb{Z}$ and $(n) = n \cdot \mathbb{Z}$. If $M = \{m_1, \ldots, m_k\} \subseteq \mathbb{Z}$, what is (M), the ideal generated by M?

Start with two elements, m_1 and m_2, then $a \cdot m_1 + b \cdot m_2 \in (M)$, which implies that $gcd(m_1, m_2) \cdot \mathbb{Z} \subseteq (M)$. Since $M \subseteq gcd(m_1, m_2) \cdot \mathbb{Z}$, it follows that $(M) = gcd(m_1, m_2) \cdot \mathbb{Z}$.

Example 4.7. $x \in R^* \Rightarrow (x) = R$

Example 4.8. *The rational numbers $\mathbb{Q}$ are a subring (and even a subfield) of $\mathbb{R}$ it is however not an ideal of $\mathbb{R}$.*

4.2 Fields

Recall the properties of a field:

- $(K, +)$ is an Abelian group, with neutral element 0.
- $(K\backslash\{0\}, \cdot)$ is an Abelian group, with neutral element 1.
- $\forall a, b, c \in K$: $a \cdot (a + b) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$.
- $0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x \Rightarrow 0 | 0 \cdot x$ and $x \cdot 0 = 0$.

If $(K_i)_{i \in I}$ is a family of fields, then $\bigcap_{i \in I} K_i$ is a subfield.

Definition 4.13. $\bigcap_{K' \text{ subfield of } K} K'$ *is called the* ***prime field*** *of K, denoted by $P(K)$. $\{0\}$ is not a field, because every field has at least two elements and in every field $0 \leq 1$ holds.*

Definition 4.14. *$ord_{(K,+)}(1)$ is called the* ***characteristic of K****, denoted by $char(K)$, where $ord_G(a) = \min\{i > 0 \mid a^i = e\}$. Notice:*

$$1, 1 + 1, 1 + 1 + 1, \ldots, \underbrace{1 + 1 + 1 + \ldots + 1}_{char(K)} = 0 \text{ if it is finite.}$$

If $ord_{(K,+)}(1) = \infty$ then $char(K) = 0$.

Example 4.9.

$$\begin{aligned} (\mathbb{R}, +, \cdot) : & \; char(\mathbb{R}) = 0 \\ & \; char(\mathbb{Q}) = 0 \\ & \; char(\mathbb{C}) = 0 \\ (\mathbb{Z}, +, \cdot 0 : & \; char(\mathbb{Z}_2) = 2 \\ & \; char(\mathbb{Z}_p) = p \text{ if } p \in \mathbb{P}. \end{aligned}$$

Properties of $P(K)$: Two cases have to be distinguished:

- **Case 1:** $char(K) = 0$. Let K' denote a subfield of K, then $\forall K'$: $0, 1 \in K'$ implies $0, 1 \in P(K)$. From there it follows:

$$\begin{aligned} & 1, 1 + 1, 1 + 1 + 1, \ldots = k - 1, k \in \mathbb{N} \\ & -1, (-1) + (-1), \ldots = k(-1) = -(k \cdot 1) = (-k) \cdot 1 \\ & k \cdot 1, (-k) \cdot 1, (k \cdot 1) \cdot (l \cdot 1)^{-1} \in P(K), \quad k \in \mathbb{Z}, l \in \mathbb{N}\backslash\{0\} \\ & \{(k \cdot 1)(l \cdot)^{-1} \mid k, l \in \mathbb{Z}, l > 0\} \cong \mathbb{Q} \\ & P(K) \cong \mathbb{Q} \Rightarrow |K| = \infty \end{aligned}$$

- **Case 2:** $char(K) \neq 0$.

Lemma 4.1. *Let $p = ord_{(K,+)}(1) < \infty$ then:*

1. *$\forall a \in K\backslash\{0\} : ord_{(K,+)}(a) = p$.*
2. *$p \in \mathbb{P}$.*

Proof.

1. Notice that

$$p \cdot 1 = \underbrace{1+1+1+\ldots+1}_{p \text{ times}} = 0$$
$$p \cdot a = \underbrace{a+a+a+\ldots+a}_{p \text{ times}} = 0$$
$$a \cdot \underbrace{(1+1+1+\ldots+1)}_{=0} = a \cdot 0 = 0$$
$$ord(a) \leq p.$$

   Assume that $ord(a) = m$ then:

$$(m \cdot a) \cdot a^{-1} = \underbrace{\overbrace{a \cdot a^{-1}}^{-1} + \overbrace{a \cdot a^{-1}}^{-1} + \ldots + \overbrace{a \cdot a^{-1}}^{-1}}_{m \text{ times}} m \cdot 1.$$

   This implies that $m \geq p$, but also $m \leq p$, hence it follows that $m = p$ and hence $ord(a) = p$.
2. Assume $p = a \cdot b$, then:

$$0 = p \cdot 1 = \underbrace{\underbrace{1+1+\ldots+1}_{a \text{ times}} + a \cdot 1 + a \cdot 1 + \ldots + a \cdot 1}_{b \text{ times}}.$$

   From there it follows that: $b \cdot (a \cdot 1) = a \cdot 1 + a \cdot 1 + \ldots + a \cdot 1$ and hence: $ord(a \cdot 1) = b < p$ However, that is a contradiction! □

A consequence of the lemma is that $char(K) = P$ implies that $P(K) \cong \mathbb{Z}_p$.

Corollary 4.3. *Let K be a field, the characteristic cannot be 0. Then $\exists p \in \mathbb{P}$ such that for $n \in \mathbb{N}^+$: $|K| = p^n$. (There are no fields with 6 or 10 elements).*

Proof. That $P(K)$ is finite means that $\exists p \in \mathbb{P}$ such that $|P(K)| = p$, in particular: $P(K) \cong \mathbb{Z} + p$. The following can be done. Since $P(K) \subseteq K$, regard K as a vector space over $P(K)$, where the scalars are taken from $P(K)$. Since it is a finite vector space, $dim(K) = n$, it follows that there exists a basis:

$$\{a_1, a_2, \ldots, a_n\} \subseteq K \Rightarrow dim\,\langle K, P(K)\rangle = n.$$

This implies that K can be defined as:

$$K = \left\{ \sum_{i=1}^{n} \lambda_i a_i \;\middle|\; \lambda_i \in P(K), i = 1, 2, \ldots, n \right\}$$

Where $P(K)$ has p elements, from there it follows that $|K| = p^n$. □

Remark: Given p and n it follows that:
1. $\exists K : |K| = p^n$.
2. Let K and K' be fields with $|K| = |K'| = p^n$, then $K \cong K'$.

Let K be a field, then $K[x]$ is an Euclidean ring and every ideal of K is a principal ideal. Furthermore $K[x]$ is a factorial ring, there is a unique factorization into primes.

Suppose $P(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ with $a_0, a_1, \ldots, a_{n-1} \in K$. Then it can be said that: $I(P(X))$ is an ideal in $K[x]$, from which it follows that $P(x) \in I$ and $Q(x)P(x) \in Q(x) \cdot I \subseteq I$.

