

D.2.1 A **mathematical statement** (=proposition) is true/false

| A | B | $A \wedge B$ | $A \vee B$ | $A \rightarrow B$ | $A \leftrightarrow B$ |
|---|---|--------------|------------|-------------------|-----------------------|
| 0 | 0 | 0            | 0          | 1                 | 1                     |
| 0 | 1 | 0            | 1          | 1                 | 0                     |
| 1 | 0 | 0            | 1          | 0                 | 0                     |
| 1 | 1 | 1            | 1          | 1                 | 1                     |

D.2.4  
 $\neg$  negation  
 $\vee$  disjunction  
 $\wedge$  conjunction

D.2.5 A **formula** consists of logical operators and propositional symbols  
 $A \rightarrow B \equiv \neg A \vee B$

**General Concepts**

D.6.4 Syntax of a logic defines alphabet  $\Sigma$  and defines which strings in  $\Sigma^*$  are formulas

D.6.5 Semantics define a function free, which assigns each F a set of indices which are free symbols

D.6.6 Interpretation  $\mathcal{A}$  assigns each symbol in  $\Sigma$ ,  $z \in \Sigma$  a value

D.6.7  $\mathcal{A}$  is **suitable** for F if it assigns a value to all free symbols

D.6.8 Semantics also defines a function  $\sigma(F, \mathcal{A}) \rightarrow \{0, 1\}$  or  $\mathcal{A}(F)$  being the truth value of F under interpretation  $\mathcal{A}$

D.6.9 If  $\mathcal{A}(F) = 1$ ,  $\mathcal{A}$  is called a **model** for F ( $\mathcal{A} \models F$ ), for a set of formulas  $M$ :  $\mathcal{A} \models M$ , or if not a model:  $\mathcal{A} \not\models M$

**(un-)satisfiability, Tautology, Consequence, Equivalence**

D.6.10 F is **satisfiable** if there exists a model and **unsatisfiable** otherwise

D.6.11 F is **tautology** (T) if it is true for every suitable  $\mathcal{A}$  ( $\models F$  D.6.14)

D.6.12  $g$  is **logical consequence** of  $F$  ( $F \models g$ ) if every suitable interpretation for  $F$  and  $g$ , which is a model for  $F$  is also a model for  $g$  (analogously:  $F \not\models g$ )

D.6.13  $F$  and  $g$  are **equivalent**:  $F \equiv g \iff F \models g$  and  $g \models F$

L.6.2 F is tautology  $\iff \neg F$  is unsatisfiable

L.2.3  $F \rightarrow g$  is tautology  $\iff F \models g$

L.2.5  $(A \rightarrow B) \wedge (B \rightarrow C) \models A \rightarrow C$

L.2.6  $\neg B \rightarrow \neg A \models A \rightarrow B$

L.2.7  $A \wedge (A \rightarrow B) \models B$

L.2.8 for every  $k$ :  $(A_1 \vee \dots \vee A_k) \wedge (A_1 \rightarrow B) \wedge \dots \wedge (A_k \rightarrow B) \models B$

L.2.9  $(\neg A \rightarrow B) \wedge \neg B \models A$

T.2.11 for  $\mathbb{N}$  and unary  $P$ :  $P(0) \wedge \forall n (P(n) \rightarrow P(n+1)) \implies \forall n P(n)$

L.6.3 The following statements are equivalent: (Res. calculus)

- $\exists F_1, F_2, \dots, F_k \models g$
- $\exists F_1 \wedge F_2 \wedge \dots \wedge F_k \models g$  is tautology
- $\exists F_1, F_2, \dots, F_k, \neg g \models$  is unsatisfiable

**Logical Operators**

D.6.15 If  $F$  and  $g$  are formulas, so are  $\neg F$ ,  $(F \vee g)$ ,  $(F \wedge g)$

- $\mathcal{A}((F \wedge g)) = 1 \iff \mathcal{A}(F) = 1 \text{ and } \mathcal{A}(g) = 1$
- $\mathcal{A}((F \vee g)) = 1 \iff \mathcal{A}(F) = 1 \text{ or } \mathcal{A}(g) = 1$
- $\mathcal{A}(\neg F) = 1 \iff \mathcal{A}(F) = 0$
- $\mathcal{A}((F \wedge g)) = 0 \iff \mathcal{A}(F) = 0 \text{ or } \mathcal{A}(g) = 0$
- $\mathcal{A}((F \vee g)) = 0 \iff \mathcal{A}(F) = 0 \text{ and } \mathcal{A}(g) = 0$

General concepts - unsatisfiability, tautology, consequence, equivalence - logical operators

- L.6.1
- $F \wedge F \equiv F$  and  $F \vee F \equiv F$
  - $F \wedge g \equiv g \wedge F$  and  $F \vee g \equiv g \vee F$
  - $(F \wedge g) \wedge h \equiv F \wedge (g \wedge h)$  and  $(F \vee g) \vee h \equiv F \vee (g \vee h)$
  - $F \wedge (F \vee g) \equiv F$  and  $F \vee (F \wedge g) \equiv F$
  - $F \wedge (g \vee h) \equiv (F \wedge g) \vee (F \wedge h)$
  - $F \vee (g \wedge h) \equiv (F \vee g) \wedge (F \vee h)$
  - $\neg \neg F \equiv F$
  - $\neg(F \wedge g) \equiv \neg F \vee \neg g$  and  $\neg(F \vee g) \equiv \neg F \wedge \neg g$
  - $F \vee \neg F \equiv \top$  and  $F \wedge \neg F \equiv \perp$
  - $F \vee \perp \equiv F$  and  $F \wedge \top \equiv F$
  - $F \vee \neg F \equiv \top$  and  $F \wedge \neg F \equiv \perp$

idempotence  
Commutativity  
associativity  
absorption  
distributive law  
distributive law  
double negation  
de Morgan's rules  
tautology rules  
unsatisfiability rules

