Diskrete Mathematik

Chapter 2 - Math. Reasoning

True Prop: Theorem, Lemma, Corollary A true proposition is often called a theorem , a lemma or a corollary.

Logical Equivalence Two formuals F and G are called *equivalent*, denoted as $F \equiv G$ if they correspond to the same function, i.e. they have the same truth values for all possible inputs.

Logical Consequence A formula G is a *logical consequence* of a formula F if for all combinations of inputs, the truth value of G is 1 if the truth value of F is 1. Intuitively, G is true if F is true. It is written as $F \models G$, respectively $F \leq G$

Implication The implication $A \to B$ is defined as $\neg A \vee B$

Propositional formula For a fixed universe, a formula with a fixed interpretation (e.g. no moving parts"), this means all variables have been resolved, is called a propositional formula since it can either be true or false.

- Lemma: F is tautology iff. $\neg F$ unsatisfiable.
- If F is a tautology one writes $\models F$.

Forms of Proof:

- MODUS PONENS A proof of a statement S is by use of the so-called *modus ponens* proceeds in two steps:
  1. Statem a statement R and prove R.
  2. Prove $R \implies S$
- CASE DESTINCTION A proof of a statemen S by *case distinction* proceedds by stating a finite list of mathematical statements $R_1, \cdots R_k$ (the cases) and then proving thast one of the cases must occur and also proving $R_i \implies S$ for $i = 1, \ldots, k$
- PROOF BY CONTRADICTION A *Proof by contradiction* of a statement S proceeds by stating a mathematical statement T, then assuming S is false and using S as false to prove that T is true, but then realizing T should actually be false. We have therefore shown that S cannot be false.
- PIGEON HOLE PRINCIPLE If n pigeons are distributed among $k > 0$ holes, one pigeon hole contains at least $\lceil \frac{n}{k} \rceil$ pigeons. **Ex.** Select 7 distinct numbers $\{1, \ldots, 11\}$, then two will sum to 11. *Proof:* We have 6 pigeonholes: $\{1, 11\}, \{2, 10\}, \{3, 9\}, \{4, 8\}, \{5, 7\}, \{6\}$.

Chapter 6 - Logic

Proof Systems A proof system $\Pi = (\mathcal{S}, \mathcal{P}, \tau, \phi)$ has 4 elements and is defined on an alphabet Σ

- $\mathcal{S}$ is the set of syntactic representations of mathematical statements with $\mathcal{S} \subseteq \Sigma^*$
- $\mathcal{P}$ is the set of syntactic representations of proof strings with $\mathcal{P} \subseteq \Sigma^*$
- τ is the truth function where $\tau : \mathcal{S} \to \{0, 1\}$ which assigns a truth value to a statement.
- ϕ is the verification function with $\phi : \mathcal{S} \times \mathcal{P} \to \{0, 1\}$ with $\phi(s, p) = 1$ if p is a valid proof for s.
- **Sound**: A proof system is sound if no false statement has a proof. i.e. $\forall s \in \mathcal{S}$ for which $\exists p \in \mathcal{P}$ when $\phi(s, p) = 1$ we have $\tau(s) = 1$.
- **Complete**: A proof system is complete if every true statement has a proof. i.e. $\forall s \in \mathcal{S}$ with $\tau(s) = 1$, $\exists p \in \mathcal{P}$ such that $\phi(s, p) = 1$

Example Proof System: $\Sigma = \{0, 1\}$, $\mathcal{S} = \mathcal{P} = \{0, 1\}^3$, $\tau(s) = 1$ if s contains at most one 0. $\theta(s, p) = 1$ if s contains at most two 0 and $s = p$. Complete since we can find proof for every true statement but not sound since wrong statements e.g. 001 have proof.

Propositional Logic

Logical Consequence A formula G is a logical consequence of a formula F, denoted $F \models G$ or $M \models G$ if every interpretation suitable for both F, G which is a model for F is also a model for G.

Equivalence F, G are equivalent iff. $F \models G$ and $G \models F$

Set of formulas: All of the above can also be said for a set of formulas M which can be seen as the conjunction (AND) of all formuals withing M. If $M = \varnothing$ then every interpretation is a model for M.

Extending Predicate Logic Assume we wanted to add the symbol $\heartsuit$, with $F \heartsuit G$ is true iff. F and G have the same truth value:
Syntax: If F and G are formulas so is $F \heartsuit G$.
Semantics: $\mathcal{A}(F \heartsuit G) = 1$ iff. $\mathcal{A}(F) = \mathcal{A}(G)$

Lemma 6.3 The following are equivalent:

- $\{F_1, \ldots, F_k\} \models G$
- $\{F_1 \wedge F_2 \wedge \ldots \wedge F_k\} \to G$ is a tautology
- $\{F_1, \ldots, F_k, \neg G\}$ is unsatisfiable.

Conjunctive Normal Form $F = \{A \vee \ldots \vee B\} \wedge \cdots \wedge \{B \vee \ldots \vee D\}$
Rows eval 0, or negative
Disjunctive Normal Form $F = \{A \wedge \ldots \wedge B\} \vee \cdots \vee \{C \wedge \ldots \wedge D\}$
Rows eval 1, and

A	B	C	$(A \wedge \neg B) \vee (B \wedge \neg C)$
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	0

We therefore obtain the following DNF

$$F \equiv (\neg A \wedge B \wedge \neg C) \vee (A \wedge \neg B \wedge \neg C) \vee (A \wedge \neg B \wedge C) \vee (A \wedge B \wedge \neg C)$$

as the disjunction of 4 conjunctions. And we obtain the following CNF

$$F \equiv (A \vee B \vee C) \wedge (A \vee B \vee \neg C) \wedge (A \vee \neg B \vee \neg C) \wedge (\neg A \vee \neg B \vee \neg C).$$

Lemma 6.2. *For any formulas F, G, and H we have*

1) $F \wedge F \equiv F$ *and* $F \vee F \equiv F$ *(idempotence);*
2) $F \wedge G \equiv G \wedge F$ *and* $F \vee G \equiv G \vee F$ *(commutativity);*
3) $(F \wedge G) \wedge H \equiv F \wedge (G \wedge H)$ *and* $(F \vee G) \vee H \equiv F \vee (G \vee H)$ *(associativity);*
4) $F \wedge (F \vee G) \equiv F$ *and* $F \vee (F \wedge G) \equiv F$ *(absorption);*
5) $F \wedge (G \vee H) \equiv (F \wedge G) \vee (F \wedge H)$ *(distributive law);*
6) $F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H)$ *(distributive law);*
7) $\neg\neg F \equiv F$ *(double negation);*
8) $\neg(F \wedge G) \equiv \neg F \vee \neg G$ *and* $\neg(F \vee G) \equiv \neg F \wedge \neg G$ *(de Morgan's rules);*
9) $F \vee \top \equiv \top$ *and* $F \wedge \top \equiv F$ *(tautology rules);*
10) $F \vee \bot \equiv F$ *and* $F \wedge \bot \equiv \bot$ *(unsatisfiability rules).*
11) $F \vee \neg F \equiv \top$ *and* $F \wedge \neg F \equiv \bot$.

Group Axioms in Predicate Logic:

$$\underbrace{\forall x \forall y \forall z (f(f(x,y),z) = f(x, f(y,z)))}_{\text{associativity}} \wedge \underbrace{\exists e \forall x (f(x,e) = f(e,x) = x}_{\text{neutral}} \wedge \underbrace{\exists y f(x,y) = f(y,x) = e)}_{\text{inverse}}$$

Predicate Logic

Substitution $F[x/g(a,z)]$ means that we are substituting every freely occuring x in F with $g(a,z)$.

Interpretation: An interpretation/structure is a tuple $A = (U, \phi, \psi, \xi)$ where U is a non empty universe, ϕ assisngs each function a function, ψ assigns predicated 0 or 1, ξ assigns variable a value in U. One also writes U^A, f^A, x^A, P^A
Always specify universe and all free variables.

Example 6.21. For the formula

$$F = \forall x \left(P(x) \vee P(f(x,a)) \right),$$

a suitable structure $\mathcal{A}$ is given by $U^{\mathcal{A}} = \mathbb{N}$, by $a^{\mathcal{A}} = 3$ and $f^{\mathcal{A}}(x,y) = x + y$, and by letting $P^{\mathcal{A}}$ be the "evenness" predicate (i.e., $P^{\mathcal{A}}(x) = 1$ if and only if x is even). For obvious reasons, we will say (see below) that the formula evaluates to true for this structure.