Now look at the set $\{R(x) \mid \exists Q(x) \in K[x] : P(x)Q(x) = R(x)\}$, this set is already an ideal and it is also a subset of I and it is the smallest ideal of I, which means that it is equal to I.

Take a look at the ring $K[x]/P(x)$ which is defined as the ideal $K[x]$ modulo the ideal generated by $P(x)$. Then it holds that, for $\equiv$ a congruence relation:

$$\begin{aligned} A(x) \equiv B(x) \mod P(x) &\Leftrightarrow P(x) | A(x) - B(x) \\ A(x) \equiv B(x) \wedge C(x) \equiv D(x) &\mod P(x) \\ \Rightarrow A(x) + C(x) \equiv B(x) + D(x) &\mod P(x) \\ \Rightarrow A(x) \cdot C(x) \equiv B(x) \cdot D(x) &\mod P(x). \end{aligned}$$

Notice that $\equiv$ is compatible with the ring operations. This means that $K[x]/P(x)$ is a quotient ring. What are the residue classes? Notice that $P(x) \equiv 0 \mod P(x)$, this means:

$$x^n \equiv -a_{n-1}x^{n-1} - a_{n-2}x^{n-2} - \ldots - a_1x - a_0 \mod P(x).$$

Where each polynomial $Q(x)$ fulfills: $Q(x) \equiv \widetilde{Q}(x) \mod P(x)$ and $\deg \widetilde{Q}(x) < n$.

Example 4.10. *Let $\mathbb{R}[x]/x^2 - 1$ and look at the following polynomial:*

$$\begin{aligned} x^4 - 3x^3 + 2x^2 - 5x + 1 &\equiv x^2 - 3x + 2 - 5x + 1 \\ &\equiv x^2 - 8x + 3 \\ &\equiv -8x + 4. \end{aligned}$$

With the residue classes:

$$\mathbb{R}[x]/x^2 - 1 = \{\overline{ax + b} \mid a, b \in \mathbb{R}\}$$

There are zero-divisors: $\overline{x - 1}$ and $\overline{x + 1}$ from which it follows that $\mathbb{R}[x]/x^2 - 1$ is not an integral domain.

In general: $K[x]/P(x) = \{\overline{\sum_{i=0}^{n-1} b_i x_i} \mid b_i \in K\}$. If $P(x) = Q(x)R(x)$, where $\deg(Q(x)) \geq 1$ and $\deg(R(x)) \geq 1$, it follows that $K[x]/P(x)$ is not an integral domain.

Theorem 4.8. *Let K be a field and $P(x) \in K[x]$. Then $K[x]/P(x)$ is a field if and only if $P(x)$ is irreducible.*

Proof.

" $\Rightarrow$ " : Assume that $K[x]/P(x)$ is a field. This means that the polynomial $P(x)$ must be irreducible, otherwise $K[x]/P(x)$ would have zero-divisors.

" $\Leftarrow$ " : Assume that $P(x)$ is irreducible, clearly $K[x]/P(x)$ is a commutative ring, with a 1-element: $\overline{1} = 1 + (P(x))$. To show that every non-zero element has an inverse. Let

$A(x) \not\equiv 0 \mod P(x)$. Without loss of generality, assume that $\deg(A(x)) < \deg(P(x))$ then it follows that $gcd(A(x), P(x)) = 1$.

Using the Euclidean algorithm, it is possible to find $B(x)$ and $C(x)$ such that:

$$A(x)B(x) + P(x)C(x) = 1.$$

Take $1 \equiv A(x)B(x) \mod P(x)$. From this it follows that $B(x) = (A(x))^{-1}$ in $K[x]/P(x)$, but $A(x) \not\equiv 0 \mod P(x)$. Now $(K[x]/P(x))^* = K[x]/P(x)\backslash\{\overline{x}\}$ where $(K[x]/P(x))^*$ is the set of units. This implies that $K[x]/P(x)$ is a field. □

Remarks: If $P(x)$ is irreducible and $\deg(P) > 2$, then $P(x)$ has no zeros, since otherwise, say $P(a) = 0$, then $x - a | P(x)$, which would be a contradiction.

K is a subfield of $K[x]/P(x)$ and $K \hat{=}$ constant polynomials.

4.2.1 Algebraic extensions of a field K

Let $P(x)$ be irreducible over K, this means that $P(x) = 0$ has no solutions in K. Suppose $P(a) = 0$, then $a \notin K$, but $a \in L \supsetneq K$, $P(x)$ is monic: i.e.:

$$P(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0.$$

Theorem 4.9. *Let K and L be fields, such that $K \subseteq L$ and let $a \in L$ be a zero of some polynomial in $K[x]$. Now, if $a \notin K$ then $\exists!$ monic and irreducible polynomial in $K[x]$ having a as a zero.*

Proof. Again existence and uniqueness have to be proven. The existence follows trivially, since $K[x]$ is a factorial ring and an integral domain.

For the proof of uniqueness assume that there are two polynomials $P_1(x)$ and $P_2(x)$ which are monic and irreducible, such that $P_1(x) \neq P_2(x)$ and $P_1(a) = P_2(a) = 0$, then $d(x) = gcd(P_1(x), P_2(x)) = A(x)P_1(x) + B(x)P_2(x)$ which implies that $d(a) = 0$, but $d(x) = 1$, which gives a contradiction. From the contradiction it follows that $P(x)$ is unique and has a minimal degree among all $Q(x)$, with $Q(a) = 0$. □

As a consequence to the above proof the following can be shown. Let

$$P(x) = x^n + \sum_{i=0}^{n-1} p_i x^i$$

Take the second part (remainder term) and plug in a for x. This produces the term $\sum_{i=0}^{n-1} p_i a^i \neq 0$, with degree smaller than $\deg(P(x))$. By definition we know that: $a^n + \sum_{i=0}^{n-1} p_i a^i = 0$. This corresponds to $\sum_{i=0}^{n-1} c_i x^i$ in $K[x]/P(x)$.

It follows that $\overline{x^n + \sum_{i=0}^{n-1} p_i x^i} = \overline{0}$. Which suggests an isomorphism, with:

$$L = \left\{ \sum_{i=0}^{n-1} c_i a^i \;\middle|\; c_i \in K \right\}$$

This is the smallest field with $a \in L$ and moreover: $L \cong K[x]/P(x)$.

Definition 4.15. *Let $P(x)$ be monic and irreducible over K, with degree $\deg(P) = n$ and $P(a) = 0$. Define $L = \{\sum_{i=0}^{n-1} c_i a^i \mid c_i \in K\}$. Then a is **algebraic** over K, $P(x)$ is a **minimal polynomial of** a **over** K and L is an **algebraic extension of** K. Now $L = K(a)$, which means that "K adjoined a".*

Example 4.11. *Let $\mathbb{C} = \mathbb{R}(i) \cong \mathbb{R}[x]/x^2 + 1 = \{\overline{a + bx} \mid a, b \in \mathbb{R}\}$, some calculations that can be carried out here are:*

$$\begin{aligned}(a + bx)(c + dx) &\equiv ac + (ad + bc)x + bd\underbrace{x^2}_{\equiv -1} \\ &\equiv ac - bd + (ad + bc)x \\ (a + bi)(c + di) &\equiv ac + (ad + bc)i + bdi^2 \\ &\equiv ac - bd + (ad + bc)i\end{aligned}$$

Notice: this is the same as the complex numbers!

