Discrete Mathematics

Kellerkinder

January 24, 2026

1 Graph Theory

1.1 Definition & Notation

- $G=(V,E)$
- Directed Edge $e=(v,w)$; $v\to w$
- Undirected Edge $e=\{v,w\}=\{w,v\}=vw$
- $d(v)$... degree
  - $d^+(v)$... out-degree
  - $d^-(v)$... in-degree
- $\Gamma(v)$... set of neighbours
  - $\Gamma^+(v)$... successors
  - $\Gamma^-(v)$... predecessors

Walk, Trail Circuit

- **Walk**: sequence of edges (no jumps)
  - $\exists$ walk v to w: $v\sim w$
- **Trail**: sequence of edges (no jumps, no repeating edges)
  - **Circuit/Closed Trail**: same start and end vertex
- **Path**: no repeating edges, no repeating vertices
  - **Cycle/Closed Path**: same start and end vertex

Handshaking Lemma

$$\sum_{v\in V} d(v)=2|E| \text{ or } \sum_{v\in V} d^+(v)=\sum_{v\in V} d^-(v)=|E|$$

1.2 Trees & Forests

Isomorphism

$G\cong H \iff \exists\varphi: V(G)\mapsto V(H)$ and $vw\in E(G)\iff \varphi(v)\varphi(w)\in E(H)$

Spanning Subgraphs & Spanning Forests

Spanning Forest $\iff$

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

If G connected $\Rightarrow F$ *spanning tree*

Minimum or Maximum Spanning Trees

- $G=(V,E)$ and weight function $w: E\to\mathbb{R}, e\mapsto w(e)$. Then $T=(V,F)\subseteq G$ *minimum spanning tree* if $w(F)$ minimal
- `GREEDY(V, E, w)` constructs the minimum spanning tree (MST):
  - Sorts the edges of G by weight ascending
  - Adds the next smallest edge to T (such that T remains a tree) until G is spanned

Matrix-Tree-Theorem (Kirchhoff)

$G=(V=\{v_1,...,v_n\},E)$ simple, undirected, connected, with adjacency matrix A
$D=\mathrm{diag}(d(v_1),...,d(v_n))$; $(D-A)':=(D-A)$ without 1 row and 1 column
$\Rightarrow \det((D-A)')=$ number of spanning trees of G

Independence Systems

Independence System (E,S): $S\subseteq 2^E$ and S is closed under inclusion. $A\in S\wedge B\subseteq A\Rightarrow B\in S$

Matroids & GREEDY

An independence system $M=(E,S)$ is called a matroid if $\forall A,B\in S$ such that $|B|=|A|+1$: $\exists v\in B\setminus A$ with $A\cup\{v\}\in S$
Let $G=(V,E)$ be an undirected graph and $S=\{F\subseteq E \mid F$ is a forest$\}$; then (E,S) is a matroid.
If $M=(E,S)$ is a matroid with a weight function $w: E\mapsto\mathbb{R}$ then `GREEDY` computes a A maximal/minimal weight with respect to the inclusion.

1.3 Special Graphs

Planar Graphs

Definition: 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 edges intersect. A graph is planar $\iff$ there is **no** subgraph which is a subdivision of K_5 or of $K_{3,3}$.
Euler's Polyhedron Formula: if G is connected and planar graph, then $\alpha_0-\alpha_1+\alpha_2=2$. α_0... Vertices, α_1... Edges, α_2... Faces
Dual Graphs: 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.

Bipartite Graphs and Matching

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

- $V=V_1\cup V_2$, $V_1\cap V_2=\emptyset$
- $vw\in E\Rightarrow v\in V_1, w\in V_2$

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 $wm\in E\iff wFm$. A *feasible marriage* is a matching of W $F_l\subseteq F$ (i.e $\forall x\in W: \exists! y\in M$ such that xF_ly). Now the theorem states the following: there is a feasible marriage, if and only if: $\forall W_0\subseteq W: |\{y\in M \mid \exists x\in W_0: xFy\}|\geq|W_0|$ or in different words: $|\bigcup_{w\in W_0}\Gamma(w)|\geq|W_0|$