Some general info:

Definition 6.31. (Syntax of predicate logic.)

- A *variable symbol* is of the form x_i with $i \in \mathbb{N}$.[47]
- A *function symbol* is of the form $f_i^{(k)}$ with $i, k \in \mathbb{N}$, where k denotes the number of arguments of the function. Function symbols for $k = 0$ are called *constants*.
- A *predicate symbol* is of the form $P_i^{(k)}$ with $i, k \in \mathbb{N}$, where k denotes the number of arguments of the predicate.
- A *term* is defined inductively: A variable is a term, and if $t_1, \dots, t_k$ are terms, then $f_i^{(k)}(t_1, \dots, t_k)$ is a term. For $k = 0$ one writes no parentheses.
- A *formula* is defined inductively:
  - For any i and k, if $t_1, \dots, t_k$ are terms, then $P_i^{(k)}(t_1, \dots, t_k)$ is a formula, called an *atomic* formula.
  - If F and G are formulas, then $\neg F$, $(F \wedge G)$, and $(F \vee G)$ are formulas.
  - If F is a formula, then, for any i, $\forall x_i\, F$ and $\exists x_i\, F$ are formulas.

Definition 6.36. (Semantics.) For a structure $\mathcal{A} = (U, \phi, \psi, \xi)$, we define the value (in U) of terms and the truth value of formulas under that structure.

- The value $\mathcal{A}(t)$ of a term t is defined recursively as follows:
  - If t is a variable, then $\mathcal{A}(t) = \xi(t)$.
  - If t is of the form $f(t_1, \dots, t_k)$ for terms $t_1, \dots, t_k$ and a k-ary function symbol f, then $\mathcal{A}(t) = \phi(f)(\mathcal{A}(t_1), \dots, \mathcal{A}(t_k))$.
- The truth value of a formula F is defined recursively as follows:
  - $\mathcal{A}((F \wedge G)) = 1$ if and only if $\mathcal{A}(F) = 1$ and $\mathcal{A}(G) = 1$;
  - $\mathcal{A}((F \vee G)) = 1$ if and only if $\mathcal{A}(F) = 1$ or $\mathcal{A}(G) = 1$;
  - $\mathcal{A}(\neg F) = 1$ if and only if $\mathcal{A}(F) = 0$.
  - If F is of the form $F = P(t_1, \dots, t_k)$ for terms $t_1, \dots, t_k$ and a k-ary predicate symbol P, then $\mathcal{A}(F) = \psi(P)(\mathcal{A}(t_1), \dots, \mathcal{A}(t_k))$.
  - If F is of the form $\forall x\, G$ or $\exists x\, G$, then let $\mathcal{A}_{[x \to u]}$ for $u \in U$ be the same structure as $\mathcal{A}$ except that $\xi(x)$ is overwritten by u (i.e., $\xi(x) = u$):

$$\mathcal{A}(\forall x\, G) = \begin{cases} 1 & \text{if } \mathcal{A}_{[x \to u]}(G) = 1 \text{ for all } u \in U \\ 0 & \text{else} \end{cases}$$

$$\mathcal{A}(\exists x\, G) = \begin{cases} 1 & \text{if } \mathcal{A}_{[x \to u]}(G) = 1 \text{ for some } u \in U \\ 0 & \text{else.} \end{cases}$$

Lemma 6.8. *For any formulas F, G, and H, where x does not occur free in H, we have*

1) $\neg(\forall x\, F) \equiv \exists x\, \neg F$;
2) $\neg(\exists x\, F) \equiv \forall x\, \neg F$;
3) $(\forall x\, F) \wedge (\forall x\, G) \equiv \forall x\, (F \wedge G)$;
4) $(\exists x\, F) \vee (\exists x\, G) \equiv \exists x\, (F \vee G)$;
5) $\forall x\, \forall y\, F \equiv \forall y\, \forall x\, F$;
6) $\exists x\, \exists y\, F \equiv \exists y\, \exists x\, F$;
7) $(\forall x\, F) \wedge H \equiv \forall x\, (F \wedge H)$;
8) $(\forall x\, F) \vee H \equiv \forall x\, (F \vee H)$;
9) $(\exists x\, F) \wedge H \equiv \exists x\, (F \wedge H)$;
10) $(\exists x\, F) \vee H \equiv \exists x\, (F \vee H)$.

Universal Instantiation For any formula F and term t we have $\forall x F \models F[x/t]$ *Proof:* Let t be any term, If $\mathcal{A}(\forall x F) = 1$ then we have $\mathcal{A}_{[x \to u]}(F) = 1$, therefore also for $u = \mathcal{A}(t)$ implying $A(F[x/t]) = 1$.

Example - Prenex Form:
$F \equiv \forall x(P(x) \vee \exists x Q(f(x))) \wedge \exists y R(g(y, x))$ renaming vars
$F \equiv \forall u(P(u) \vee \exists z Q(f(z))) \wedge \exists y R(g(y, x))$ now taking quantors to front $F \equiv \forall u \exists z \exists y((P(u) \vee Q(f(z))) \wedge R(g(y, x)))$.
Example - Tautology proof:
$F \equiv (\forall x(P(x) \to Q(x)) \wedge P(y)) \to Q(y)$
$F \equiv \exists x \neg(\neg P(x) \vee Q(x)) \vee (\neg P(y) \vee Q(y))$
$F \equiv \exists y \neg G \vee G$, which is a tautology by showing it holds for any interpret.

Calculi

A **derivation rule** is a rule for deriving a formula from a set of formulas $\{F_1, \dots, F_k\} \vdash_R G$
A **logical calculus** K is finite set of derivation rules $\{R_1, \dots R_m\}$.
A **derivation** is a finite list of applications of rules. We write $M \vdash_K G$ if there is a derivation of G from M in K.
Completeness A calculus K is complete if $M \models F \implies M \vdash_K F$.A calculus K is sound/correct it $M \vdash_K F \implies M \models F$,
If $F \vdash_K G$ holds for a sound calculus then $\models (F \to G)$.
Resolution Calculus For a formula F transform it into CNF s.t. $F = (A \vee \dots B) \wedge \dots \wedge (C \vee \dots D)$.
Define $\mathcal{K}(F) = \{\{A, \dots, B\}, \dots, \{C, \dots, D\}\}$. Let $\mathcal{K}(M) = \bigcup_{i=1}^{k} \mathcal{K}(F_i)$. We now say that a clause K is a resolvent clause of clauses K_1 and K_2 if there is a literal L such that $L \in K_1$ & $\neg L \in K_2$ and $K = (K_1 \setminus \{L\}) \cup (K_2 \setminus \{\neg L\})$
Example $\{A, \neg B, \neg C\}$ and $\{\neg A, C, D, \neg E\}$ have two resolvents: $\{\neg B, \neg C, C, D, \neg E\}$ if elim. A and $\{A, \neg B, \neg A, D, \neg E\}$ if elim. C.
One writes $\{K_1, K_2\} \vdash_{res} K$. If K can be derived (finite steps) on writes $\mathcal{K} \vdash_{res} K$. If one can derive the empty clause $\varnothing$ this is equivalent to M being unsatisfiable.
Res is sound i.e. if $\mathcal{K} \vdash_{res} K$, then $\mathcal{K} \models K$. We show res rule is correct. Assume $K_1, K_1 \vdash_{res} K$, then either $\mathcal{A}(L) = 1$ making e.g. K_1 true, but K_2 with $\neg L$ is also true so $K_2 \setminus \neg L$ is true, hence $K_1 \setminus \{L\}) \cup (K_2 \setminus \{\neg L\}$ is true under $\mathcal{A}$.
Res is not complete We can never derive $A \models A \vee B$
Show F is tautology Show $\neg F$ is unsatisfiable.
Show logical consequence Assume $H = \{F_1, F_2, ..., F_n\}$ Show $H \models G$ by showing unsatisfiability of $\{F_1, F_2, ...F_n, \neg G\}$

Chapter 3 - Set, Relations & Functions

Set Relations
$A = B :\iff \forall x(x \in A \leftrightarrow x \in B)$
$A \subseteq B :\iff \forall x(x \in A \leftarrow x \in B)$
It follows directly from the set equality that $A = B \iff (A \subseteq B) \wedge (B \subseteq A)$

Set one Element Proof: For any a and b: $\{a\} = \{b\} \implies a = b$. We prove this indirectly by showing $a \neq b \implies \{a\} \neq \{b\}$

Ordered Pair $(a, b) := \{\{a\}, \{a.b\}\}$

Empty set is subset The empty set is a subst of every set. Assume there is a set A for which $\varnothing \not\subseteq A$. So there exists $x \in \varnothing$ with $x \notin A$. This is a contradiction since $\varnothing$ is empty.