Example 4.12. *Take a look at $\mathbb{Q}[x]/x^2 - 2 \cong \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. It follows that $x^2 - 2 = 0$, from which it follows that $x = \pm\sqrt{2}$ and hence $\sqrt{2}$ is a zero of the irreducible polynomial $x^2 - 2$ which implies: $\sqrt{2}$ is irrational and algebraic.*

However, π is a non algebraic number, it is part of the transcendent numbers: $\nexists P(x) \in \mathbb{Q}[x]$ such that $P(\pi) = 0$. Other examples of transcendent numbers are $ln(2)$ and e. Notice that $\sqrt[n]{a}$ is algebraic, since $x^n - a$ is a possible polynomial.

Example 4.13. *Now look at $K[x]/ax + b \cong K$, where $a, b \in K$ and $a \neq 0$. Then $x = a^{-1}b$. It is also possible to ajoin the square roots of the primes, this gives a chain of field, for example $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.*

Some remarks:

1. A maximal field has only irreducible polynomials of degree 1. This means, there is no proper algebraic extension. Such fields are called algebraically closed. An example of such a field is $\mathbb{C}$.
2. Let K be a field, then there exists a field L, where $K \subseteq L$ and L is algebraically closed. Every field has an algebraically closure.
3. Suppose $|K| = p \cong \mathbb{Z}_p$ and $p \in \mathbb{P}$ then for every $n \in \mathbb{N}^+$, there is an irreducible polynomial $P(x) \in K[x]$. Therefore:

$$|K[x]/P(x)| = \left| \left\{ \overline{\sum_{i=1}^{n-1} c_i x^i} \;\middle|\; c_i \in K \right\} \right| = p^n.$$

   A field with exactly p^n elements is $\mathbb{Z}_p[x]/P(x)$, with $P(x)$ irreducible and of degree n, such a field is of order p^n and is called a **Galois field** denoted by $GF(p^n)$.

Proposition 4.1. *Let $M(x)$ be the minimal polynomial of $a \in K$ and $f(x) \in K[x]$ such that $f(a) = 0$. Then $M(x)|f(x)$. Obviously: if $g(x) = M(x) \cdot h(x)$ then $g(a) = 0$.*

Proof. Let $f(x) = M(x)p(x) + q(x)$, with $\deg(q(x)) < \deg(M(x))$. It is known that $f(a) = 0$ and also that $g(a) = 0 + q(a)$. From there it follows that $q(a)$, which can only be the case if $q(x) = 0$. □

4.2.2 Finite Fields

Let K be a finite field. Then $char(K) = p$, for $p \in \mathbb{P}$,$P(K) \cong \mathbb{Z}_p$ and $|K| = p^n$, $|K^*| = |K \backslash \{0\}| = p^n - 1$. Let $a \in K^*$, with $ord_{K^*}(a) = r$ is maximal, then $r|p^n - 1$ and for $y \in K^*$, $ord_{K^*}(y)|ord_{K^*}(a) = r$.

$\forall y \in K^* : y^r = 1$, then all $y \in K^*$ are zeros of $x^r - 1$. In a field the number of zeros of a polynomial $P(x)$ is bounded by the degree of $P(x)$, which is in this case r. This means the number of elements in K^* has to be bounded by r: $p^n - 1 \leq r$ and from here it can be concluded that $p^n - 1 = r$.

Theorem 4.10. *Let K be a finite field, then $(K^*, \cdot)$ is an acyclic group (this means: it has a generator).*

Corollary 4.4. *$\forall a \in K$: $a^{p^n} = a$, for the polynomial $x^{p^n} - x$, which has every element of the field as a zero. It holds that $x^{p^n} - x = \prod_{a \in K} (x - a)$.*

Definition 4.16. *A generator of K^* is called a **primitive element of** K, its minimal polynomial over $\mathbb{Z}_p$ is called a **primitive polynomial**.*

Theorem 4.11. *Let $q(x) \in \mathbb{Z}_p[x]$ be a monic, irreducible polynomial of degree n. Then $q(x)$ is a primitive polynomial of $K = GF(p^n)$ if and only if $q(x)|x^{p^n-1} - 1$ and $\forall k : 1 \leq k \leq p^n - 1 : q(x) \nmid x^k - 1$.*

Proof.
" $\Rightarrow$ " : Suppose $q(x)$ is a minimal polynomial of a, where $\langle a \rangle = K^*$, with a a primitive element. Since $a^{p^n-1} - 1 = 0$ it follows that $q(x)|x^{p^n-1} - 1$. Since $k < p^n - 1$ it follows that $a^k - 1 \neq 0$, because $ord_{(K^*,\cdot)}(a) = |K^*| = p^n - 1$. But then $q(x) \nmid x^k - 1$, which proofs the $\Rightarrow$ side.

" $\Leftarrow$ " : Suppose $q(a) =$, then $a \in L \supsetneq \mathbb{Z}_p$ which implies: $ord(a)$ in $\mathbb{Z}_p(a)$. Certainly: $a^{p^n-1} - 1 = 0$ and $ord(a) = k < p^n - 1 : a^k - 1 = 0$, but $x^k - 1$ must then be a multiple of $g(x)$ which is a contradiction.

It has to be shown that $q(x)$ is a minimal polynomial of primitive element a. Then $q(x) = (x - a)(x - a^p)(x - a^{p^2}) \dots (x - a^{p^{n-1}})$, which suggests that there are n zeros. How many primitive elements are there? $|K| = p^n$ and let l denote the number of primitive elements. Then $\langle a \rangle = K^*$ implies that $ord(a) = p^n - 1$. This means:

$$ord(a^k) = \frac{p^{n-1}}{gcd(p^{n-1}, k)} = p^{n-1} \Leftrightarrow gcd(p^n - 1, k) = 1.$$

Let $K^* = \{a^0, a^1, \dots, a^{p^n-2}\}$, which generates all the primitive elements. It follows that if a^k is a primitive element then $l = \varphi(p^n - 1)$. And if a is a primitive element then a^p, a^{p^2},...,$a^{p^{n-1}}$ are primitve elements as well. Any zero that generates K^* is primitve. This implies that $n|\varphi(p^n - 1)$ and the number of primitive polynomials is: $\frac{1}{n}\varphi(p^n - 1)$. □

Lemma 4.2. *Let $a, b \in K$, $p = char(K)$, then $(ab)^p = a^p b^p$ and $(a + b)^p = a^p + b^p$.*

Proof. It is known that:

$$p \cdot 1 = \underbrace{1+1+\ldots+1}_{p \text{ times}}. p \cdot a = \underbrace{a+a+\ldots+a}_{p \text{ times}}.$$

By the binomium from Newton it follows that: $(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}$. Where, by definition as well, $\binom{p}{k} = \frac{(p-1)!}{p \cdot k! \cdot (p-k)!}$. However: $\frac{(p-1)!}{k!(p-k)!} \in \mathbb{Z}$ which suggest that $\sum_{k=0}^{p} \frac{(p-1)!}{p \cdot k! \cdot (p-k)!} = 0$.