**Logical calculi**

D.6.17 Derivation rule  $\exists F_1, \dots, F_k \models g$  or  $\frac{F_1, \dots, F_k}{g}$  derives new formula from set of formulas

D.6.18 Application of derivation rule  $R$ : 1) select  $N \models M$  ( $M$  is set of formulas)

2) Specify formulas for placeholder  $N \models g$  3) add  $g$  to set:  $M' = M \cup \{g\}$

D.6.19 Calculus  $K$  is a finite set of derivation rules:  $K = \{R_1, \dots, R_m\}$

D.6.20 Derivation of formula  $g$  from  $M$  in  $K$  is a finite sequence of applications of rules in  $K$ , leading to  $g$ :  $M \vdash_K g$

D.6.21 Derivation rule is **correct** if for every  $M$  and  $F$ :  $M \vdash F \implies M \models F$

D.6.22 Calculus is **correct/sound** if for every  $M$  and  $F$ :  $M \vdash F \implies M \models F$

Calculus is **complete** if for every  $M$  and  $F$ :  $M \models F \implies M \vdash F$  ex:  $\neg \vdash \neg \neg F$

L.6.3 If  $\exists F_1, \dots, F_k \models g$  holds for a sound calculus, then:  $F \models (F_1 \wedge \dots \wedge F_k \rightarrow g)$   
( $F \models g \iff F \wedge \neg g$  is unsatisfiable)

**Propositional logic**

D.6.23 Atomic formula is a formula and of the form  $A_i$ ,  $i \in \mathbb{N} \implies$  D.6.15

D.6.24 Truth assignment is a function  $\mathcal{A}: \Sigma \rightarrow \{0, 1\}$  which applies an interpretation  $\mathcal{A}$  on a set of atomic formulas  $\Sigma$ .  $\mathcal{A}(F) = \mathcal{A}(A_i) \implies$  D.6.7 D.6.16

D.6.25 Literal is an atomic formula or its negation

D.6.26 CNF - Conjunctive normal form:  $(L_1 \vee \dots \vee L_{m_1}) \wedge \dots \wedge (L_{n_1} \vee \dots \vee L_{n_m})$

D.6.27 DNF - Disjunctive normal form:  $(L_1 \wedge \dots \wedge L_{m_1}) \vee \dots \vee (L_{n_1} \wedge \dots \wedge L_{n_m})$

T.6.4 Every formula is equivalent to a formula in CNF and in DNF

Recipe  $F \mapsto$  DNF/CNF

- compute truth table
- take the rows which are true/false, write (row)  $\vee \wedge$  (rows)
- write all symbols  $(A_1 \vee \dots \vee A_n)$   $A_i$ : if  $A_i = 1/0$  else  $\neg A_i$

**Resolution Calculus** ( $\text{Res} = \{ \text{res} \}$ )

D.6.28 Clause is a set of literals

D.6.29  $\mathcal{K}(F)$  denotes the set  $\{ \{L_1, \dots, L_{m_1}, \neg L_{n_1}, \dots, \neg L_{n_m}\} \}$ , where  $F$  is a formula in CNF.  $\implies$  D.6.26. The set of clauses for  $M = \{F_1, \dots, F_k\}$ :  $\mathcal{K}(M) = \bigcup_{i=1}^k \mathcal{K}(F_i)$

D.6.30 Clause is **resolvent** of clauses  $K_1, K_2$  if there is a literal  $L$  s.t.  $L \in K_1$ ,  $\neg L \in K_2$  and  $K = (K_1 \setminus \{L\}) \cup (K_2 \setminus \{\neg L\})$

L.6.5 The resolution calculus is sound  $\mathcal{K} \models K \implies \mathcal{K} \models K$  (D.6.22)

Ex Prove that the resolution calculus is not complete: Let  $t = A$  and  $g = A \vee B$ . We know  $F \models g$  but we can't derive  $\mathcal{K}(A \vee B)$  from  $\mathcal{K}(A)$  using the resolution calculi

A set  $M$  of formulas is unsatisfiable  $\iff \mathcal{K}(M) \models \emptyset$  Tautology:  $\mathcal{K}(M) \models \emptyset$

Resolution step must be carried out one by one  $\exists A \exists B \exists C \exists D \exists E \exists F \exists G \exists H \exists I \exists J \exists K \exists L \exists M \exists N \exists O \exists P \exists Q \exists R \exists S \exists T \exists U \exists V \exists W \exists X \exists Y \exists Z \exists \neg A \exists \neg B \exists \neg C \exists \neg D \exists \neg E \exists \neg F \exists \neg G \exists \neg H \exists \neg I \exists \neg J \exists \neg K \exists \neg L \exists \neg M \exists \neg N \exists \neg O \exists \neg P \exists \neg Q \exists \neg R \exists \neg S \exists \neg T \exists \neg U \exists \neg V \exists \neg W \exists \neg X \exists \neg Y \exists \neg Z \exists \neg \neg A \exists \neg \neg B \dots$

One can write  $\exists K_1, K_2 \models K$ . CNF!