The empty set is unique: Assume there exist two, then $\varnothing_1 \subseteq \varnothing_2$. But also $\varnothing_2 \subseteq \varnothing_1$. This implies $\varnothing_1 = \varnothing_2$.

Power Set We define the power set of A, denoted $\mathcal{P}(A)$ as the set of all subsets of A: $\mathcal{P}(A) := \{S | S \subseteq A\}$
For a finite set of cardinality k, the power set has cardinality 2^k.

Exist. unendl. A, sd. $A \in \mathcal{P}(A)$. per ind. $\{\varnothing\} \in \mathcal{P}(\{\varnothing\})$. Schritt: Belieb. $S \in \mathcal{P}(A) \Rightarrow S \subseteq A \overset{I.H.}{\subseteq} \mathcal{P}(A) \Rightarrow S \in \mathcal{P}(\mathcal{P}(A))$

Theorem 3.4. *For any sets A, B, and C, the following laws hold:*

Idempotence:	$A \cap A = A$; $A \cup A = A$;
Commutativity:	$A \cap B = B \cap A$; $A \cup B = B \cup A$;
Associativity:	$A \cap (B \cap C) = (A \cap B) \cap C$; $A \cup (B \cup C) = (A \cup B) \cup C$;
Absorption:	$A \cap (A \cup B) = A$; $A \cup (A \cap B) = A$;
Distributivity:	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$; $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;
Consistency:	$A \subseteq B \iff A \cap B = A \iff A \cup B = B$.

Cartesian Product The cartesian product of $A \times B$ is the set of all ordered pairs with the first component from A and the second from B.

$$A \times B = \{(a, b) | a \in A \wedge b \in B\}$$

The cardinalities are: $|A \times B| = |A| \cdot |B|$

Relations

Binary relation ρ from a set A to a set B is a subset of $A \times B$. If $B = A$, then ρ is relation on A, one usually writes $a\rho b$. Can be represented in bool $|A| \times |B|$ matrix, or as graph with $|A| + |B|$ vertices only containing edges from a to b if $a\rho b$. There are 2^{n^2} different relations on a set with cardinality n.

Inverse Relation The inverse of a relation ρ from A to B is the relation $\hat{\rho}$ from B to A such that: $\forall a \in A \forall b \in B(A\rho b \leftrightarrow b\hat{\rho}a)$

Composition of Relation Let ρ be a relation from A to B and let σ be a relation form B to C. then the composition of ρ and σ, denoted $\rho\sigma$ (or $\rho \circ \sigma$) is the relation from A to C where: $a\rho\sigma c :\Leftrightarrow \exists b \in B(a\rho b \wedge b\sigma c)$

Properties of Relations

Eigenschaft	Formel	Menge
reflexiv	$\forall a(a\rho a)$	$id \subseteq \rho$
irreflexiv	$\forall a(a\rho a)$	$\rho \cap id = \varnothing$
symmetrisch	$a\rho b \iff b\rho a$	
antisymmetrisch	$\forall a \forall b : (a\rho b \wedge b\rho a) \to a = b$	$\rho \cap \hat{\rho} = id$. z.B. $\leq, \geq$
transitiv	$\forall a \forall b \forall c : ((a\rho b \wedge b\rho c) \to a\rho c)$	$\rho^2 \subseteq \rho$.

Eigenschaft	Matrix	Graph
reflexiv	diags $= 1$	every vertex has loop
irreflexiv	diags $= 0$	
symmetrisch	symmetrisch	undirected (evtl. loops)
antisymmetrisch		no cycle length 2
transitiv		

Number of symmetric relations on $\{1, 2, 3\}$?
A symmetric relation always contains both e.g. $(1, 2), (2, 1)$ 2^3 combina-

tions. Furthermore, it might contain $(1,1)$, ..., therefore $2^3 * 2^3$ combinations are possible.

Relation transitive $\iff \rho^2 \subseteq \rho$ ($\Rightarrow$) Assume ρ transitive. Assume $(a,b) \in \rho^2$, by def $\exists c : (a,c) \in \rho \wedge (c,b) \in \rho$, by transitivity $(a,b) \in \rho$. ($\Leftarrow$) If $(a,b) \in \rho \wedge (b,c) \in \rho$ and therefore $(a,c) \in \rho^2$, since $\rho^2 \subseteq \rho$ also $(a,c) \in \rho$, implying transitivity.

Transitive Closure The transitive closure is $\rho^\star = \bigcup_{n=1}^{\infty} \rho^n$

Equivalence Relation An equivalence relation on a set A is reflexive, symmetric and transitive.

Equivalence Class For equivalence relation θ on set A and for $a \in A$, the set of elements of A that are equivalent to a is called the equivalence class of a and is denoted as $[a]_\theta$. The intersection of two equivalence relations is also an equivalence relation.. e.g. $(\equiv_3 \cap \equiv_2) = \equiv_{15}$

Set of Equivalence Classes The set $A/\theta := \{[a]_\theta | a \in A\}$ is called the quotient set of A by θ, or simply A modulo θ or $A \mod \theta$

Theorem - Equiv. Classes form partition The set A/θ of equivalence classes of an equivalence relation θ on A is a partition of A. *Proof:* $\forall a \in A : a \in [a]$. First we show $a\theta b \implies [a] = [b]$. Let $c \in [a]$ impl. $c\theta a$ impl. $c\theta b$ impl. $c \in [b]$. Remains to show $a \not\theta b \implies [a] \cap [b] = \varnothing$ by contradict.

Partial Order / Posets A partial order on a set A is reflexive, antisymmetric and transitive. A set A together with a partial order $\preceq$ on A is called a partially ordered set (or simply as poset) denoted $(A;\preceq)$.If drawn as a graph it doesn't have any cycles.
Ex: $>, <$ are not partial orders since they are not reflexive. However $\leq, \geq$ are (on e.g. $\mathbb{R}$).

Comparable / totally ordered For a poset $(A;\preceq)$, two elements are called comparable if $a \preceq b$ or $b \preceq a$.
If any two elements in $(A;\preceq)$ are comparable, then A is called totally ordered by $\preceq$.

Example - Powerset / totally Orderable The poset $(\mathcal{P}(A), \subseteq)$ is not totally ordered if $|A| \geq 2$. Since $\{1\}$ and $\{2,3\}$ are not comparable.

Cover In a poset $(A;\preceq)$ and element b is said to cover a if $a \prec b$ and there is no c such that $a \prec c$ and $c \prec b$. $\rightarrow$ b is direct superior of a.

Hasse Diagram The hasse diagram of a finite poset $(A;\preceq)$ is the directed graph whose vertices are labelled with the elements of A and where there is an edge from a to b if and only if b covers a.