1.4 Graph Colorings

- **Vertex Coloring:** $c: V\to C$ where a C is a set of colors. *feasible* if $vw\in E\Rightarrow c(v)\neq c(w)$
- **Edge Coloring:** $\bar{c}: E\to C$
- everything that can be done with a vertex coloring can also be done with an edge coloring
- **Chromatic Number:** $\chi(G)$ is the minimal number of colors such that there is a feasible coloring.
  - $\chi(K_n)=n$
  - $\chi(K_{n,m})=2$
  - $\chi(T)=2$ if T is a tree and $|V|>1$
  - $\chi(G)=1\iff E(G)=\emptyset$
  - $\chi(G)=2\iff E(G)\neq\emptyset$ and G is bipartite
  - $\chi(G)=2\iff E(G)\neq\emptyset$ and all cycles have **even** length
  - $\chi(G)\leq 1+\max_{v\in V} d(v)$
  - G is planar $\Rightarrow \chi(G)\leq 5$

Ramsey Theory

- **Definition:** 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.
  - Coloring is edge coloring
- $R(r,s)\leq R(r-1,s)+R(r,s-1)$
- $R(n_1,n_2,...,n_r)=\min\{n \mid$ all r-edge colorings of K_n (colors $c_1,...,c_r$) have a c_j-colored K_{n_j} for some $j\}$

2 Advanced Combinatorics

Double Counting

Given two sets A and B and a relation $R\subseteq A\times B$, such that $aRb\iff(a,b)\in R$: Let $R_i=\{b\in B \mid a_iRb\}$ (all b related to a) and $S_j=\{a\in A \mid aRb_j\}$. Then: $|R|=\sum_{i=0}^n|R_i|=\sum_{j=0}^m|S_j|$

Pigeon Hole Principle

Let $A_1,...A_k$ be finite pairwise disjoint sets, $|A_1\cup...\cup A_k|>k\cdot r$, for $r\in\mathbb{N}$; This implies: $\exists i: |A_i|>r$. If $r=1$, then it follows that: $f: A\mapsto B, |A|>|B|\Rightarrow\exists b\in B: |f^{-1}(b)|\geq 2$

Principle of Inclusion & Exclusion

$|A_1\cup...\cup A_2|=\sum_{\emptyset\neq I\subseteq\{1,...,n\}}(-1)^{|I|+1}|\bigcap_{i\in I}A_i|$
For $|A\cup B\cup C|=|A|+|B|+|C|-|A\cap B|-|A\cap C|-|B\cap C|+|A\cap B\cap C|$
If the sets are not necessarily pairwise disjoint, then:

$$A_1,...A_n\subseteq |A\setminus\bigcap_{i=1}^n A_i|=|A|+\sum_{\emptyset\neq I\subseteq\{1,...,n\}}(-1)^{|I|}|\bigcap_{i\in I}A_i| = \sum_{I\subseteq\{1,...,n\}}(-1)^{|I|}|\bigcap_{i\in I}A_i|$$

2.1 Enumerative Combinatorics

Counting Sets

6 Basic Problems:

1. # of permutations: $n!$
2. # of k-subsets of A: $\binom{n}{k}$
3. # of ordered k-subsets: $k!\binom{n}{k}$
4. # of k-multisets (elements can be used more than once): $\binom{n+k-1}{k}$
5. # of arrangements of a multiset (element b_i appears k_i times): $\frac{n!}{k_1!k_2!...k_m!}$
6. # of ordered k-multisets: n^k

Stars and bars: Number of assignments of n items into k boxes $\binom{n+k-1}{k-1}$

Useful theorems:

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

Vandermonde: $\forall n\in\mathbb{N}, \forall x,y\in\mathbb{C}$ and $k\in\mathbb{N}$: $\binom{x+y}{n}=\sum_{k=0}^n\binom{x}{k}\binom{y}{n-k}$

Binomials: $(1+b)^k=\sum\binom{k}{i}b^i$

in general: $\binom{a}{k}=\frac{a^{\underline{k}}}{k!}=\frac{a(a-1)(a-2)...(a-(k-1))}{k!}=\frac{1}{k!}\cdot\prod_{i=0}^{k-1}n-i$