Empty clause unsatisfiable, empty clause set tautology  
logical calculi - propositional logic - resolution calculus - Predicate logic

**Predicate Logic**

D.6.31 Syntax:

- symbols
- variable symbol:  $x_i$ ,  $i \in \mathbb{N}$
  - function symbol:  $f_i^{(n)}$ ,  $i, k \in \mathbb{N}$ ,  $k = \# \text{arguments}$ ,  $k=0$ : constants
  - predicate symbol:  $P_i^{(n)}$ ,  $i, k \in \mathbb{N}$ ,  $k = \# \text{arguments}$
- inductively
- term = variable or:  $t_1, \dots, t_k$  are terms  $\implies f_i^{(k)}(t_1, \dots, t_k)$  is term
  - formula

- $t_1, \dots, t_k$  are formulas  $\implies P_i^{(k)}(t_1, \dots, t_k)$  is an **atomic formula**
- $F$  and  $g$  are formulas  $\implies \neg F, (F \wedge g), (F \vee g)$  are formulas
- $F$  is formula  $\implies$  for any  $i$   $\forall x_i F$  and  $\exists x_i F$  are formulas

D.6.32 Every variable is either **free** or **bound**. If a variable  $x$  occurs in a (sub) formula of the form  $\forall x g$  or  $\exists x g$  then it is bound, otherwise it is free.  $F$  is **closed** if all variables are bound

D.6.33  $FC[x/H]$  denotes the formula obtained from  $F$  by substituting every free occurrence of  $x$  (variable) by  $t$  (term)

D.6.34 Semantic: interpretation/structure is a tuple  $\mathcal{A} = (U, \phi, \psi, \xi)$

- $U$  non-empty set, the universe  $\rightsquigarrow U^{\mathcal{A}}$
- $\phi$  function assigning to each function symbol a function:  $k$ -ary function if:  $\phi(f): U^k \rightarrow U \rightsquigarrow f^{\mathcal{A}}$
- $\psi$  function assigning to each predicate symbol a predicate:  $k$ -ary function if:  $\psi(P): U^k \rightarrow \{0, 1\} \rightsquigarrow P^{\mathcal{A}}$
- $\xi$  function assigning to each variable symbol a value in  $U$

D.6.35  $\mathcal{A}$  is **suitable** for  $F$  if all functions, predicates, free variables are defined

D.6.36 Semantic for  $\mathcal{A}$ :

- value  $\mathcal{A}(t)$ 
  - variables  $t = x_i$ :  $\mathcal{A}(t) = \xi(x_i)$
  - $F$  in form  $F = f(t_1, \dots, t_k) \implies \mathcal{A}(F) = \phi(f)(\mathcal{A}(t_1), \dots, \mathcal{A}(t_k))$
- truth value of a formula:  $\rightsquigarrow$  D.6.16 and
  - $F$  in form  $F = P(t_1, \dots, t_k) \implies \mathcal{A}(F) = \psi(P)(\mathcal{A}(t_1), \dots, \mathcal{A}(t_k))$
  - $F$  in form  $\forall x g$  or  $\exists x g$   $\implies$  then let  $\mathcal{A}[x \mapsto u]$  for  $u \in U$  be the same structure as  $\mathcal{A}$  except that  $\xi(x)$  is overwritten by  $u$   $\xi(x) = u$ 
    - $\mathcal{A}(\forall x g) = \begin{cases} 1 & \text{if } \mathcal{A}[x \mapsto u](g) = 1 \text{ for all/some } u \in U \\ 0 & \text{else} \end{cases}$
    - $\mathcal{A}(\exists x g) = \begin{cases} 1 & \text{if } \mathcal{A}[x \mapsto u](g) = 1 \text{ for all/some } u \in U \\ 0 & \text{else} \end{cases}$

L.6.8 For any formulas  $F, g$  and  $H$ , where  $x$  isn't free in  $H$

- $\neg(\forall x F) \equiv \exists x \neg F$
- $\neg(\exists x F) \equiv \forall x \neg F$
- $(\forall x F) \wedge (\forall x g) \equiv \forall x (F \wedge g)$
- $(\exists x F) \vee (\exists x g) \equiv \exists x (F \vee g)$
- $\forall x \forall y F \equiv \forall y \forall x F$
- $\exists x \exists y F \equiv \exists y \exists x F$
- $(\forall x F) \wedge H \equiv \forall x (F \wedge H)$
- $(\forall x F) \vee H \equiv \forall x (F \vee H)$
- $(\exists x F) \wedge H \equiv \exists x (F \wedge H)$
- $(\exists x F) \vee H \equiv \exists x (F \vee H)$

L.6.9 If one replaces a sub-formula  $g$  of  $F$  by an equivalent (to  $g$ ) formula  $H$ , then the resulting formula is equivalent to  $F$

L.6.10 For a formula  $g$  in which  $y$  does not occur:  
 $\forall x g \equiv \forall y g[x/y]$   $\exists x g \equiv \exists y g[x/y]$