If $k = 0$ or $k = p$, it is defined that $\binom{p}{k} = 1$. From this it follows that:

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} = \binom{p}{0} a^0 b^p + \binom{p}{p} a^p b^0 = b^p + a^p = a^p + b^p. \qquad \square$$

Properties of homomorphism: Let $\varphi : K \to K$, where $x \mapsto x^p$ (a field homomorphism). Then $kern\varphi$ is an ideal of K, but K is a field, which means that $\{0\}$ and K are the only ideals. Take a look at the following:

$$\varphi(1) = 1^p \neq 0 \Rightarrow 1 \notin kern\varphi \Rightarrow kern\varphi\{0\}.$$

From this it follows that φ is injective, it is bijective and φ is an automorphism.

Theorem 4.12. *Let $K = GF(p^n)$ then $\varphi : K \to K$ and $x \mapsto x^p$ is an automorphism.*

Remark: The following functions are automorphisms:

$$\varphi, \varphi \circ \varphi, \varphi \circ \varphi \circ \varphi, \ldots$$
$$\varphi, \varphi^2, \ldots, \varphi^{n-1}, \varphi^n = id_K.$$

Where the second row gives all automorphisms.

Definition 4.17. *$(\{\psi : K \to K \mid \varphi \text{ automorphism}\}, \circ) = \langle\psi\rangle$ is a cyclic group and it is the **automorphism group** of K: $Aut(K)$. The following properties hold for such a group:*

$$\forall x, y \in K : \psi(x+y)\psi(x) + \psi(y)$$
$$\psi(xy) = \psi(x)\psi(y).$$

Consequence: $K = \mathbb{Z}_p(a) \cong GF(p^n)$ if the minimal polynomail of a, $q(x) \in \mathbb{Z}_p[x]$ has degree n. By definitions, $q(a) = 0$, $\psi \in Aut(K)$ and $b = \psi(a)$, this implies that $q(b) = q(\psi(a)) = \psi(0) = 0$. Notice $\psi(a) \in \{a, a^p, \ldots, a^{p^{n-1}}\}$. Therefore: $q(x) = (x-a)(x-a^p)\ldots(x-a^{p^{n-1}})$.

4.3 Applications

4.3.1 Linear code

Definition 4.18. *Let $K = GF(q)$ and define $f : K^k \to K^n$ to be a linear (a homomorphsim on the level of vector spaces), injective image of the whole set $C = f(K^k)$, which is a subspace of K^n ($C \leq K^n$), with $dim(C) = k$, this is called a (n,k)-**linear code**.*

The elements of K^k are: $x_1, \ldots, x_k \in K^k$ and of K^n are: $c_1, c_2, \ldots, c_n \in K^n$, written as words or messages. $\underline{c}$ denotes the word c.

*Let $\underline{c} \in K^n$, the **Hamming weight** of $\underline{c}$ is defined as:*

$$w(\underline{c}) = w(c_1 c_2 \ldots c_n) = |\{i \mid c_i \neq 0\}|.$$

*The base of C is: $\underline{c}_1, \underline{c}_2, \ldots, \underline{c}_k$. The **generating matrix** of C, G, is an $k \times n$-matrix:*

$$G = \begin{pmatrix} \underline{c}_1 \\ \underline{c}_2 \\ \vdots \\ \underline{c}_k \end{pmatrix}.$$

*A code C is called **systematic** if: $v = v_1 v_2 \ldots v_k$, which implies that $v \cdot G = v_1 v_2 \ldots v_k c_{k+1} \ldots c_n$.*

Let $f : K^k \to K^n$ and $\underline{x} \mapsto \underline{x} \cdot G$, then $\underline{x} \in K^k$ can be written as:

$$\underline{x} = \lambda_1 * 100 \ldots 0 + \lambda_2 \cdot 010 \ldots 0 + \ldots + \lambda_k \cdot 0 \ldots 001.$$

This implies that $000 \ldots 010 \ldots 0 * G = \underline{c}_j$. Furthermore:

$$\underline{x} \cdot G = \sum_{i=1}^{k} \lambda_i c_i \Rightarrow f(K^k) = [\underline{c}_1, \underline{c}_2, \ldots, \underline{c}_k] = C.$$

Theorem 4.13. *Every (n,k)-linear code has an equivalent (with respect to error detection and correction) systematic (n,k)-linear code. For a systematic (n,k)-linear code the generating matrix has the form: $G = (I_{k\times k} A_{k\times(n-k)})$. Then: $\underline{x}G = x_1 x_2 \ldots x_k v_{k+1} \ldots v_n$. With $d(\underline{v}, \underline{w}) = w(\underline{v} - \underline{w})$ the Hamming distance.*

Now look at the minimal Hamming distance: $w_{\min}$. Let $w_{\min}(\underline{x}), \underline{x} \in C \backslash \{00 \ldots 0\}$, then $w_{\min} = d$: up to $d-1$ errors can be detected and up to $\frac{d}{2} - 1$ errors can be corrected. Now look at $w_{\min}(\underline{x}), \underline{x} \in C \backslash \{0\}$, with $w_{\min} = d_{\min} = \min d(\underline{x}, \underline{y}) : \underline{x}, \underline{y} \in C$, which implies that $\underline{x} - \underline{y} \in C$.

Now $d(\underline{x}, \underline{y}) = w(\underline{x} - \underline{y})$ implies that $d_{\min} \geq w_{\min}$, $\underline{x} \in C$ implies: $w(\underline{x} = d(\underline{x}, \underline{0})$, where $\underline{0} \in C$. Then $d_{\min} \leq w_{\min}$. And hence $d_{\min} = w_{\min}$.

Definition 4.19. *The **dual code** $C^\perp$ is defined as: $C^\perp = \{\underline{v} \in K^n \mid \underline{uv} = 0, \forall u \in C\}$, the dual code has a generating matrix as well, this is H and H is called a **check matrix** of C, because:*

$$G * H^T = \begin{pmatrix} \underline{c}_1 \\ \underline{c}_2 \\ \vdots \\ \underline{c}_k \end{pmatrix} \cdot \begin{pmatrix} \underline{h}_1^T & \underline{h}_2^T & \ldots & \underline{h}_{n-k}^T \end{pmatrix} = 0_{k\times(n-k)}.$$

Remark: $\underline{c} \in C \Leftrightarrow \underline{c} \cdot H^T = \underline{0}$.