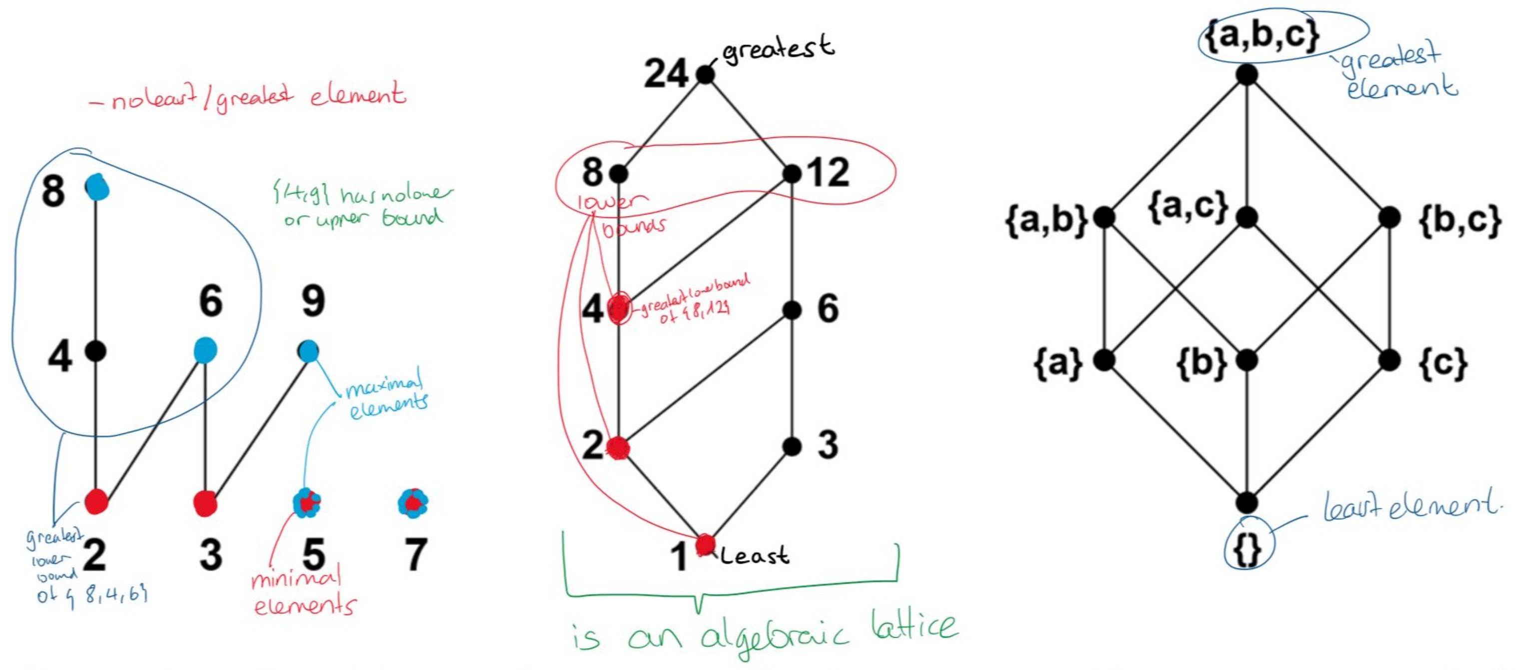

Figure 3.1: The Hasse diagrams of the posets $(\{2,3,4,5,6,7,8,9\};|)$, $(\{1,2,3,4,6,8,12,24\};|)$, and $(\mathcal{P}(\{a,b,c\});\subseteq)$.

Special Elements in a poset Let $(A;\preceq)$ be a poset and let $S \subseteq A$ be some subset of A. Then:

1. $a \in S$ is a minimal (maximal) element of S if there exists no $b \in S$ with $b \prec a$ ($b \succ$ a).
2. $a \in S$ is the least (greatest element) of S if $a \preceq b$ ($a \succeq b$) for all $b \in S$.
3. $a \in A$ is the lower (upper) bound of S if $a \preceq b$ ($a \succeq b$) for all $b \in S$
4. $a \in A$ is the greatest lower bound (least upper bound) of S if a is the greatest (least) element of the set of all lower (upper bounds of S)

Well ordered posets A poset $(A;\preceq)$ is well-ordered if it is totally ordered and if every non-empty subset of A has a least element.
Every totally ordered finite poset is well-ordered.

Meet and Join Let $(A,\preceq)$ be a poset. If a and b (i.e. the set $\{a,b\} \subseteq A$) have a greatest lower bound, then it is called the meet of a and b., often denoted $a \wedge b$. If a and b have a least upper bound, then it is called the join of a and b, often denoted $a \vee b$.

Examples of meet and join:

- $(\mathbb{N}, \leq)$,$a \wedge b = \min(a,b)$, $a \vee b = \max(a,b)$
- $(\mathbb{N} \setminus \{0\}, |)$, $a \wedge b = ggt(a,b)$, $a \vee b = kgv(a,b)$
- $(\mathcal{P}(A), \subseteq)$, $a \wedge b = a \cap b$, $a \vee b = a \cup b$

Lattice A poset in which every pair of elements has a meet and a join.

Composition of functions The composition of a function $f : A \rightarrow B$ and $g : B \rightarrow C$, denoted $g \circ f$ or simply gf, is defined by $(g \circ f)(a) = g(f(a))$.

Cardinalities of Sets

1. $A \sim B$, if there exists a bijection $A \rightarrow B$.
2. $A \preceq B$, if $A \sim C$ for some subset $C \subseteq B$.
3. A is called if $A \preceq \mathbb{N}$ and uncountable otherwise.

Bernstein Schröder: $A \preceq B \wedge B \preceq A \implies A \sim B$

Theorems on Countability

- The relation $\preceq$ is transitive: $A \preceq B \wedge b \preceq C \implies A \preceq C$
- $A \subseteq B \implies a \preceq B$
- A set A is countable if and only if it is finite of if $A \sim \mathbb{N}$
- The set $\{0,1\}^* := \{\epsilon, 0, 1, 00, 11, 01, 11, 000, 001, \cdots\}$ of finite binary sequences is countable.
- The set $\{0,1\}^\infty$ is uncountable $\rightarrow$ cantors diagonal argument.

Countability of composite sets

- For an $n \in \mathbb{N}$, the set A^n of n-tuples over A is countable.
- The union $\bigcup_{i \in \mathbb{N}} A_i$ of a countable list $A_1, A_2, \ldots$ of countable sets is countable.
- The set A^* of finite sequences of elements from A is countable.

Computable functions A function $f : \mathbb{N} \rightarrow \{0,1\}$ is called computable if there is a program that , for every $n \in \mathbb{N}$, when given n as an input, outputs $f(n)$.

Existence of uncomputable functions $\mathbb{N} \rightarrow \{0,1\}$ *Proof* $\{0,1\}^\star \prec \{0,1\}^\infty$. Uncountably many function but countably many programs that can be computed.

Functions

Injective $\forall x_1, x_2 \in M : f(x_1) = f(x_2) \implies x_1 = x_2$ or $x_1 \neq x_2 \implies f(x_1) \neq f(x_2)$

Surjective $\forall y \in N \exists x \in M : y = f(x)$

Inverse of injective is surjective let $f : A \rightarrow B$ be injective for any A, B. We prove $\exists g : B \rightarrow A$ is surjective. Define $g(x) = f^{-1}(x)$ if $f^{-1}(x)$ exists, and else $g(x) = a$ arbitrary.

The converse is also true: Let $g : B \rightarrow A$ be surj. we show $\exists f : A \rightarrow B$ injective. Let g be surjective. Since g is surjective we define $(g \circ f)(a) = g(f(a)) = g(b) = a$ with $f(a) = b$ for any b.
Now assume $f(a) = f(a')$, by def we get $a = g(f(a)) = g(f(a')) = a'$ implying injectivity.

$h \mapsto f \circ h \circ g$ **injektiv**. $f : A \rightarrow B$ injective and $g : B \rightarrow A$ surjective. Thus $\phi : A^A \rightarrow B^B$ injective. *Beweis* Wts. $\forall h_1 \neq h_2 \in A^A \Rightarrow \phi(h_1) \neq \phi(h_2)$. Let $h_1 \neq h_2$, $\exists a_0 \in A : h_1(a_0) \neq h_2(a_0)$ Let $g(b) = a_0$ which exists since g surjective. Thus: $h_1(g(b)) \neq h_2(g(b))$. Since f injective: $f(h_1(g(b))) \neq f(h_2(g(b))) \Leftrightarrow f \circ h_1 \circ g \neq f \circ h_2 \circ g \Leftrightarrow \phi(h_1) \neq \phi(h_2)$ as we wanted.