D.6.37 Rectified form: no variable occurs both as free and bound

L.6.11 Universal instantiation: for any  $F$  and  $t$ :  $\forall x F \models FC[x/t]$

D.6.38 Prenex form:  $Q_1 x_1 Q_2 x_2 \dots Q_n x_n g$ ,  $Q_i$  are quantifiers ( $\forall/\exists$ ), none is

T.6.12 For every formula there is an equivalent in prenex form

Recipe  $F \mapsto$  Prenex

- rename all bound variables
- remove all  $\rightarrow$
- apply L.6.11
- shift  $\exists, \forall$  to front

T.6.13  $\exists x \forall y (P(x,y) \leftrightarrow \neg P(y,x)) \equiv \exists x \exists y (P(x,y) \leftrightarrow \neg P(y,x))$  is tautology  
 C.6.14  $U^A = \text{all sets}$ ,  $P(u,v) = u \in v \rightsquigarrow$  Russell paradox  
 C.6.15  $U^A = \mathbb{N}$ ,  $P(u,v) = u$ -th bit in  $v$ -th sequence  $\rightsquigarrow$  Kants diagonalising argument  
 C.6.16  $U^A = \mathbb{N} = \{0,1\}^*$ ,  $P(u,v) =$  Output bit of  $v$ -th program of input  $u$   $\rightsquigarrow$  uncomputable function  
 Ex Prove  $\forall x (F \wedge G) \vdash (\forall x F) \wedge G$   
 Let  $F$  and  $G$  be any suitable formulas. Let  $\lambda$  be any structure suitable for  $\forall x (F \wedge G)$  and  $(\forall x F) \wedge G$   
 Assume  $\lambda \models (\forall x (F \wedge G)) = 1$   
 $\lambda \models_{x \rightarrow u} (F \wedge G) = 1$  for any  $u \in U^A$  (Sem V)  
 $\lambda \models_{x \rightarrow u} F = 1$  and  $\lambda \models_{x \rightarrow u} G = 1$  for any  $u \in U^A$  (Sem V)  
 $\lambda \models (\forall x F) = 1$  and  $\lambda \models_{x \rightarrow u} G = 1$  for any  $u \in U^A$  (Sem V)  
 Case 1:  $x$  does not occur free: Then for any  $u$  we have  $\lambda \models_{x \rightarrow u} G = \lambda(G)$ . So  $\lambda(G) = \lambda \models_{x \rightarrow u} G = 1$   
 Case 2:  $x$  does occur free: Then  $x$  occurs free in  $(\forall x F) \wedge G$ . So, if  $\lambda$  is suitable, it defines  $x \in U^A$   
 Since  $\lambda \models_{x \rightarrow u} G = 1$  for all  $u \in U^A$ , we have in particular for  $u = x^A$ ,  $\lambda \models_{x \rightarrow x^A} G = 1$ . So,  $\lambda(G) = \lambda \models_{x \rightarrow x^A} G = 1$   
 Therefore:  $\lambda \models (\forall x F) = 1$  and  $\lambda(G) = 1 \xrightarrow{\text{sem}} \lambda \models ((\forall x F) \wedge G) = 1$

**Proof systems**

D.6.1 Proof system is a quadruple  $\Pi = (S, P, \tau, \phi)$   
 $S$ : Statement  $\tau$ : truth function  $\tau: S \rightarrow \{0,1\}$   
 $P$ : proof  $\phi$ : verification function  $\phi: S \times P \rightarrow \{0,1\}$   
 D.6.2 A proof system is **sound** if no false statement has a proof:  
 for all  $s \in S$  for which there exists  $p \in P$  with  $\phi(s,p) = 1$ , we have  $\tau(s) = 1$   
 D.6.3 A proof system is **complete** if every true statement has a proof:  
 for all  $s \in S$  with  $\tau(s) = 1$ , there exists  $p \in P$  with  $\phi(s,p) = 1$   
 Ex It is defined that  $S = P = \{0,1\}^*$  give  $\tau$  and  $\phi$   
 $\tau(s) = 1$  if  $s$  contains at most one 0  
 $\phi(s,p) = 1$  if  $s$  contains at most two 0 and  $s = p$   
 $\tau(s) = 1$  if  $s$  contains at least one 1  
 $\phi(s,p) = 1$  if  $d(s,p) = 3$  and  $p$  contains exactly one 0  
 $\hookrightarrow$  Hamming distance

**Proof Pattern**

D.2.13 Composition of implications: If  $S \Rightarrow T$  and  $T \Rightarrow U$  are both true, then one concludes that  $S \Rightarrow U$  is true  $\rightsquigarrow$  L.2.5  
 D.2.14 Direct proof of an implication: Prove  $S \Rightarrow T$ , by assuming  $S$  and then proving  $T$  under this assumption  
 D.2.15 Indirect proof of an implication: Prove  $S \Rightarrow T$ , by assuming  $T$  is false and proving that  $S$  is false under this assumption L.2.6  
 D.2.16 Modus Ponens: Proof  $S$  by finding a suitable  $R$ . Prove  $R$ . Prove  $R \Rightarrow S$  L.2.7  
 D.2.17 Case distinction: Proof  $S$  by finding a finite list of statements  $R_1, \dots, R_k$  ( $=$  Cases). Prove the one occurs. Prove  $R_i \Rightarrow S$  for  $i = 1, \dots, k$  L.2.8  
 D.2.18 Proof by contradiction: Proof  $S$  by finding suitable statement  $T$ . Prove that  $T$  is false. Assume  $S$  is false and prove that  $T$  is true under the assumption ( $=$  contradiction)  $\rightsquigarrow$  L.2.9  
 D.2.19 Existence Proof: Prove  $S$  by showing  $S$  holds for at least one  $x \in X$ , if true **constructive** else **non-constructive**  
 T.2.10 Pigeonhole principle: the following statement is used in existence proof: If set of  $n$  objects is partitioned into  $k < n$  sets, then at least one of these sets contains at least  $\lceil \frac{n}{k} \rceil$  objects  
 Proof systems - Proof pattern - Sets/relations/functions - relations - special properties on relations - equivalence relations - poset