Let C be a system, then $G = (I_{k\times k} A_{k\times(n-k)})$, which implies that $H = (-A^T I_{(n-k)\times(n-k)})$.

Definition 4.20. *Let $S_H(\underline{v}) = \underline{v} \cdot H^T$ be the **syndrome** of $\underline{v}$. Now $S_H(\underline{v}) = \underline{0} \Leftrightarrow \underline{v} \in C$.*

Theorem 4.14. *Let $C \leq K^n$ be a (n,k)-linear code, with check matrix H and $(C,+) \trianglelefteq (K^n,+)$, then $\underline{u}, \underline{v}$ are in the same coset $a + C$ of K^n/C if and only if $S_H(\underline{u}) = S_H(\underline{v})$. Furthermore: $|K^n| = q^n$, $|C| = q^k$ and $|K^{n-k}| = |\underbrace{K^n/C}_{coset}| = q^{n-k}$.*

Proof. $\underline{u} + C = \underline{v} + C \Leftrightarrow \underline{u} - \underline{v} \in C \Leftrightarrow S_H(\underline{u} - \underline{v}) = \underline{0} \Leftrightarrow S_H(\underline{u}) = S_H(\underline{v})$. □

Example 4.14.

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix} \qquad H = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

$$Code\ C = \{00000, 10110, 01101, 11011\}$$

Coset	*Syndrome*
$00000 + C = C$	000
$00001 + C = \{00001, 10111, 01100, 11010\}$	001
$00001 + C = \{00010, 10100, 01111, 11001\}$	010
$00001 + C = \{00011, 10101, 01110, 11000\}$	011
$00001 + C = \{00100, 10010, 01001, 11111\}$	100
$00001 + C = \{01000, 11110, 00101, 10011\}$	101
$00001 + C = \{10000, 00110, 11101, 01011\}$	110
$00001 + C = \{01010, 11100, 00111, 10001\}$	111

s	000	001	010	011	100	101	110	111
$\tilde{w}(s)$	00000	00001	00010	00011	00100	01000	10000	01010
				B				B

4.3.2 Polynomial codes

Let $K = GF(q)$ and let $K_{n-1}[x] = \{p(x) \in K[x] \mid \deg(p(x)) \leq n-1\}$ be a vector space over K, with $dim(K_{n-1}[x]) = n$ and $K_{n-1}[x] \cong K^n$. Take $g(x) \in K[x]$ such that $\deg(g(x)) = n-k$. Define the following injective, linear mapping F:

$$F : F(p(x)) = p(x) \cdot g(x), p(x) \in K_{k-1}[x]$$
$$F : K_{k-1}[x] \to K_{n-1}[x].$$

It follows that $C = \{p(x)g(x) \mid p(x) \in K_{k-1}[x]\}$ where of course: $C \leq K_{n-1}[x]$ and $dim(C) = K$. Define the span to be:

$$C = [g(x), x \cdot g(x), \ldots, x^{k-1} \cdot g(x)].$$

Where $g(x)$ is called the **generating polynomial of** C. Define the **check polynomial** as follows: $c(x) \cdot h(x) \hat{=} 0$ and $f(x) : K[x]/f(x)$:

$$\begin{aligned} c(x) \in C &\Leftrightarrow c(x) \cdot h(x) \equiv 0 \mod f(x) \\ &\Leftrightarrow c(x) = p(x)g(x) \\ &\Leftrightarrow c(x)h(x) = p(x)g(x)h(x) \equiv 0 \mod f(x), \forall p(x) \in K_{k-1}[x]. \end{aligned}$$

Where $\deg(g(x)) = n - k$, $\deg(f(x)) = n$ and $\deg(h(x)) = k$, it should be the case that $g(x)h(x) \equiv 0 \mod f(x)$, which implies that $f(x) = \lambda g(x)h(x)$. If f, g and h are monic, then $f(x) = g(x)h(x)$ and $f(x)$ is a **principal polynomial** of C. Furthermore:

$$v(x)h(x) \equiv 0 \mod f(x) \Leftrightarrow f(x) = g(x)h(x) | v(x)h(x) \Leftrightarrow g(x) | v(x) \Leftrightarrow v(x) \in C.$$

Syndromes. Take a look at the following equivalences:

$$\begin{aligned} v(x) + C = w(x) + C &\Leftrightarrow v(x) - w(x) \in C \\ &\Leftrightarrow (v(x) - w(x))h(x) \equiv 0 \mod f(x) \\ &\Leftrightarrow v(x)h(x) \equiv w(x)h(x) \mod f(x) \\ &\Leftrightarrow v(x) \equiv w(x) \mod g(x). \end{aligned}$$

With these equivalences a **syndrome** can be defined as: $S(v(x)) = v(x) \mod g(x)$, possible syndromes are therefore all the polynomials $p(x) \in K_{n-k-1}[x]$.

Definition 4.21. *A code C is cyclic if $\underline{c} = c_1 c_2 \dots c_n \in C$ and every cyclic permutation is also in C. This means:*

$$\begin{aligned} &\underline{c} = c_1 c_2 \dots c_n \in C \Rightarrow c_n c_1 c_2 \dots c_{n-1} \in C \\ &\Leftrightarrow c_1 + c_2 x + \dots + c_n x^{n-1} \in C \Rightarrow c_n + c_1 x + \dots + c_{n-1} x^{n-1} \in C \end{aligned}$$

This is nothing else than $x \cdot c(x) \mod (x^n - 1)$.

Theorem 4.15. *A (n, k)-polynomial code is cyclic if and only if $g(x) | x^n - 1$.*

Proof.
" $\Leftarrow$ " : $f(x) = x^n - 1$ can be chosen as principal polynomial of C. From there this side of the proof follows immediately.

" $\Rightarrow$ " : Let $c(x) = c_0 + c_1 x + \dots + c_{n01} x^{n-1} \in C$ and let π be a cyclic permutation, such that: $\pi(c(x)) = c_{n-1} + c_0 x + \dots + c_{n-2} x^{n-1} \in C$. However: $\pi(c(x)) = xc(x) - c_{n-1}(x^n - 1)$ implies that $\overline{\pi c(x)} = \overline{xc(x)}$ in $K[x]/x^n - 1$ and then $\overline{\pi^i c(x)} = \overline{x^i c(x)}$ in $K[x]/x^n - 1$.

If $g(x) \in C$, then $\pi^i g(x) \in C$ which implies that $x^i g(x) \mod x^n - 1 \in C$. In particular:

$$(x^k \underbrace{g(x)}_{\deg(g(x))=n-k} \mod x^n - 1) = x^k g(x) - (x^n - 1) \in C$$

which implies that $g(x) | x^n - 1$. □

4.3.3 BCH-codes

The BCH-codes are named after Bose, Chaudhuri and Hocquenghem. Take a, the n-th primitive root of unity ($a^n - 1 = 0, |\langle a \rangle| = n$) in $GF(q)$. Let A denote the set: $A = \{a^{i_1}, \dots, a^{i_m}\}$, with $i_1, \dots i_m \leq n - 1$ and let $M(A)$ be the following $m \times n$-matrix:

$$M(A) = \begin{pmatrix} 1 & a^{i_1} & \dots & a^{(n-1)i_1} \\ 1 & a^{i_2} & \dots & a^{(n-1)i_2} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & a^{i_m} & \dots & a^{(n-1)i_m} \end{pmatrix}$$

If $i_j = i + j - 1$, then $A = \{a^i, a^{i+1}, \dots, a^{i+n-1}\}$, where A is called **gap-free**, which means in some way simple.