Chapter 4 - Number Theory

Theorem 2.1: (Euclid) For all integers a and $d \neq 0$ there exist unique integers q and r satisfying

$$a = dq + r \quad \text{and} \quad 0 \leq r < |d|$$

Definition: Greatest Common Divisor For integers a and b (both not 0), an integer d is called the greatest common divisor of a and b if d divides both a and b and if every common divisor of a and b divides d:

$$d|a \wedge d|b \wedge \forall c((c|a \wedge c|b) \rightarrow c|d)$$

Euclids Extended Algorithm

$(s_1, u_1, v_1) := (a, 1, 0)$;
$(s_2, u_2, v_2) := (b, 0, 1)$;
while $s_2 > 0$ **do begin**
  $q := s_1$ **div** s_2;
  $t := (s_2, u_2, v_2)$;
  $(s_2, u_2, v_2) := (s_1, u_1, v_1) - q(s_2, u_2, v_2)$;
  $(s_1, u_1, v_1) := t$;
end;
$d := s_1$; $u := u_1$; $v := v_1$;

EUCLID(a, b)
if $b == 0$
  return a
else return EUCLID$(b, a \bmod b)$

Example: Find $u, v \in \mathbb{Z}$ s.t. $62u + 58v = ggT(62, 58)$. Perform algorithm with $s_1 = 62, s_2 = 58$, then $u_1 = u$ (for 62) and $v_1 = v$ (for 58)

Definition: Least Common Multiple The least common mulitple l of two positive integers a and b, denoted $l = lcm(a, b)$, is the common multiple of a and b, which divides every common multiple of a and b. $a|l \land b \land l \land \forall m((a|m \land b|m) \to l|m)$

Some facts about gdc **and** lcm**:**
if $a = \prod_i p_i^{e_i}$ and $b = \prod_i p_i^{f_i}$ then $gcd(a, b) = \prod_i p_i^{\min(e_i, f_i)}$ and $lcm(a, b) = \prod_i p_i^{\max(e_i, f_i)}$. This implies $gdc(a, b) \cdot lcm(a, b) = a \cdot b$ because $\forall i$ we have $\min(e_i, f_i) + \max(e_i, f_i) = e_i + f_i$

Bézout's Lemma For $a, b \in \mathbb{Z} \setminus \{0\} \exists u, v \in \mathbb{Z}$ such that $gcd(a, b) = ua + vb$

Example Proof Number of Divisors Odd Let D_n be the set of divisors of n. Show $|D_n|$ odd $\iff \exists c : c^2 = n$. *Proof:* We write two divisors as tuple (a, b) when $ab = n$. We can only have an odd number of tuples if (c, c) is a tuple.

Show Irrationality $\log_2(2015)$ is irrat. since AFSOC $\frac{p}{q} = \log_2(2015) \Rightarrow 2^p * 2015 = 2^q$, but then prime decomp. not unique.

Modulus

Definition: Modulo Congruence For $a, b, m \in \mathbb{Z}$ with $m \geq 1$ we say that a is congruent to b modulo m if m divides $a - b$. We write $a \equiv b \mod m$ or simply $a \equiv_m b$.
or in short: $a \equiv_m b :\iff m|(a - b)$

Remainder Equalities: For any $a, b, m \in \mathbb{Z}$ with $m \geq 1$ we have $R_m(a+b) = R_m(R_m(a)+R_m(b))$ and $R_m(a*b) = R_m(R_m(a)*R_m(b))$

Lemma 4.19 - Solutions to Congruences: $ax \equiv_m 1$ is a congruence equation which has a solution iff. $gcd(a, m) = 1$. The solution is unique. One can find that solution called the multiplicative inverse if one uses the extended euclidean algorithm, setting $b = m$. look at the factor that would multiply with a.

Ex: $R_{990}(5^{722})$

a) ges: $R_{990}(5^{722}) \equiv R_{2*5*9*11}(5^{722})$. Dies ist (nach dem CRT) äquivalent zum Finden der Reste $a_1, a_2, a_3,$ und a_4, so dass die folgenden Gleichungen gelten:
$x \equiv_2 a_1$, mit $a_1 = 1$, weil $R_2((5^{722})^1 * 1) = R_2(1 * 1) = 1$ ist
$x \equiv_5 a_2$, mit $a_2 = 0, trivial$
$x \equiv_9 a_3$, mit $a_3 = 7$, weil $R_9((5^6)^{120} * 5^2) = R_9(1 * 5^2) = 7$ ist
$x \equiv_{11} a_4$, mit $a_4 = 3$, weil $R_{11}((5^{10})^{72} * 5^2) = R_{11}(1 * 5^2) = 3$ ist
Dabei verwendeten wir, dass $p \nmid a \implies a^{p-1} \equiv_p 1$ gilt.
Jetzt wenden wir das CRT wie gewohnt an und erhalten
$x = R_{990}(1 * 1 * 495 + 0 * 2 * 198 + 7 * 5 * 110 + 3 * 6 * 90) = 25$

Chinese Remainder Theorem: Theory Let $m_1, \dots, m_r$ be pairwise prime integers and let $M = \prod_{i=1}^r m_i$. For every list $a_1, \dots a_r$ with $0 \leq a_i < m_i$ for $1 \leq i \leq r$, the system of congruence equations $x \equiv_{m_1} a_1 \land \dots \land x \equiv_{m_r} a_r$ for x has a unique solution x satisfying $0 \leq x < M$: **By contruction:** Let $M_i = M/m_i$ and $M_i N_i \equiv_{m_i} 1$ (using euclidean algorithm) then we have the solution $x = R_M\left(\sum_{i=1}^r a_i M_i N_i\right)$

Chinese Remainder Theorem: Example

Assume we have:

find inverse & using Euclid

$x \equiv_3 1$ $M_1 = 140$, $140 \equiv_3 2$, $2y_1 \equiv_3 1$, $y_1 = 2$
$x \equiv_4 1$ $M_2 = 105$, $105 \equiv_4 1$, $1y_2 \equiv_4 1$, $y_2 = 1$
$x \equiv_5 1$ $M_3 = 84$, $84 \equiv_5 4$, $4y_3 \equiv_5 1$, $y_3 = 4$
$x \equiv_7 0$ $M_4 = 60$, $60 \equiv_7 4$, $4y_4 \equiv_7 1$, $y_4 = 2$
$M = 3 \cdot 4 \cdot 5 \cdot 7 = 420$

3, 4, 7, 5 are pairwise coprime
→ we can use CRT

$x = \underbrace{1 \cdot 140 \cdot 2}_{\text{mod 3 part}} + \underbrace{1 \cdot 105 \cdot 1}_{\text{mod 4 part}} + \underbrace{1 \cdot 84 \cdot 4}_{\text{mod 5 part}} + \underbrace{0 \cdot 60 \cdot 2}_{\text{mod 7 part}} = 721$