D.2.13 Proof by counterexample: Proof  $S$  is not true for all  $x$  by finding a counterexample. (Constructive existence proof)  
 D.2.20 Proof by induction: Prove Base Case  $P(0)$ . Prove for any  $n$   $P(n) \Rightarrow P(n+1)$  T.2.11

**Sets, Relations and Functions**

D.3.1 Cardinality of a finite set  $A = |A| = \#$  of elements in  $A$   $|\emptyset| = 0$   
 D.3.2  $A = B \iff \forall x (x \in A \leftrightarrow x \in B)$   
 D.3.3  $A \subseteq B \iff \forall x (x \in A \rightarrow x \in B)$  every  $x \in A$ , is also in  $B$   
 L.3.1  $\exists a \exists b \Rightarrow \exists b \exists a \Rightarrow a = b$   
 Def Ordered pairs  $(A,B) = \{ \{a,b\}, \{a,b\} \}$ , has to satisfy:  $(a,b) = (c,d) \iff a=c \wedge b=d$   
 L.3.2  $A = B \iff (A \subseteq B) \wedge (B \subseteq A)$ , follows from D.3.2 / D.3.3  
 L.3.3  $A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$   
 D.3.4 Union:  $A \cup B = \{x | x \in A \vee x \in B\}$   
 D.3.4 Intersection:  $A \cap B = \{x | x \in A \wedge x \in B\}$   
 D.3.5 Difference:  $B \setminus A = \{x \in B | x \notin A\}$   
 T.3.4  
 $A \cap A = A$  and  $A \cup A = A$  Idempotence  
 $A \cap B = B \cap A$  and  $A \cup B = B \cup A$  Commutativity  
 $A \cap (B \cap C) = (A \cap B) \cap C$  and  $A \cup (B \cup C) = (A \cup B) \cup C$  Associativity  
 $A \cap (A \cup B) = A$  and  $A \cup (A \cap B) = A$  Absorption  
 $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$  and  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$  Distributivity  
 $A \subseteq B \iff A \cap B = A \iff A \cup B = B$  Consistency

D.3.6 Empty set contains no elements:  $\emptyset = \{x | \neg (x \in A)\} = \{x | x \notin A\}$   
 L.3.5 There exists only one empty set  
 L.3.6 Empty set is a subset of every set:  $\forall A (\emptyset \subseteq A)$   $\emptyset \subseteq \emptyset$   
 D.3.7 Power set of a set  $A$ , is the set of all subsets:  $\mathcal{P}(A) = \{S | S \subseteq A\}$   
 $|A| = k \Rightarrow |\mathcal{P}(A)| = 2^k$ ,  $\mathcal{P}(\emptyset) = \{\emptyset\}$ ,  $\mathcal{P}(\{0\}) = \{\emptyset, \{0\}\}$   $\forall A \mathcal{P}(A) = \{ \emptyset, \dots \}$   
 D.3.8 Cartesian product of two sets is the set of all ordered pairs:  $A \times B = \{(a,b) | a \in A \wedge b \in B\}$   
 $\phi \times A = \emptyset$ , cartesian product not associative  $\{0\} \times \{\{0\}\} = \{\emptyset, \{0\}\}$   
**Relation**  
 D.3.9 Relation  $p$  from a set  $A$  to set  $B$  is a subset of  $A \times B$ . If  $A=B$ ,  $p$  is relation on  $A$   
 D.3.10 Identity relation  $id_A = \{(a,a) | a \in A\}$   
 D.3.12 Inverse of  $p$ :  $p^{-1} = \{(a,b) | (b,a) \in p\}$   
 D.3.13 Composition of  $p$  and  $q$ :  $p \circ q = \{(a,c) | \exists b ((a,b) \in p \wedge (b,c) \in q)\}$   
 L.3.7 The composition of relations is associative:  $p \circ (q \circ r) = (p \circ q) \circ r$   
 L.3.8  $p \circ p = p^2$

**Special properties on relations**

D.3.13 Reflexive  $a p a$ ,  $id \subseteq p$   $(a,a) \in p$   
 D.3.14 Irreflexive  $a \not p a$  for all  $a \in A$ ,  $p \cap id = \emptyset$   $(a,a) \notin p$   
 D.3.15 Symmetric  $a p b \iff b p a$ ,  $p = p^{-1}$   $(a,b) \in p \Rightarrow (b,a) \in p$   
 D.3.16 Antisymmetric  $a p b \wedge b p a \Rightarrow a = b$ ,  $p \cap p^{-1} \subseteq id$   $(a,b) \in p \Rightarrow (b,a) \notin p$   
 D.3.17 Transitive  $a p b \wedge b p c \Rightarrow a p c$   $(a,b) \in p \wedge (b,c) \in p \Rightarrow (a,c) \in p$   
 L.3.9 A relation is transitive  $\iff p^2 \subseteq p$   
 D.3.18 Transitive closure  $p^+ = \bigcup_{n \in \mathbb{N}} p^n$