$n!\cdot 2^n=(1\cdot 2)\cdot(2\cdot 2)\cdot...\cdot(n\cdot 2)$

$\frac{(2n)!}{n!2^n}=1\cdot 3\cdot...\cdot(2n-1)$

Stirling Numbers

First kind: $s_{n,k}=$ # of permutations of $\{1...n\}$ with k cycles

- $s_{n,1}=(n-1)!$, $s_{n,n-1}=\binom{n}{2}$, $s_{n,n}=1$
- $s_{n,0}=0$, $s_{0,n}=0$, $s_{0,0}=1$ (!!)
- $\sum_{k=1}^n s_{n,k}=n!$

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

Second kind: $S_{n,k}=$ # of k partitions of $A=\{1...n\}$
$\Leftrightarrow \forall i: A_i\neq\emptyset$, $i\neq j\Rightarrow A_i\cap A_j=\emptyset$, $\bigcup_{i=1}^k A_i=A$

- $S_{n,1}=1$, $S_{n,n-1}=\binom{n}{2}$, $S_{n,n}=1$
- $S_{n,0}=0$, $S_{0,n}=0$, $S_{0,0}=1$ (!!)
- $S_{n,2}=2^{n-1}-1$

$\forall n,k>0: S_{n,k}=S_{n-1,k-1}+kS_{n-1,k}$

2.2 Generating Functions

Definition & Properties

Let $(a_n)_{n\geq 0}, a\in\mathbb{C}$ be a sequence; Then $A(z)=\sum_{n\geq 0}a_nz^n$ is the **generating function** of a_n.

- $A(z)+B(z)=\sum_{n\geq 0}(a_n+b_n)z^n$ (linearity)
- $A(z)B(z)=\sum_{n\geq 0}\sum_{k\geq 0}a_kb_{n-k}z^n$ (Cauchy-Schwarz Product)
- $A(z)/B(z)=C(z)$, when $b_0\neq 0$

Operations on Generating Functions

- $(\alpha a_n+\beta b_n)_{n\geq 0}\Leftrightarrow\alpha A(z)+\beta B(z), \alpha,\beta\in\mathbb{C}$
- $(\gamma^na_n)_{n\geq 0}\Leftrightarrow A(\gamma z)$
- $1\doteq(1)_{n\geq 0}\Leftrightarrow\frac{1}{1-z}=\sum_{n\geq 0}z^n$
- $(a^n)_{n\geq 0}\Leftrightarrow\frac{1}{1-az}=\sum_{n\geq 0}a^nz^n$
- $\frac{1-z^{n+1}}{1-z}=\sum_{k=0}^n z^k$
- $\sum_{n\geq 0}\frac{z^n}{n!}=e^z$
- $(a_{n-1})_{n\geq 1}\Leftrightarrow zA(z)$ (index shift)
- $(na_n)_{n\geq 0}\Leftrightarrow zA'(z)$ (derivative)
- $\frac{1}{(1-z)^k}=(1-z)^{-k}=\sum\binom{n+k-1}{k-1}z^n=\sum_{n\geq 0}\binom{n+k-1}{n}z^n$ (transform back)

Unlabelled Combinatorial Structures

Combinatorial structure: $(A,|\cdot|)$, $A\neq\emptyset$; $|\cdot|$ is weight function; $\forall x\in A$: $|x|\in\mathbb{N}$
Counting sequence of A: $(a_n)_{n\geq 0}, a_n=|\{x\in A: |x|=n\}|<\infty$; "How many x of weight n?"
The counting sequence has a generating function $A(z)$, also called generating function of A.