$721 \equiv_{420} 301 \Rightarrow \underline{\underline{x = 301}}$

Diffie-Hellman

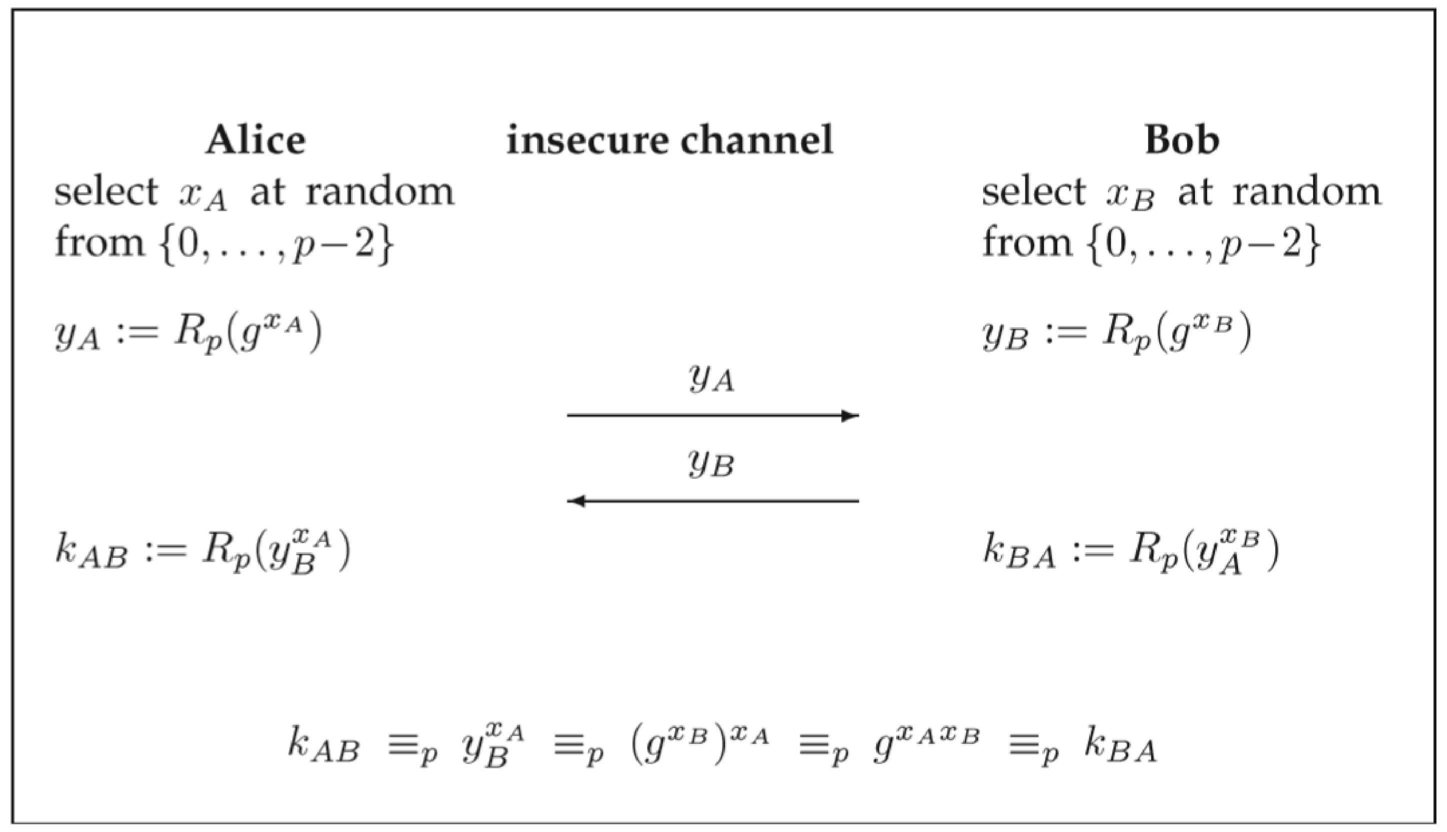

Figure 4.2: The Diffie-Hellman key agreement protocol.

Divisibility Rules

- 11: Alternating sum: $2728 \to 2 - 7 + 2 - 8 = -11$
- 9: Quersumme durch 9 teilbar.
-7: Ziehe letzte Ziffer zweimal von Zahl ohne letze Ziffer ab. Wiederhole solange nötig. Wenn Resultat durch 7 teilbar, so war es auch die Zahl. z.B: $7|17059?$, $1705 - 18 = 1687$, $168 - 14 = 154$, $15 - 8 = 7$, somit $7|17059$.

Chapter 5 - Algebra

Definition: Algebra An algebra is a pair $\langle S; \Omega \rangle$, where S is a set (the carrier of the algebra) and $\Omega = (\omega_1, \cdots \omega_n)$ a list of operations on S. Some terms that are relevant:

- Left neutral element: $e * a = a$
- Associativity: A binary relation $*$ is associative iff. $a*(b*c) = (a*b)*c$
- Left inverse element b of a: $b * a = e$

Definition: Monoid A monoid is an algebra $\langle M; *, e \rangle$ where $*$ is associative and e is the neutral element.
Definition: Group A group is an algebra $\langle G; *, ^\wedge, e \rangle$ satisfying the following conditions:

G1 $*$ is associative
G2 There exists a neutral element $e \in G$ such that $a * e = e * a = a$
G3 Every $a \in G$ has an inverse $\hat{a}$ such that $a * \hat{a} = \hat{a} * a = e$

An abellian group is a group that commutes d.h.: $ab = ba$
Some Group Lemmas A group fulfills the following: $\widehat{(\hat{a})} = a$, $\widehat{a \times b} = \hat{b} * \hat{a}$, $a * b = a * c \implies b = c$, $b * a = c * a \implies b = c$, equation $a * x = b$ has unique solution x for any a, b

Group of order 4 commutes. AFSOC $xy \neq yx$, build cases, show that there must be one more element. Then conclude that e, x, y, xy, yx are distint.

Morphisms

A homomorphisms is a mapping between two groups with $\phi(a * b) = \phi(a) * \phi(b)$. It fulfills: $\phi(e_G) = e_H$, $\phi(a^{-1}) = \widehat{\phi(a)}$, $\phi(a^n) = \phi(a)^n$, A group always gets mapped onto a subgroup. **Isomorphism** is a bijective homomorphism.

Definition: Direct Products of Groups The direct product of n groups $\langle G_1, *_1 \rangle, \cdots, \langle G_n, *_n \rangle$ is the algebra $\langle G_1 \cdots * G_n; * \rangle$ where $*$ is defined component wise: $(a_1, \dots, a_n) * (b_1, \dots b_n) = (a_1 *_n b_1, \dots, a_n *_n b_n)$

Definition: Group Homomorphism A function ψ from a group $\langle G; *, \hat{}, e \rangle$ to a group $\langle H; *', \tilde{}, e' \rangle$ is a group homomorhpism iff. for all a, b we have $\psi(a*b) = \psi(a)*\psi(b)$. If ψ is a bijection it is an isomorphism and we write $G \simeq H$, called homeomorphic.

Generator maps onto Generator: ϕ a homomorphism from a cyclic group $\langle g \rangle = G$ to a group H. wts. $\phi(g)$ generates H. *Proof* g Generator of G. wts. $\forall h \in H \exists k \in N : h = \phi(g)^k$. Since bijective $r = \phi^{-1}(h)$, $r \in G$. $\exists n : g^n = r \Rightarrow \phi(g)^n = \phi(g^n) = \phi(r) = h$, cause $\phi(g^n) = \phi(g)^n$ via induct.

Definition: Subgroup A subset $H \subseteq G$ of a group $\langle G; *, \wedge, e\rangle$ is calld a subgroup if $\langle H; *, \wedge, e\rangle$ is a group; closed under all operations. This means that the neutral element is always in the subgroup.

Union of subgroups is not subgroup AFSOC $H_1 \cup H_2 = H_3$. Dann $\exists a \in H_1, a \notin H_2$ und $\exists b \in H_2, b \notin H_1$. Dann $ab \in H_3$, somit entweder $ab \in H_1$ oder $ab \in H_2$. Contradict.

Definition: Order of Group Element Let G be a group and a an element of G. The minimal m for which $a^m = e$ is called $ord(m)$. If no such m exist we have $ord(m) = \infty$. By def $ord(e) = 1$

Definition: Order of Group Let G be a group, the order of G is defined as $|G|$

Finite Group every Element finite order: *Proof:* Since G is finite we must have $a^r = a^s = b$ for some r, s with $r < s$. Then $a^{s-r} = a^s * a^{-r} = b * b^{-1} = e$.

Intersection of two Subgroups is Subgroup Let H_1, H_2 be two subgroups. Trivially $e \in H_1, H_2$, we show $H_3 = H_1 \cap H_2$ is closed: $a, b \in H_1, H_1$, hence $ab \in H_1, H_2$, resulting in $ab \in H_3$. Similarly $c^{-1} \in H_1, H_2$ so $c^{-1} \in H_3$.

Isomorphic Subfields Let p be a prime number. The field F_{p^m} is (isomorphic to) a subfield of F_{p^n} if and only if $m|n$. (not in lecture)

Cyclicity & Generators

Definition: Cyclic Group A group $G = \langle g\rangle$ generated by an element $g \in G$ is called cyclic and g is called the generator of G.

Remark about Generators: If G is a group and $a \in G$ has finite order then $a^m = a^{R_{ord(a)}(m)}$. We define $\langle a\rangle = \{a^n | n \in Z\} = \{e, a, a^2, \dots, a^{ord(a)-1}\}$. Not all groups are cyclic!

Find all generators of $\langle \mathbb{Z}_{17}^*; \otimes\rangle$: We first note that $\mathbb{Z}_{17}^* = \{1, \dots, 16\}$. We know that all elements generate a subgroup, we need to find the elements generating a subgroup of size 16. We check which elements $a^8 \neq 1$, these are our generators of the whole group. They are: $\{3, 5, 6, 7, 10, 11, 12, 14\}$ which are 8 elements which is $\phi(16) = 8$.