**Equivalence Relations**

D.3.19 Equivalence relation is reflexive, symmetric, and transitive  
 D.3.20 Equivalence classes: set of elements, which are equivalent to  $a$  in an equivalence relation  $\theta$ :  $[a]_\theta = \{b \in A | b \theta a\}$   
 L.3.10 An intersection of two equiv. relations, on the same set is an equiv relation  
 D.3.21 Partition of a set  $A$ , is a set of mutually disjoint subsets of  $A$ .  $A = \bigcup_{i \in I} S_i$   $S_i \cap S_j = \emptyset$  for  $i \neq j$  and  $\bigcup_{i \in I} S_i = A$  ( $I =$  Index set) satisfying:

D.3.22 Quotient set of  $A$  by  $\theta$  /  $A$  modulo  $\theta$ : Set of equivalence classes of an equivalence relation  $\theta$ :  $A/\theta = \{[a]_\theta | a \in A\}$   
 T.3.11 The set  $A/\theta$  of equiv. classes of an equiv. relation is a partition of  $A$   
 Ex Let  $p, q$  be an equivalence relation, prove that  $p \circ q$  is an equiv. relation if  $p \circ q = q \circ p$   
 $\bullet$  reflexive:  $\forall a \in A (a p a \wedge a q a) \Rightarrow (a, a) \in p \circ q$  ( $p, q$  reflexive)  
 $\Rightarrow \forall a \in A (a p \circ q a)$  (def  $\circ$ )  
 $\bullet$  symmetric: For any  $a, b \in A$ ,  $(a,b) \in p \circ q$   
 $\Rightarrow (b,a) \in p \circ q$  (def inverse)  
 $\Rightarrow (b,a) \in q \circ p$  ( $q \circ p = p \circ q$ )  
 $\Rightarrow (b,a) \in p \circ q$  (L.3.8)  
 $\Rightarrow (b,a) \in p \circ q$  (symmetry of  $p, q$ )  
 $\bullet$  transitive: Use L.3.9 to show  $(p \circ q)^2 = p \circ q$   
 $(p \circ q) \circ (p \circ q)$   
 $\Rightarrow p \circ (q \circ p) \circ q$  (L.3.7)  
 $\Rightarrow p \circ (p \circ q) \circ q$  ( $q \circ p = p \circ q$ )  
 $\Rightarrow (p \circ p) \circ (q \circ q)$  (L.3.7)  
 $\Rightarrow p^2 \circ q^2 \Rightarrow p \circ q$  ( $p, q$  are transitive)

**Partial ordered set (Poset)**

D.3.23 Partial order on a set is a relation which is reflexive, antisymmetric, and transitive. A set  $A$  with a partial order  $\leq$  is called Partially ordered set ( $A, \leq$ )  
 D.3.24 Two elements are **comparable** if  $a \leq b$  or  $b \leq a$ , else **incomparable**  
 D.3.25 **Totally ordered** if any two elements in the set are comparable  
 D.3.26 Element  $b$  **covers** element  $a$  if  $a < b$  and no exists  $s.t. a < c < b$   
 D.3.27 Hasse diagram of a finite Poset, is a directed graph, whose vertices  $\in A$  and edge  $(a,b)$  means that  $a$  covers  $b$   
 D.3.28 Direct product of posets  $(A, \leq) \times (B, \leq)$  is the set  $(A \times B)$  with the relation  $\leq$ .  $(a_1, b_1) \leq (a_2, b_2) \iff a_1 \leq a_2 \wedge b_1 \leq b_2$   
 $(A, \leq) \times (B, \leq)$  is a poset  
 T.3.12 Lexicographic order:  $(a_1, b_1) \leq_{lex} (a_2, b_2) \iff a_1 < a_2 \vee (a_1 = a_2 \wedge b_1 \leq b_2)$   
 D.3.29 Let  $(A, \leq)$  be a poset and  $S \subseteq A$ .  $a \in A$  is...

1) **minimal** **maximal** if:  $\exists b \in A$  s.t.  $b < a$ ,  $b > a$  upper bound  
 2) **least** **greatest** if  $\forall b \in A$   $a \leq b$ ,  $a \geq b$   $A \cup B$   
 3) **lower** **upper** bound of  $S$  if  $\forall b \in S$   $a \leq b$ ,  $a \geq b$   
 4) **greatest lower** **least upper** bound of  $S$  if  $a$  is the **greatest** **least** of the set of all **lower** **upper** bounds of  $S$   
 D.3.30 Well-ordered poset if it is totally ordered and every non-empty subset has a least element  
 D.3.31 Meet join: if  $\{a,b\}$  has **greatest lower** **least upper** bound:  $a \vee b$   
 D.3.32 Lattice is a poset in which every pair has a meet and a join  
 Ex. Show that  $\forall a,b ((a p b \wedge b p a) \rightarrow a = b) \iff p \cap p^{-1} = id$   
 Let  $(a,b) \in p \cap p^{-1}$  be arbitrary  
 $(a,b) \in p \cap p^{-1} \wedge p \cap p^{-1} = id$   
 $\iff (a,b) \in p \wedge (a,b) \in p^{-1} \rightarrow (a,b) \in id$  (def  $\cap$ ,  $id = p \cap p^{-1}$ )  
 $\iff (a,b) \in p \wedge (b,a) \in p \rightarrow (a,b) \in id$  (def inverse)  
 $\iff (a p b \wedge b p a) \rightarrow a = b$  (def  $id$ )  
 $\iff p$  is antisymmetric