1. $C=A\cup B, A\cap B=\emptyset$; $(A,|\cdot|_A),(B,|\cdot|_B)$; $|x|_c=\begin{cases}|x|_A & \text{if } x\in A\\ |x|_B & \text{if } x\in B\end{cases}$
   $c_n=a_n+b_n\Rightarrow C(z)=A(z)+B(z)$
2. $C=A\times B$, $(x,y)\in C$, $x\in A, y\in B$; $|(x,y)|=|x|_A+|y|_B$
   $c_n=\sum_{k=0}^n a_kb_{n-k}\Rightarrow C(z)=A(z)\cdot B(z)$
3. $C=\mathrm{seq}(A)=\{\varepsilon\}\cup(x_1,x_2,...x_k)_{k\geq 0}=\{\varepsilon\}\cup A\cup A^2\cup A^3\cup...$; $|x|_C=\sum_{i=1}^k|x_i|_A$
   $C(z)=\frac{1}{1-A(z)}$, only if we define $a_0=0$
4. $C=\mathrm{seq}_{k\leq y}(A)=\{\varepsilon\}\cup(x_1,x_2,...x_k)_{k\leq y}$, $C(z)=\frac{1-A(z)^{y+1}}{1-A(z)}$ (finite sequence)
5. $C=\mathrm{set}(A)=2^A$ (power set)
   $C(z)=\exp\left(\sum_{k\geq 1}\frac{(-1)^{k-1}}{k}A(z^k)\right)$

Labelled Combinatorial Structures

Labelled combinatorial structure: Elements are numbered $\Longrightarrow$ switching of two equal elements does make a difference! $\hat{A}(z)=\sum_{n\geq 0}a_n\frac{z^n}{n!}$

1. $\hat{C}=\hat{A}\cup\hat{B}, \hat{A}\cap\hat{B}=\emptyset$; $(\hat{A},|\cdot|_{\hat{A}}),(\hat{B},|\cdot|_{\hat{B}})$; $|x|_c=\begin{cases}|x|_{\hat{A}} & \text{if } x\in\hat{A}\\ |x|_{\hat{B}} & \text{if } x\in\hat{B}\end{cases}$
   $c_n=a_n+b_n\Rightarrow\hat{C}(z)=\hat{A}(z)+\hat{B}(z)$
2. $\hat{C}=\hat{A}*\hat{B}$, $\hat{C}=\{(x,y) \mid x\in\hat{A}, y\in\hat{B}; x,y$ labelled in order preserving way$\}$; $|(x,y)|=|x|_{\hat{A}}+|y|_{\hat{B}}$; $\hat{C}(z)=\hat{A}(z)\cdot\hat{B}(z)$
3. $\hat{C}=\mathrm{seq}(\hat{A})=\{\varepsilon\}\cup(x_1,x_2,...x_k)_{k\geq 0}=\{\varepsilon\}\cup\hat{A}\cup\hat{A}^2\cup\hat{A}^3\cup...$
   $\hat{C}(z)=\frac{1}{1-\hat{A}(z)}$
4. $\hat{C}=\mathrm{set}(\hat{A})=2^{\hat{A}}$ (labelled power set)
   $\hat{C}(z)=\sum_{k\geq 0}\frac{\hat{A}(z)^k}{k!}=\exp(\hat{A}(z))$
5. $\hat{C}=\mathrm{cyc}(\hat{A})$; $\hat{C}(z)=\sum_{k\geq 0}\frac{\hat{A}(z)^k}{k}=\log\left(\frac{1}{1-\hat{A}(z)}\right)$
6. $\hat{C}=\mathrm{set}(\mathrm{cyc}(\hat{A}))=\frac{1}{1-\hat{A}(z)}$

3 Number Theory

3.1 Divisibility & Factorization

GCD

Let $a,b\in\mathbb{Z}$; then $d=\gcd(a,b)\iff$

- $d|a$ and $d|b$ (makes it divisor)
- $t|a$ and $t|b\Rightarrow t|d$ (makes it greatest)

Euclidean Algorithm

$a,b\in\mathbb{Z}\setminus\{0\}, d=\gcd(a,b)\iff\exists e,f\in\mathbb{Z}$ such that $d=ae+bf$ (*Bézout's Identity*)

Commutative Ring (with 1)

- $(R,+)$ is an **Abelian group** (0-element, $\forall a: \exists -a$)
- $(R,\cdot)$ is a **semigroup** (additionally: $\exists$ neutral element, distributive law holds)
- R is an **integral domain** $\iff\nexists a,b\in R\setminus\{0\}: a\cdot b=0$