Theorem 4.16. *Let a be a primitive n-th root of unity in $GF(q)$ and let $A = \{a^i, a^{i+1}, \dots, a^{i+m-1}\}$ with $i + m - 1 < n$ be gap-free. Then any m columns of $M(A)$ are linear independent.*

Proof. Let $j \neq k$ it follows that $a^j \neq a^k$. With this the following can be done:

$$\det \begin{pmatrix} a^{j_1 * i} & a^{j_2 * i} & \dots & a^{j_m * i} \\ a^{j_1 * (i+1)} & a^{j_2 * (i+1)} & \dots & a^{j_m * (i+1)} \\ \vdots & \vdots & \ddots & \vdots \\ a^{j_1 * (i+m-1)} & a^{j_2 * (i+m-1)} & \dots & a^{j_m * (i+m-1)} \end{pmatrix}$$

$$= a^{(j_1 + j_2 + \dots j_m) i} * \det \begin{pmatrix} 1 & 1 & \dots & 1 \\ a^{j_1} & a^{j_2} & \dots & a^{j_m} \\ a^{j_1 * 2} & a^{j_2 * 2} & \dots & a^{j_m * 2} \\ a^{j_1 * 3} & a^{j_2 * 3} & \dots & a^{j_m * 3} \\ \vdots & \vdots & \ddots & \vdots \\ a^{j_1 * (m-1)} & a^{j_2 * (m-1)} & \dots & a^{j_m * (m-1)} \end{pmatrix} \overset{\text{Vandermonde}}{\neq} 0$$

Remember: the determintante of a Vandermonde-matrix can easily caltulated:

$$\det \begin{pmatrix} 1 & 1 & \dots & 1 \\ t_1 & t_2 & \dots & t_m \\ t_1^2 & t_2^2 & \dots & t_m^2 \\ \vdots & \vdots & \ddots & \vdots \\ t_1^{m-1} & t_2^{m-1} & \dots & t_m^{m-1} \end{pmatrix} = \prod_{1 \leq i < j \leq m} (t_j - t_i)$$

Which concludes the proof. □

Theorem 4.17. *Let C be a cyclic (n, k)-polynomial code over $GF(q)$, with generating polynomial $g(x)$ and a an n-th primitive root of unity in $GF(q)$. If there exists an b such that $b \geq 0$ and there exists an δ, such that $\delta \geq 2$ and $g(a^{i+b}) = 0$ for $0 \leq i \leq \delta - 2$, then $w_{\min}(C) \geq \delta$.*

Proof. Suppose $\mathbf{c} = c_0 c_1 \dots c_{n-1} \in C \hat{=} c_0 + c_1 x + \dots + c_{n-1} x^{n-1} = c(x) = g(x) \cdot \widetilde{c}(x)$. If $g(x_0) = 0$ then $c(x_0) = 0$ and in particular: $c(a^{i+b}) = 0$ for $0 \leq i \leq \delta - 2$. Let $(*)$ denote $c(a^{i+b}) = \sum_{l=0}^{n-1} c_l a^{l \cdot (i+b)}$.

Let $A = \{a^b, a^{b+1}, \ldots, a^{b+\delta-2}\}$ then $\underline{c} \cdot M(A)^T$ is:

$$\begin{aligned}
\underline{c} \cdot M(A)^T &= (c_0, c_1, \ldots, c_{n-1}) \begin{pmatrix} 1 & 1 & \ldots & 1 \\ a^b & a^{b+1} & \ldots & a^{b+\delta-2} \\ (a^2)^b & (a^2)^{b+1} & \ldots & (a^2)^{b+\delta-2} \\ \vdots & \vdots & \vdots & \vdots \\ (a^{n-1})^b & (a^{n-1})^{b+1} & \ldots & (a^{n-1})^{b+\delta-2} \end{pmatrix} \\
&= (c(a^b), c(a^{b+1}), \ldots, c(a^{b+\delta-2})) \\
&= \underbrace{(0, 0, \ldots, 0)}_{\delta-1}
\end{aligned}$$

Assume that d is a code word different from zero: $\underline{d} = d_0 d_1 \ldots d_{n-1} \in C \backslash \{0\}$, with $w(\underline{d}) < \delta$ and the positions in $d_{i_j} \neq 0$ are i_j for $1 \leq j \leq w(\underline{d})$.

Take a column number i_j, for $j = 1, \ldots, w(\underline{d})$ of $M(A) \to M$. **Claim:** $\underline{d} \cdot M^T = d \cdot M(A)^T$. Notice that $(d_{i_1}, d_{i_2}, \ldots, d_{i_{w(\underline{d})}}) \cdot M^T = \underline{d} \cdot M(A)^T = 0$. But this is a contradiction, since at most $\delta - 1$ columns of $M(A)$ are taken and $|A| = \delta - 1$, since A is gap free. Therefore, any $\delta - 1$ columns are linearly independent and $d_{i_1} \ldots d_{i_{w(d)}} \neq 0$ is a linear combination of those columns. □

Example 4.15. *Let $g(x) = x^3 + x + 1$ and $f(x) = x^7 - 1$ over $\mathbb{Z}_2 = GF(2)$, notice that $x^7 - 1 = x^7 + 1$, since in this field $+$ and $-$ do not matter. Such a construction forms a polynomial (linear) code, a $(7, 4)$-linear code C. Take a look at $g(a) = 0$. This means that it must be the case that $a^3 = a + 1$. What happens if a^3 is squared?*

$$\begin{aligned}
(a^3)^2 = (a^2)^3 = (a+1)^2 = a^2 + 1 \\
\Rightarrow g(a^2) = 0.
\end{aligned}$$

This can be repeated for $(a^4)^3$, from which it follows that $g(a^4) = 0$. Since g is a polynomial of degree 3 and the number of zeros is bounded by the degree, it follows that all the zeros are found. In $\mathbb{Z}_2(a)$ $g(x)$ has the zeros a, a^2 and a^4.

Notice that $A = \{a, a^2\}$ is a gap-free set. From which it follows that $b = 1$ and $\delta = 3$. This means that the minimal distance of C is minimal three: $w_{\min}(C) \geq 3$ and that there can be three errors detected and one error corrected.