Cyclic Groups are Abelian A cyclic group of order n is isomorphic to $\langle Z_n; \oplus\rangle$ and hence abelian. *Proof:* Let $G = \langle g\rangle$ be a cyclic group of order n. The bijection $\mathbb{Z}_n \to G : i \mapsto g^i$ is a group homomorph. since $i \oplus j \mapsto g^{i+j} = g^i * g^j$.

Lagrange Theorem Let G be a finite group and H a subgroup of G. Then the order of H divides the order of G, i.e. $|H|$ divides $|G|$

Generated Groups are cyclic if G finite Let G be a finite group. Then $a^{|G|} = e$ for every $a \in G$. *Proof:* We have $|G| = k * ord(a)$ for some k (Lagrange). Hence $a^{|G|} = a^{k*ord(a)} = a^{ord(a)^k} = e^k = e$.

Groups of Prime order is Cyclic Every group of prime order is cyclic and in such a group every element except the neutral element is a generator. Since no other non-trivial subgroups can be formed.

Order of Cyclic Groups The group $\mathbb{Z}_m^*$ is cyclic $\iff m = 2 \vee m = 4 \vee m = p^e \vee m = 2p^e$ for p any odd prime and $e \geq 1$

Multiplicative Groups & Totient Function

Definition: Multiplicative Group / Inverse We define

$$\mathbb{Z}_m^* = \{a \in Z_m | gcd(1, m) = 1\}$$

This is the set of all integers modulo m which have an inverse. For it to have an inverse by section 4.5.3 $gcd(a, m)$ must be 1.

Definition: Euler function The euler function $\phi : \mathbb{Z}^+ \to \mathbb{Z}^+$ is defined as the cardinality of $\mathbb{Z}_m^* : \phi(m) = |\mathbb{Z}_m^*|$

Example: Euler function $\mathbb{Z}_m^* = \{1, 5, 7, 11, 13, 17\}$, so $\phi(18) = 6$. Furthermore if p prime then $\phi(p) = p - 1$ since $gcd(p, l) = 1 \forall l$

Evaluating Eulers function If the prime factorization of m is $m = \prod_{i=1}^r p_i^{e_i}$ then

$$\phi(m) = \prod_{i=1}^r (p_i - 1) p_i^{e_i - 1}$$

It is not injective since $\phi(6) = 2 = \phi(2)$. Also not surjective, odd numbers have no preimage since if $gcd(k, n) = 1$, $gcd(n - k, n) = 1$ too. If $n > 2$ all rel. prime to n match up into pairs $\{k, n - k\}$. So $\phi(n)$ even.

Fermat's & Euler's Corollary For all $m \geq 2$ and all a with $gcd(a, m) = 1$ we have $a^{\phi(m)} \equiv_m 1$ & for every prime p and every a not divisible by p: $a^{p-1} \equiv_p 1$ *Proof:* We know that G finite so $a^{|G|} = e$ for every $a \in G$

RSA Theorem Let G be some finite group and let $e \in Z$ be relatively prime to $|G|$ ($gcd(e, |G|) = 1$). The unique e-th root of y, namely $x \in G$ satisfying $x^e = y$ is

$$x = y^d$$

where d is the multiplicative inverse of e modulo $|G|$, i.e. $ed \equiv_{|G|} 1$

RSA: Explained We look at $\mathbb{Z}_n^*$ where $n = pq$ with p, q being large primes. The order of $\mathbb{Z}_n^*$ is $|\mathbb{Z}_n^*| = \phi(n) = (p-1)(q-1)$. We can encrypt a message m with $y = R_n(m^e)$ and decrypt it with $m = R_n(y^d)$ where $ed \equiv_{(p-1)(q-1)} 1$.

Alice	insecure channel	Bob
Generate primes p and q $n = p \cdot q$ $f = (p-1)(q-1)$		
select e $d \equiv_f e^{-1}$	$\xrightarrow{n, e}$	plaintext $m \in \{1, \dots, n-1\}$
$m = R_n(y^d)$	$\xleftarrow{y}$	ciphertext $y = R_n(m^e)$

Rings and Fields

Definition: Ring A ring $\langle R; +, -, 0, *, 1\rangle$ is an algebra for which:

1. $\langle R; +, -, 0\rangle$ is a commutative group
2. $\langle R; *, 1\rangle$ is a monoid
3. $a(b + c) = (ab) + (bc)$ left associativity and right associativity $(b + c)a = (ba) + (ca)$

If $ab = ba$ we call the ring commutative.

Simple Ring Corollary's For any ring we have $0a = a0 = 0$ & $(-a)b = -(ab)$ & $(-a)(-b) = ab$ & if the ring R is non-trivial then $1 \neq 0$.
Divisors: Like usual, but -1 and negative values are also divisors.

Commutattivity of Addition follows from other Axioms $\langle R, +, -, 0, \cdot, 1\rangle$, look at $(1 + 1)(a + b)$

Polynomials

Definition: Polynomial Rings A Polynomial over a ring is of the form $a(x) = a_d x^d + \dots + a_0 x^0 = \sum_{i=0}^d a_i x^i$. The degree is the greatest i for $a_i \neq 0$. But $deg(0) \overbrace{=}^{\text{def}} -\infty$. The set $R[x]$ is the set of Polynomials in x over R.
$a(x) + b(x) = \sum_{i=0}^{\max(d,d')} (a_i + b_i) x^i$
$a(x) * b(x) = \sum_{i=0}^{d+d'} \left(\sum_{k=0}^{i} a_k b_{i-k}\right) x^i = \sum_{i=0}^{d+d'} \left(\sum_{k=0}^{u+v=i} a_u b_v\right) x^i$
$= a_d b_{d'} x^{d+d'} + \ldots + (a_0 b_2 + a_1 b_1 + a_2 b_0) x^2 + (a_0 b_1 + a_1 b_0) x + a_0 b_0$

$R[x]$ a ring For any ring R, $R[x]$ is also a ring. Can be shown using axioms.

$a(x) \in F[x]$, in F a field, has at most d roots. *Proof* AFSOC $deg(a(x)) = d$ but has $e > d$ roots. Then the poly. $\prod_{i=1}^e (x - \alpha_i)$ divs $a(x)$. but this would mean $a(x)$ has degree at least e, contradict.

Monic Polynomial, if ratinal root then integer $a(x) \in \mathbb{Z}[x]$, $r \in \mathbb{Q}$, $a(r) = 0$, then $r \in \mathbb{Z}$ *Proof* Insert $\frac{p}{q}$ then $0 = q^n f(\alpha) = p^n + q\left(a_{n-1} p^{n-1} + \dots + a_1 q^{n-2} p + a_0 q^{n-1}\right)$ Show $q|p$, hence $q = 1$.

Lagrange Polynomial Interpolation: Assume we have values pairs $\beta_1 = a(\alpha_1), \ldots, \beta_{d+1} = a(\alpha_{d+1})$, then we define $a(x) = \sum_{i=1}^{d+1} \beta_i u_i(x)$ (of degree d) with $u_i(x) = \frac{(x-\alpha_1)*\cdots*(x-\alpha_{i-1})*(x-\alpha_{i+1})*\cdots*(x-\alpha_{d+1})}{(\alpha_i-\alpha_1)*\cdots*(\alpha_i-\alpha_{i-1})*(\alpha_i-\alpha_{i+1})*\cdots*(\alpha_i-\alpha_{d+1})}$

Lagrange Polynomial Example Let $a(x)$ be a Polynomial of degree 4 over $GF(7)[x]$.We know that $a(x)$ has a double root at $x = 2$. Moreover: $a(3) = 2$, $a(4) = 3, a(6) = 5$. Find a: Since 2 is a double root $a(x) = (x-2)^2 b(x)$. Now we can use Lagrange Poly Interpol. to determine $b(x)$.

Lagrange Interpo. Theorem Polynomial of degree at most d can uniquely be determined by and $d+1$ values of $a(x)$.