Euclidean Ring

R is a **Euclidean ring** if R is an **integral domain** and there is a *euclidian function* $n: R\to\mathbb{N}$ 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. $\forall a,b\in R\setminus\{0\}: n(a)\leq n(a\cdot b)$

- **Units:** $R^*=\{a\in R: \exists a^{-1}\}$

Field

A field is a **commutative group** with two operations: *addition* and *multiplication* such that

- $(K,+)$ is an **Abelian group**
- $(K\setminus\{0\},\cdot)$ is an **Abelian group**
- the distribute laws hold

Prime Numbers

- $p\in\mathbb{P}\iff\pm 1$ and $\pm p$ are the only divisors of p
- let $n\in\mathbb{N}^+$, then $\exists p_1,p_2,...p_r\in\mathbb{P}$ such that $p_1^{e_1}\cdot p_2^{e_2}\cdot...\cdot p_r^{e_r}=n$, for $r\geq 0$
- $\nu_p(n)$... multiplicity of p in the factorization of n (*Factorization is unique up to the order of the factors*)
  - $\gcd(a,b)=\prod_{p\in\mathbb{P}}p^{\min(\nu_p(a),\nu_p(b))}$
  - $\mathrm{lcm}(a,b)=\prod_{p\in\mathbb{P}}p^{\max(\nu_p(a),\nu_p(b))}$
  - $a|b\iff\forall p\in\mathbb{P}: \nu_p(a)\leq\nu_p(b)$
  - $n=\prod_{p\in\mathbb{P}}p^{\nu_p(n)}$
- $|\mathbb{P}|=\infty$

3.2 Congruence Relations and Residue Classes

A *residue class* is defined as: $a+m\cdot\mathbb{Z}=\bar{a}$, where $a+m\cdot\mathbb{Z}=\{a+k\cdot m \mid k\in\mathbb{Z}\}$ (notice $\bar{a}\subsetneq\mathbb{Z}$ and $\bar{a}=\overline{a+m}$). Definition: $\bar{a}+\bar{b}:=\overline{a+b}$ and $\bar{a}\cdot\bar{b}:=\overline{a\cdot b}$

- Let $\bar{a}\in\mathbb{Z}_m$, then the *inverse element* is defined as follows: $\bar{x}\in\mathbb{Z}_m$ such that: $\bar{x}\cdot\bar{a}=\bar{1}$ then $\bar{x}=\bar{a}^{-1}$.
- $\exists\bar{a}^{-1}\in\mathbb{Z}_m\iff\gcd(a,m)=1$

Prime Residue Classes

$\mathbb{Z}_m^*=\{\bar{a}\in\mathbb{Z}_m \mid \gcd(a,m)=1\}$ contains all invertible elements, can further be defined as $\mathbb{Z}_m^*=\{x\in\mathbb{Z}_m \mid \exists x^{-1}: x\cdot x^{-1}=1\}$ (also called **Group of Units**)

- Some rules:
  - $ab\equiv ac(m)\Rightarrow b\equiv c(m)$
  - $ab\equiv ac(m)\Rightarrow b\equiv c(m)$ if $ax\equiv 1(m)$ has a solution $\iff\gcd(a,m)=1$

3.3 Systems of Congruences

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 $b_j=\left(\frac{m}{m_j}\right)^{-1}\bmod m_j$.
The chinese remainder theorem can be applied to all **euclidean rings**

3.4 Euler-Fermat Theorem

Euler's Totient Function

$\varphi(m)=|\{x \mid 0\leq x\leq m-1, \gcd(x,m)=1\}|=|\mathbb{Z}_m^*|$
Two cases:

1. Suppose $m\in\mathbb{P}$, then $\varphi(m)=m-1$
2. $m=p^e$, for $p\in\mathbb{P}$ and $e\geq 1$: Now $\bar{a}\in\mathbb{Z}_m\Rightarrow\gcd(a,p^e)=\begin{cases}1 & \text{if } \bar{a}\in\mathbb{Z}_m^*\\ p^f & \text{with } 1\leq f<e\end{cases}$

Let $m=p_1^{e_1}p_2^{e_2}...p_r^{e_r}$, then: $\varphi(m)=m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_r}\right)$