Example 4.16. *The goal here is to construct a code over $GF(16) = GF(2^4)$, with a minimal distance of at least 5: $w_{\min} \geq 5$. Since $n = 2^4 - 1 = 15$, a cyclic code C is needed. A code C is cyclic if and only if $g(x) | x^{15} - 1$. Since the field is of characteristic 2, it follows that + and - do not matter, as in the previous example. It follows:*

$$\begin{aligned}
x^{15} - 1 &= x^{15} + 1 \\
&= (x+1)(x^2 + x + 1) \underbrace{(x^4 + x + 1)}_{g_1(x)} (x^4 + x^3 + 1) \underbrace{(x^4 + x^3 + x^2 + x + 1)}_{g_2(x)}
\end{aligned}$$

This is the complete characterization of the code. Start by looking at $g_1(x)$. Then $g_1(a) = 0 = g_1(a^2) = g_1(a^4) = g_1(a^k)$, for $k > 5$. Here the largest gap-free subset is $A = \{a, a^2\}$. Now, if

the polynomial $g_2(x)$ is chosen to look at, it turns out that $g_2(a^3) = 0$, of course this polynomial was right chosen. But with the polynomials $g_1(x)$ and $g_2(x)$ it follows that $g_1(x)g_2(x)$ has zeros a, a^2, a^3, a^4, which is the largest gap-free set, of size four. From which it follows that $b = 1$ and $\delta = 5$.

If $g_1(x)g_2(x)$ is taken as a generating polynomial of C, then $w_{\min}(C) \geq \delta = 5$. More general: if there is a primitive element, then $x^{p^n-1} - 1 = \prod_{k=1}^{p^n-1}(x - a^k)$. And for $GF(p^n)$: $x^{p^n} - x = \prod_{a \in K}(x - a)$.

4.3.4 Reed-Solomon-Codes

These kind of codes depend on the parameters $RS(s, k, t)$, where there are s bits in one block and k blocks in one record. A record can be regarded as a word of k blocks of s bits: $b = b_0 b_1 b_2 \dots b_{k-1}$ for $b_i \in GF(2^s)$, with coding $c = c_0 \dots c_{k-1} c_k c_{k+1} \dots c_{k+2t-1}$ and $c_i \in GF(2^s)$.

For a cyclic code: $GF(2^s)^k \to GF(2^s)k + 2t$, where s is free, $k+2t \leq 2^s-1$, $g(x) = \prod_{i=1}^{2t}(x - a^i)$ and a primitive element of $GF(2^s)$. An immediate consequence of this is the following theorem.

Theorem 4.18. *Let $w_{\min}(RS(s, k, t)) \geq 2t + 1$, then it is possible to detect $2t$ errors and correct t errors.*

On a CD a scratch will cause a **burst error**, a possible solution to this problem is **interleaving**. Let there be t code words and store them in a $t \times n$-matrix. Instead of reading row by row, the codes are read column by column, which gives a (nt, nk)-code.

4.3.5 Linear shift registers

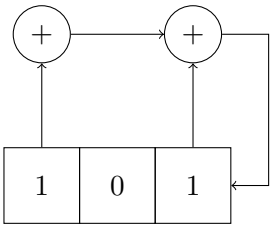


Figure 4.1: Example of a linear shift register, initialized with 101

Example 4.17. *Let there be a set of three registers, with in every register one bit, see figure... The example register generates the following code:* $101, 010, 100, 001, 011, 111, 110$. *Since there are only $2^3 = 8$ states, the code has to be periodic.*

More in general, there is a shift register of length k, taken over a field $GF(q)$. This means: there are q^k possible states and $q^k - 1$ non-zero states. In the general case as well, there is a finite number of possible states, from which it follows that a periodic sequence is generated.

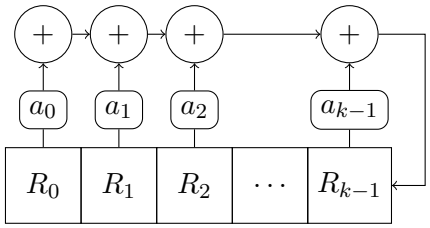


Figure 4.2: A general linear shift register

The sequences are vectors:

$$\underline{s}_0 = (s_0, s_1, s_2, \ldots, s_{k-1}) = (s_0^{(0)}, \ldots, s_0^{(k-1)})$$
$$\underline{s}_1 = (s_1, s_2, s_3, \ldots, s_{k-1}, \sum_{i=0}^{k-1} a_i s_i) = (s_1^{(0)}, \ldots, s_1^{(k-1)})$$
$$\underline{s}_{t+1} = (s_t^{(1)}, s_t^{(2)}, \ldots, s_t^{(k-1)}, \sum_{i=0}^{k-1} a_i s_t^{(i)}).$$

Then $s_0, s_1, s_2, \ldots, s_{n+k} = a_0 s_n + a_1 s_{n+1} + \ldots + a_{k-1} s_{n+k-1}$ is a linear recurrence with constant coefficients and order k. These can be described as a generating function, which is always rational:

$$S(x) = \sum_{n \geq 0} s_n x^n = \frac{g(x)}{f(x)}.$$

Where $f(x), g(x)$ are polynomials, with $f(x) = 1 - a_{k-1}x - a_{k-2}x^2 - \ldots - a_0 x^k$ and $\deg(g(x)) < k$.

Example 4.18. *Start with the following shift register, over field $K = GF(2)$, $k = 4$. Define the sequence as: $(a_0, a_1, a_2, a_3) = (1, 1, 0, 1)$, then $f(x) = x^4 + x^3 + x + 1$. Assume that the initial vector is $\underline{s}_0$. With all this, take a look at the following four examples in table 4.1:*

(a) period 6	(b) period 3	(c) period 2	(d) period 1
$\underline{s}_0 =$ 1000	$\underline{s}_0 =$ 1001	$\underline{s}_0 =$ 1010	$\underline{s}_0 =$ 1111
0001	0010	0101	
0011	0100		
0111			
1110			

Table 4.1: Different period-length with different initial vector $\underline{s}_0$

Now take another polynomial/shift register: $f(x) = x^4 + x^3 + 1 \hat{=} (1, 1, 0, 0)$. And take $\underline{s}_0 = 1000$. Then the following sequence of codes are generated:

$$\begin{aligned}\underline{s}_0 = \quad & 1000\\ & 0001\\ & 0010\\ & 0100\\ & 1001\\ & 0011\\ & 0110\\ & 1101\\ & 1010\\ & 0101\\ & 1011\\ & 0111\\ & 1111\\ & 1110\\ & 1100\end{aligned}$$

Since the words are of length 4, it follows that the maximal period is $2^4 - 1 = 15$*, this is an example of a initial vector that generates a code sequence of maximum period. Take a look at the polynomial* $x^4 + x^3 + x + 1$*:*

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

However, the polynomial $x^4 + x^3 + 1$ *is irreducible over* $GF(2)$*. Is this why a sequence of maximum period can be generated? This would suggest that if something has to look random, a code with many bits and maximum period is needed. Can this be done with irreducible polynomials?*

Theorem 4.19. *Let* (s_n) *be a shift register sequence (SRS) and let* $f(x)$ *be irreducible. Then* t *is a period, i.e.* $s_{n+t} = s_n, \forall n \in \mathbb{N}$ *if and only if* $f(x)|x^t - 1$*.*

Proof.
" $\Rightarrow$ ": Let $s_{n+t} = s_n \forall n \in \mathbb{N}$. Then for $S(x)$ it follows:

$$\begin{aligned}S(x) &= (s_0 + s_1x + \ldots + s_{t-1}x^{t-1})(1 + x^t + x^{2t} + \ldots)\\ &= \underbrace{(s_0 + s_1x + \ldots + s_{t-1}x^{t-1})}_{\sigma(x)} \frac{1}{1 - x^t} = \frac{\sigma(x)}{1 - x^t}\end{aligned}$$

Notice that $\frac{\sigma(x)}{1-x^t} = \frac{g(x)}{f(x)}$ with $f(x)$ irreducible. This implies: $f(x)|x^t - 1$.