Functions

- D.3.33 Function  $f: A \rightarrow B$  from a domain  $A$  to codomain  $B$ , is a relation from  $A$  to  $B$ , with the properties:
  - 1)  $\forall a \in A \exists b \in B \ a \mapsto b$  ( $f$  is totally defined)
  - 2)  $\forall a \in A \forall b, b' \in B \ (a \mapsto b \wedge a \mapsto b' \Rightarrow b = b')$  ( $f$  is well-defined)
- D.3.34 Set of functions from  $A \rightarrow B: B^A$
- D.3.35 Partial function is a relation  $A \rightarrow B$  such that only 2nd property holds
- D.3.36 Image:  $S \subseteq A, f(S) = \{f(a) \mid a \in S\}$  ( $A \rightarrow B$ )
- D.3.37 Image/range:  $f(A) \subseteq B, \text{im}(f)$  ( $A \rightarrow B$ )
- D.3.38 Preimage:  $T \subseteq B, f^{-1}(T)$  set of values that map onto  $T: f^{-1}(T) = \{a \in A \mid f(a) \in T\}$
- D.3.39 A function  $f: A \rightarrow B$  is called:
  - 1) injective: if  $a \neq b \Rightarrow f(a) \neq f(b)$
  - 2) surjective: if  $f(A) = B$ , then  $\forall b \in B \ \exists a \in A$ , such that  $b = f(a)$
  - 3) bijective: if 1) and 2)

- D.3.40 Inverse of bijective function  $f^{-1}: B \rightarrow A$
- D.3.41 Composition of a function  $f: A \rightarrow B, g: B \rightarrow C$ :  $g \circ f = g \circ f = g(f(a))$
- L.3.44 Function composition is associative:  $(h \circ g) \circ f = h \circ (g \circ f) \rightsquigarrow L.3.7$
- Ex Prove that for  $f: A \rightarrow A$  exists a  $g$  such that  $g \circ f = \text{id}$   $\Leftrightarrow f$  is injective  $\Rightarrow$  Consider  $f(a) = f(b)$ :

Zero divides of a ring:  
GF[3]  $x^2 + 2$   
1. Find roots of poly  $x^2 + 2$   
 $p(0) = 0^2 + 2 = 2 \neq 0$   
 $p(1) = 1^2 + 2 = 3 = 0$   
 $p(2) = 2^2 + 2 = 6 = 0$   
3. Multiples (divisors from GF[3]) give all zero divisors  
6. Doublecheck  $(x+1)(x+2) = x^2 + 3x + 2 = x^2 + 2$   
Ex Prove that every  $a \in D \setminus \{0\}$  is a unit. Define  $f_a: D \rightarrow D, x \mapsto ax$ 

- injective: Assume  $x, y \in D, x \neq y$  and  $f(x) = f(y)$   
 $0 = f_a(y) - f_a(x) = ay - ax = a(y - x) = a(y - x)$   
Since  $a \neq 0, y - x$  has to be  $0 \Rightarrow x = y$  (or  $a$  is zero divisor)
- surjective: If  $f_a$  was not injective we would have  $y \notin \text{im}(f_a)$  for some  $y \in D$ . Which for finite  $D$  implies  $\text{im}(f_a) < |D|$   
This is a contradiction to the fact that  $f_a$  is injective, therefore is  $f_a$  surjective

The inverse of  $a$  is  $f_a^{-1}(1)$  and therefore  $a$  is unit  
Ex Prove that:  $F: \mathbb{N}^n \rightarrow \mathbb{N}^n: f \mapsto f \circ f$  is not surjective.  
Hint: use  $h(0) = 1, h(1) = 0$  and  $h(x) = x$  for  $x \geq 2$   
Assume that  $F$  is surjective, therefore we have a  $g$  s.t.  $g \circ g = h$ 

- Case:  $g(0) = 0 \Rightarrow (g \circ g)(0) = g(0) = 0$
- Case:  $g(1) = 1 \Rightarrow (g \circ g)(1) = g(1) = 1$
- Case:  $g(0) = 1, g(1) = 0 \Rightarrow (g \circ g)(0) = g(1) = 0$
- Case:  $g(0) = x, g(1) = y$  with  $x, y \geq 2$   
 $\Rightarrow (g \circ g)(0) = g(y) = 1$  since  $h(0) = 1$ , this contradicts  $h(x) = x$