Fermat's Little Theorem

If $\gcd(a,m)=1$ then $a^{\varphi(m)}\equiv 1(m)$. In particular: $p\in\mathbb{P}, p\nmid a\Rightarrow a^{p-1}\equiv 1(p)$
Theorem: Let $p,q\in\mathbb{P}\setminus\{2\}$ such that $p\neq q$. Let $m=p\cdot q$ and $v=\mathrm{lcm}(p-1,q-1)$; then $\forall a,k\in\mathbb{Z}: a^{kv+1}\equiv a(m)$

3.5 RSA-Algorithm

- (m,e)... public key
- (m,d)... private key
- **Encryption:** $E(a_j)=b_j:=a_j^e \bmod m$
- **Dencryption:** $D(b_j)=a_j:=b_j^d \bmod m$
- # number of fixpoints: $\gcd(e-1,p-1)\cdot\gcd(e-1,q-1)$

Groups and Cyclic Groups

- **Group:** Let G be a group and $x\in G$, then $\mathrm{ord}_G(x)=\min\{i\in\mathbb{N}^+ \mid x^i=e\}$. If e is the neutral element, then $\mathrm{ord}_G(e)=1$ since $e^1=e$. If $a\neq e$, then $\mathrm{ord}_G(a)>1$
- **Cyclic Group:** Let $\langle x\rangle$ denote the group generated by x. Examples
  - $\langle e\rangle=\{e\}$ is the trivial group
  - $\langle x\rangle=\{e,x,x^2,x^3,...\}$
  - $\mathbb{Z}_m^*$ is cyclic
    - $\iff\exists$ primitive root mod m
    - $\iff m\in\{2,4\}\cup\{p^e \mid p\in\mathbb{P}\setminus\{2\}, e\geq 1\}\cup\{2p^e \mid p\in\mathbb{P}\setminus\{2\}, e\geq 1\}$
- **Primitive Root mod** m: $\bar{a}\in\mathbb{Z}_m^*$ then $\langle\bar{a}\rangle=\mathbb{Z}_m^*\Rightarrow\mathbb{Z}_m^*=\{\bar{a},\bar{a}^2,\bar{a}^3,...,\bar{a}^{\varphi(m)}\}$ (Hint: $\bar{a}^{\varphi(m)}=1$)

The Order of Elements

$\mathrm{ord}_G(x)=|\langle x\rangle|$; Obviously $\mathrm{ord}_G(x)$ divides $|G|$, since $\langle x\rangle\leq G$

- Let $\mathrm{ord}(a)=r$; then $\mathrm{ord}(a^k)=\frac{r}{\gcd(r,k)}$
- $\exists a,b\in G: \mathrm{ord}(a)=r, \mathrm{ord}(b)=s\Longrightarrow\exists c\in G: \mathrm{ord}_G(c)=\mathrm{lcm}(r,s)$
- From the above follows: $\mathrm{ord}_G(a)$ maximal $\Longrightarrow\forall b\in G: \mathrm{ord}_G(b) \mid \mathrm{ord}_G(a)$
- In general: a is generator of finite field $K\setminus\{0\}\iff\bar{a}\in K\setminus\{0\}\wedge K\setminus\{0\}=\{\bar{a},\bar{a}^2,\bar{a}^3,...,\bar{a}^{\mathrm{ord}(K)-1}\}$
- Let $a_1,...,a_r$ with $\mathrm{ord}(a_i)=k_i$. Then $\exists a\in G$ such that $\mathrm{ord}(a)=\mathrm{lcm}(k_1,...,k_r)$.

Carmichel Function

Is defined as $\lambda(m)=\max\{\mathrm{ord}_{\mathbb{Z}_m^*}(\bar{a}) \mid \bar{a}\in\mathbb{Z}_m^*\}$, the maximal order of a unit.