" $\Leftarrow$ ": Assume that $f(x)|x^t - 1$, this implies: $\exists q(x) : f(x)q(x) = 1 - x^t$, then $S(x) = \frac{g(x)}{f(x)} =$

$\frac{g(x)q(x)}{1-x^t}$ and still $\deg(g(x)q(x)) < t$, which implies that:

$$\begin{aligned} s(x) &= g(x)q(x) + x^t S(x) \\ s(x) &= \sum s_n x^n \\ g(x)q(x) &= \sum l = 0^{t-1} h_l x^l \\ S(x) &= \sum s_n x^{n+t}. \end{aligned}$$

This means that $s_{n+t} = s_n$ from which it follows that t is indeed a period. □

Corollary 4.5. *$\exists t \leq q^n - 1$ such that $f(x)|x^t - 1$.*

Theorem 4.20 (Fundamental theorem on SRS)**.** *Let $(s_n)_{n\in\mathbb{N}}$ be a shift register over $GF(q)$, with a register of length k and generating function: $S(x) = \sum_{n\geq 0} s_n x^n = \frac{g(x)}{f(x)}$. Then the minimal period of $(s_n)_{n\in\mathbb{N}}$ is $q^n - 1$ (which is optimal) if and only if $f(x)$ is a primitive polynomial.*

Proof. The polynomial $f(x)$ is a primitive polynomial if and only if $f(x)$ is irreducible and $\forall t < q^n - 1 : f(x) \nmid x^t - 1$ and $f(x)|x^{q^k} - 1$ if and only if $\forall t < q^k - 1$ t is not a period of $(s_n)_{n\in\mathbb{N}}$ and $q^k - 1$ is a period of $(s_n)_{n\in\mathbb{N}}$. This means that the minimal period length is already the maximal possible period length. □

Appendix A

Algebraic Structures

Definition A.1. *A set R with the arithmetic operations $+$ and $\cdot$ is called a* ***ring*** $(R, +, \cdot)$ *if*

- $(R, +)$ *is an* ***Abelian group****:*
  - *closure:* $a, b \in R \implies a + b \in R$
  - *existence of additive identity:* $\exists 0 : \forall a \in R\, a + 0 = a, 0 + a = a$
  - *additive inverses:* $\forall a \in R\, \exists(-a) : a + (-a) = 0$
  - *commutativity:* $\forall a, b \in R\, a + b = b + a$
  - *associativity:* $\forall a, b, c \in R\, (a + b) + c = a + (b + c)$
- $(R, \cdot)$ *is a* ***semigroup***
  - *closure* $a, b \in R \implies a \cdot b \in R$
  - *associativity:* $\forall a, b, c \in R\, (a \cdot b) \cdot c = a \cdot (b \cdot c)$
- *distributivity*
  - $a \cdot (b + c) = a \cdot b + a \cdot c$
  - $(b + c) \cdot a = b \cdot a + c \cdot a$

  Note: Since the multiplicative structure $(R, \cdot)$ does not have to be commutative, both distributive law are needed.

This is a very basic structure, which can be equipped with further properties, like
- commutativity of the multiplication: $a \cdot b = b \cdot a$
- unity (multiplicative identity): $a \cdot 1 = 1 \cdot a = a$

If both properties are present in R, then R is called a **commutative ring with 1 element**.

Definition A.2. *A commutative ring with 1 element is called an* ***integral domain*** *if it does not contain zero-divisors, i.e.*

$$a \cdot b = 0 \implies a = 0 \text{ or } b = 0$$

$$R \text{ is an inegral domain} \iff \nexists a, b \in R \backslash \{0\} : a \cdot b = 0$$

Example A.1.
- $(\mathbb{R}, +, \cdot)$

- $(\mathbb{Z}_m, +, \cdot), m \in \mathbb{P}$
  If $m \notin \mathbb{P}$ then $m = n \cdot k$ (factorization) and $\bar{n} \cdot \bar{k} = \bar{m} = \bar{0}$. This means, for example, that $\mathbb{Z}_6$ is not an integral domain since $\bar{2} \cdot \bar{3} = \bar{0}$

- $\mathbb{Z}[x] = (\{a_0 + a_1 x + a_x x^2 + \ldots + a_n x^n \mid a_i \in \mathbb{Z}, n \in \mathbb{N}\}, +, \cdot)$

Definition A.3. *R is a **Euclidean ring** if R is an integral domain and there is a Euclidean function n:*

$$n : R \to \mathbb{N} \text{ such that } \forall a, b \in R,\ b \neq 0,\ \exists q, r \in R :$$

1. $a = bq + r$ *with* $n(r) < n(b)$ *or* $r = 0$
2. $\forall a, b \in R \backslash \{0\} : n(a) \leq n(ab)$

($\rightsquigarrow$ division with remainder)

Definition A.4. *A set K with the arithmetic operations $+$ and $\cdot$ is called a **field** $(K, +, \cdot)$ if*

- $(K, +)$ *is an **abelian group***
- $(K \setminus \{0\}, \cdot)$ *is an **abelian group***
- *The distributive laws hold.*

The algebraic structures discussed in this section have the following relations:

$$\text{rings} \supseteq \text{commutative rings} \supseteq \text{integral domains} \supseteq \text{Euclidean rings} \supseteq \text{fields}.$$

Example A.2. *Every integral domain is a ring and every field is an integral domain, but not vice versa.*

Bibliography

[1] MK Agoston. Algebraic topology, a first course. 1976.

[2] Martin Aigner. Combinatorial theory. *Heidelberg, New York*, 1979.

[3] Mark Anthony Armstrong. *Basic topology*. Springer, 1983.

[4] Reinhard Diestel. *Graph Theory {Graduate Texts in Mathematics; 173}*. Springer-Verlag Berlin and Heidelberg GmbH & Company KG, 2000.

[5] Dieter Jungnickel and Tilla Schade. *Graphs, networks and algorithms*, volume 5. Springer, 2005.

[6] William Thomas Tutte. *Introduction to the Theory of Matroids*. American Elsevier New York, 1971.