Zerodivisors & Units & Integral Domains

Definitions on Rings:

- **Characteristic of group** is defined as the order of 1 in the additive group, if it is infinite we set it 0. A field $GF(p^n)$ has characteristic p if p prime. *Proof* $0 = Char(F) * 1 = ab$ so it has zerodivs.
- **Zerodivisor:** If $a \neq 0$ in a commutative ring has $b \neq 0$ such that $ab = 0$.
- **Unit:** An element u in a (commutative) Ring is a unit, if u is invertible: $uv = vu = 1$. **The set of units is** R^*.

For Ring R, R^* is multiplicative Group:

Proof. We need to show that R^* is closed under multiplication, i.e., that for $u \in R^*$ and $v \in R^*$, we also have $uv \in R^*$, which means that uv has an inverse. The inverse of uv is $v^{-1}u^{-1}$ since $(uv)(v^{-1}u^{-1}) = uvv^{-1}u^{-1} = uu^{-1} = 1$. R^* also contains the neutral element 1 (since 1 has an inverse). Moreover, the associativity of multiplication in R^* is inherited from the associativity of multiplication in R (since elements of R^* are also elements of R and the multiplication operation is the same). $\square$

Ring with $aa = a$**,** $a = -a$ **commutes**. Look at $(a+b) = (a+b)^2$ and $(b+a)$..
$\mathbb{Z}_4$ **not a field** Since 2 doesn't have an inverse.

Ex: Number of Units in $\mathbb{Z}_{12}$ Just $|\mathbb{Z}_{12}^*| = \phi(12) = 4$

Definition: Integral Domain An Integral Domain is a nontrivial commutative ring without zerodivisors. $(\forall a \forall b (ab = 0 \implies a = 0 \vee b = 0))$

Some Integral Domains / Zero Divisors

- For a ring R, R^* is a multiplicative group.
- Any element of $\mathbb{Z}_m$ not relatively prime to m is a zerodivisor. Since if $m = ab$, a, b are zerodivisors.
- Z_m is not an integral domain if m is not prime since $ab = m$ are zero divisors.

Lemma 5.20 - Unique Divisor In an integral domain, if $a|b$ then c is unique with $b = ac$

$D[x]$ **is Integral Domain** If D is an integral domain, so is $D[x]$.

Units of $D[x]$ **are units of** D**,** $(D^* = D[x]^*)$ This means constant polynomials are only units. *Proof* Only degree 0 polynomial can be unit (because can't reduce dimensions in polynomial). They are units since they have an inverse, (from D).

Field is Int. Domain / Unit not Zero Div: A field is always an integral domain. We show every non-zero element is not a zero divisor, hence in any commutative ring, a unit $u \in R$ is not a zero div. by contradiction: Assume $uv = 0$, then $v = 1v = u^{-1}uv = u^{-1}0 = 0$, hence u is not a zero div. since $v = 0$.
$\rightarrow$ Zero doesn't have inverse but is still in field!

Fields

Definition: Field A field is a nontrivial commutative ring F in which every nonzero element is a unit, i.e. $F^* = F \setminus \{0\}$. Furthermore, $GF(p)$ stands for Galois Field with p elements, it is just a field with p elements.

Examples: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields, but $\mathbb{N}, \mathbb{Z}$ are not, no inverse $\forall$.

Direct Prod not a field $\langle F; +, \cdot \rangle$ a field. $\langle F \times F; \oplus, \otimes \rangle$ not a field. $(0,0)$ is additive neutral. But $(1,0) \otimes (0,1) = (0,0)$ so there are zerodivisors. So it is not a field.

$\mathbb{Z}_p$ **is a field iff.** p **is prime** Follows since $\mathbb{Z}_p \setminus \{0\} = \mathbb{Z}_p^*$ is a multiplicative group, iff. p is prime.

Linear Equations in Fields

We solve $5x \oplus 2y = 4, 2x \oplus 7y = 9$ over $\mathbb{Z}_{11}, GF(11)$.

$$\left(\begin{array}{cc|c} 5 & 2 & 4 \\ 2 & 7 & 9 \end{array}\right) \xrightarrow{z_2 + 2z_1} \left(\begin{array}{cc|c} 5 & 2 & 4 \\ 1 & 0 & 6 \end{array}\right)$$

$$\xrightarrow{z_1 + 6z_2} \left(\begin{array}{cc|c} 0 & 2 & 7 \\ 1 & 0 & 6 \end{array}\right) \quad \begin{array}{l} x = 6 \\ 2y = 7, \end{array} \quad y = \overset{\text{``}6}{2^{-1}} \cdot 7 = 9$$

$\rightarrow x = 6$
$y = 9$

Polynomials in fields

Polynomial Division in a field

Wir möchten $x^4 + x + 1$ durch $x^2 + x + 1$ teilen in $GF(2)[x]$

$$\begin{array}{l} (x^4 + x + 1) : (x^2 + x + 1) = (x^2 + x \\ \underline{-(x^4 + x^3 + x^2)} \\ \quad x^3 + x^2 + x + 1 \\ \underline{-(x^3 + x^2 + x)} \\ \qquad\qquad 1 \end{array}$$

Trick: make sure you stay in $GF(2)[x]$

Definition - Irreducible Polynomial A Polynomial $a(x)$ is called irreducible if it is only divisible by constant Polynomials and by constant multiples of $a(x)$. We check irreducibility of $a(x)$ of degree d by testing all monic irreducible Polynomials of degree $\leq d/2$.

Factorization of Polynomials:

- A Polynomial of degree 1 is always irreducible by def. A
- Poly of deg 2,3 must have factor of deg 1 if reducible, therefore they are irreducible if they don't have a root.
- Poly. of degree 4. First check for roots, then for irreducible factors of degree 2.
- else, check all irred. polys of deg $< d/2$.

Factorization Example: find roots of $x^2 + 3x + 2$ in $GF(5)$. We check all elements of $GF(5)$ and find that $x^2 + 3x + 2 = (x-3)(x-4)$

Multivar. Factorization Example: Factor $xy^3 + xy^2 + (x+1)y + x$ on $GF(2)[x]_{x^2+x+1}[y]$ into irred. We first check for roots and find $a(x) = 0$. Therefore we can poly div by $(x-y) = (x+y)$ Using $x^2 = x+1$ we find $a(x) = (y+x)(xy^2 + y + 1)$

Remainder & GCD The monic Polynomial $g(x)$ of largest degree such that $g(x)|a(x)$ and $g(x)|b(x)$ is the $gcd(a(x), b(x))$. If F a field and $a(x), b(x) \neq 0$ there exists unique $q(x)$ s.t. $a(x) = b(x)q(x) + r(x)$

Definition: Roots Let $a(x) \in R[x]$. An element $\alpha \in R$ for which $a(\alpha) = 0$ is called a root of $a(x)$. (to prove this use division with remainder) A Polynomial of degree d can have at most d roots.

Extension Fields: If $m(x)$ irreducib. with $deg(m) = d$ over field F, then $F[x]_{m(x)} = \{a(x) \in F[x] | dex(a(x)) < d\}$ is a field with, if F has q elements $|F[x]_{m(x)}| = q^d$ elements.

Construct a field with 9 elements: We can construct $GF(9)$ as the extension field of $GF(3)$, by listing all Polynomials in $GF(3)$ with degree smaller than 2 and modulus x^2+1. Therefore $GF(9) = \{0, 1, 2, x, 2x, x+1, x+2, 2x+1, 2x+2\}$. This builds on the fact that $GF(9) = GF(3)_m$, with m irreducible. Also all operations are alrady defined in $GF(3)_{x^2+1}$.
Find a generator of the field above The field has 9 elements, 8 of which are non zero and invertible. By lagrange's theorem the order of any element in $F^* = F \setminus \{0\}$ must divide the order of F^*. The possible orders are $\{1, 2, 4, 8\}$, we are therefore looking for an element a such that $a^4 \neq 1$. $a = x+1$ since $(x+1)^4 = 2 \neq 1$. Hence $x+1$ is a generator of F^*.

Error Correction

Let alphabet= $\mathcal{A} = GF(q)$ and let $\alpha_1, \ldots, \alpha_{n-1}$ arbitrary elements from $GF(q)$, with $E((a_0, \ldots, a_{k-1})) = (a(\alpha_1), \ldots, a(\alpha_{n-1}))$. The code has a min. dist. of $n - k + 1$. Idea: We can interpolate $a(x)$ of deg $k-1$ by any k codeword symbols.