- $\lambda(m) \mid \varphi(m)$
- $p\in\mathbb{P}\setminus\{2\}\Rightarrow\lambda(p^e)=\varphi(p^e)=p^{e-1}(p-1)$
- $\lambda(1):=\varphi(1)=1$
- $\lambda(2):=\varphi(2)=1$
- $\lambda(4):=\varphi(4)=2$
- $\lambda(2^e)=2^{e-2}$ for $e\geq 3$
- $\lambda\left(\prod_{i=1}^r p_i^{e_i}\right)=\mathrm{lcm}(\lambda(p_1^{e_1}),...,\lambda(p_r^{e_r}))=L$

4 Polynomial over Finate Fields

4.1 Rings

Ring:

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

Euclidean Ring:

- is an integral domain with $n: R\setminus\{0\}\to\mathbb{N}$ a *euclidian function* n such that $\forall a,b\in R, b\neq 0: \exists q,r\in R$:
  - $a=b\cdot q+r$
  - $n(r)<n(b)$ or $r=0$
  - $n(a)\leq n(ab)$
- $a|b\Rightarrow n(a)\leq n(b)$

Integral Domain:

- commutative ring with 1-element
- no zero divisors ($a\cdot b=0\Rightarrow a=0\vee b=0$)

Generalization of prime numbers

Let R be an *integral domain*, and let $a\in R\setminus(\{0\}\cup R^*)$, i.e. $\nexists a^{-1}$; then a is **irreducible** $\Leftrightarrow a=b\cdot c$ always implies that either $b\in R^*$ or $c\in R^*$. The element is called a **prime element** $\Leftrightarrow a|b\cdot c\Rightarrow a|b\vee a|c$. In general these are two different concepts.

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

(Unique) Factorial Rings (UFD)

Let R be an *integral domain*, such that $\forall a\in R\setminus(\{0\}\cup R^*)$ there exists an **unique representation** (up to order) $a=\varepsilon p_1p_2...p_k$, where $\varepsilon\in R^*$ and $p_1,...,p_k$ are prime elements.

- R is called a **factorial ring** or **unique factorization domain (UFD)**
- Every Euclidean ring is a factorial ring.

Recap: Cosets & Subgroups

$(G,*)$ is a group, let U be a subgroup: $U\subseteq G: a*U=\{a*x \mid x\in U\}$. These sets form a partition of the group. If $a\neq a'$, then either $a*U=a'*U$ or $(a*U)\cap(a'*U)=\emptyset$. Define the **left coset** to be the elements $a*U$ with $a\in G$ and the **right coset** to be the elements $U*a$ with $a\in G$.
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 this holds, then:

- $(a*U)*(b*U)=(a*b)*U$

The group $(G/U,*)$ is called the **quotient group**. Where G/U read as "*G modulo U*", is defined as: $G/U=\{a*U \mid a\in G\}$ Example: $\mathbb{Z}_4=\mathbb{Z}/(4*\mathbb{Z})$ with +

Ideals in Rings

Definition: Let R and S be rings, with 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: $\mathrm{kern}(\varphi)=\{x\in R \mid \varphi(x)=0\}$
Definition: Let R be a ring, $I\subseteq R$ is an **ideal** if:

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

Let $\varphi: R\to S$ be a homomorphism, then $\mathrm{kern}(\varphi)$ is an ideal of R.
Furthermore, $I\subseteq R$ is an ideal of R if and only if $\varphi(I)\subseteq S$ is an ideal of S
Theorem: Let R be a ring and $I\subseteq R$ an ideal. Define $+$ and $\cdot$ on $R/I=(R,+)/(I,+)$, called R modulo I, as follows:

- $(a+I)+(b+I):=(a+b)+I$ with $a,b\in R$
- $(a+I)\cdot(b+I):=(a\cdot b)+I$ with $a,b\in R$

This definiton $(R/I,+,\cdot)$ is called the **quotient ring** R modulo I.
Corollary: A field K has only the trivial ideals $\{0\}$ and K.
Definition: An ideal generated by only one element a (or $-a$) is called a **principal ideal**, written as (a).
Theorem: Let R be an Euclidean ring. Then every ideal is a principal ideal, i.e. R is a **principal ideal domain**.

Ring hierachy

Field $\subsetneq$ Euclidian ring $\subsetneq$ Principal ideal domain $\subsetneq$ Factorial ring (=Unique Factorization Domain) $\subsetneq$ Integral domain $\subsetneq$ Commutative ring $\subsetneq$ Ring

4.2 Fields

Prime Field & Characteristic

Definition: $\bigcap_{K' \text{ subfield of } K}K'$ is called the **prime field** (smallest field) of K, denoted by $P(K)$. Every field must include at least **0** and **1**.
Definition: $\mathrm{ord}_{(K,+)}(1)$ is called the **characteristic of K**, denoted by $\mathrm{char}(K)$, where $\mathrm{ord}_G(a)=\min\{i>0 \mid a^i=e\}$. If the order is ∞, then the $\mathrm{char}(K)=0$. Examples:

- $(\mathbb{R},+,\cdot)$: $\mathrm{char}(\mathbb{R})=0$, same for $\mathbb{Q},\mathbb{C}$
- $(\mathbb{Z},+,\cdot)$: $\mathrm{char}(\mathbb{Z}_2)=2$, $\mathrm{char}(\mathbb{Z}_p)=p$ if $p\in\mathbb{P}$

Corollary: Let K be a finite field, the characteristic cannot be 0. Then $\exists p\in\mathbb{P}$ such that for $n\in\mathbb{N}^+: |K|=p^n$. K is called the **Galois field** $\mathrm{GF}(p^n)$.

- Let K and K' be fields with $|K|=|K'|=p^n$, then $K\cong K'$

Theorem: Let K be a field and $P(z)\in K[z]$. Then $K[x]/P(x)$ is a field $\iff P(x)$ is irreducible.

Algebraic Extensions of a Field

Theorem: Let K and L be fields, such that $K\subsetneq L$ and let $a\in L$ be a zero (*root*) 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.
Definition: Let $P(x)$ be monic and irreducible over K, with degree $\deg(P)=n$ and $P(a)=0$. Define $L=\left\{\sum_{i=0}^{n-1}c_ia^i \mid c_i\in K\right\}$. 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 "*K adjoint a*". Example: $\mathbb{R}[x]$ adjoint $\sqrt{-1}=\mathbb{C}$

Finite Fields (Galois Fields)

Theorem: Let K be a finite field, then $(K\setminus\{0\},\cdot)$ is a cyclic group. This means it has a generator.
Definition: A generator a of $K\setminus\{0\}$ is called a **primitive element of K**, its minimal polynomial over $P(K)\cong\mathbb{Z}_p$ is called a **primitive polynomial** with root a.
Theorem: Let $q(x)\in\mathbb{Z}_p[x]$ be a monic, irreducible polynomial of degree n. Then $q(x)$ is a primitive polynomial of $K=\mathrm{GF}(p^n)$ if and only if $q(x) \mid x^{p^n-1}-1$ and $\forall k: 1\leq k\leq p^n-2: q(x)\nmid x^k-1$.

- This can be checked by: $q(a)=0\iff a^k\neq 1$ for $k=1,...p^n-2$ and $a^{p^n-1}=1$
- Let $a,b\in K, p=\mathrm{char}(K)$, then $(ab)^p=a^pb^p$ and $(a+b)^p=a^p+b^p$

Properties of homomorphism: Let $\varphi: K\to K$, where $x\mapsto x^p$. Then $\mathrm{kern}(\varphi)$ is an ideal of K, but K is a field, which means that $\{0\}$ and K are the only ideals. $\varphi(1)=1^p\neq 0\Rightarrow 1\notin\mathrm{kern}(\varphi)\Rightarrow\mathrm{kern}(\varphi)\neq K\Rightarrow\mathrm{kern}(\varphi)=\{0\}$. From this follows that φ is *bijective* and is called *automorphism*.
Theorem: Let $K=\mathrm{GF}(p^n)$ then $\varphi: K\to K$ and $x\mapsto x^p$ is an automorphism
Definition: $(\{\psi: K\to K \mid \psi$ automorphism$\},\circ)=\langle\varphi\rangle$ is a cyclic group and the it is the **automorphsim group** of K: $\mathrm{Aut}(K)$. The following properties hold for such a group:

- $\forall x,y\in K: \psi(x+y)=\psi(x)+\psi(y)$
- $\psi(xy)=\psi(x)\psi(y)$