Countability

- D.3.42 (i) Two sets  $A, B$  are equinumerous if a bijection exists  $A \rightarrow B: A \sim B$   
(ii)  $A$  dominates  $B$ , if  $A \cap C, C \subseteq B$  or injection exists  $A \rightarrow B: A \preceq B$   
(iii)  $A$  countable if  $A \preceq \mathbb{N}$ , else uncountable
- L.3.45 (i) relation  $\preceq$  is transitive (ii)  $A \subseteq B \Rightarrow A \preceq B$  (i)  $\sim$  is equiv. rel.
- T.3.46  $A \preceq B \wedge B \preceq A \Rightarrow A \sim B$
- T.3.47 Set  $A$  is countable  $\Leftrightarrow A$  is finite or  $A \sim \mathbb{N}$   
Cantors diagonalization argument: def  $d_{ij}$ :  $j$ -th digit of  $i$ -th sequence  
 $f(i) = d_{i0}d_{i1}d_{i2}...$ , further  $a_{ij} = a_{ji} + 1: \beta = d_{100}d_{101}d_{102}...$   $\Rightarrow$  not listed
- Functions - countability - Number Theory - Division - Primes - Congruence and modular arithmetic - multiplicative inverse - CRT - Diff-Hellmann - Algebra - Monoid / Groups

Countability

- T.3.18  $\{0, 1\}^*$  is countable, finite binary sequence: Proof:  $\{0, 1\}^* \rightarrow \mathbb{N}$  (bijection),  $f(a) = \text{dec}(11a)$
- T.3.19  $\mathbb{N} \times \mathbb{N} = \mathbb{N}^2$  is countable, ordered pairs of natural numbers Proof: We know:  
 $\mathbb{N} \sim \{0, 1\}^*, \mathbb{N} \times \mathbb{N} \sim \{0, 1\}^* \times \{0, 1\}^*$ , show:  $\{0, 1\}^* \times \{0, 1\}^* \rightarrow \{0, 1\}^*$  (bijection)  $(a, b) \mapsto 1^{|a|+|b|}ab1^{|a|+|b|}$
- C.3.20 If  $A \subseteq \mathbb{N} \wedge B \subseteq \mathbb{N} \Rightarrow A \times B \subseteq \mathbb{N}$  Proof: Prove:  $A \times B \rightarrow \mathbb{N} \times \mathbb{N}$  (bijection). Follows: T.3.19, L.3.45
- C.3.21  $\mathbb{Q}$  is countable Proof: Represent  $\mathbb{Q}$  as pair  $(m, n), m \in \mathbb{Z}, n \in \mathbb{N} \setminus \{0\}: \mathbb{Z} \preceq \mathbb{N}, C.3.2, L.3.45$
- T.3.22 Let  $A$  and  $A_i$  for  $i \in \mathbb{N}$  be countable sets
  - (i) For any  $n \in \mathbb{N}$ , the set  $A^n$  of  $n$ -tuples over  $A$  is countable
  - (ii) The union  $\bigcup_{i \in \mathbb{N}} A_i$  of a countable list  $A_1, A_2, \dots$  of countable sets is countable
  - (iii) The set  $A^*$  of finite sequences of elements from  $A$  is countable
- D.3.34 Semi infinite binary sequence  $\{0, 1\}^\omega$  equivalent:  $\mathbb{N} \rightarrow \{0, 1\}^\omega$
- T.3.23  $\{0, 1\}^\omega$  is uncountable Proof: Cantors diagonalization argument
- D.3.44 Computable functions:  $f: \mathbb{N} \rightarrow \{0, 1\}$  Program exists which gives output  $f(n)$  for every input  $n \in \mathbb{N}$
- C.3.24 There are uncomputable functions. Example: Halting problem

Number Theory

Division

- T.4.1  $\forall a, d \neq 0 \exists q, r$  (unique) satisfying:  $a = dq + r$  and  $0 \leq r < |d|$   $a, d, q, r = \text{int}$
- D.4.1  $a$  divides  $b$ :  $a|b$  if  $\exists c \ b = ac$ ,  $a = \text{divisor}$ , if  $a \neq 0, c = \text{quotient}$ ,  $b = \text{multiple}$  of  $a$
- D.4.2 Greatest common divisors (gcd): for int  $a, b$  (not both 0) an int  $d$  is gcd of  $a$  and  $b$  if  $d$  divides both  $a$  and  $b$  and if every common divisor of  $a$  and  $b$  divides  $d$ :  $\text{gcd}(a, b) \Leftrightarrow d|a \wedge d|b \wedge \forall c \ (c|a \wedge c|b) \Rightarrow c|d$
- L.4.2 For any int  $m, n, q$ :  $\text{gcd}(m, n - qm) = \text{gcd}(m, n)$  implies:  $\text{gcd}(m, R_m(n)) = \text{gcd}(m, n)$
- D.4.3 Relatively prime: if  $\text{gcd}(a, b) = 1$ , then  $a, b$  are relatively prime
- D.4.4 Ideal generated by  $a$  and  $b$ :  $(a, b) = \{ua + vb \mid u, v \in \mathbb{Z}\}$  or  $(a) = \{ua \mid u \in \mathbb{Z}\}$
- L.4.3 For  $a, b \in \mathbb{Z}$  there exists  $d \in \mathbb{Z}$  such that  $(a, b) = (d)$
- L.4.4 Let  $a, b \in \mathbb{Z}$  (not both 0): if  $(a, b) = (d) \Rightarrow \text{gcd}(a, b) = d$
- C.4.5 For  $a, b \in \mathbb{Z}$  (not both 0), there exists  $u, v \in \mathbb{Z}$  such that:  $\text{gcd}(a, b) = ua + vb$
- D.4.5 Least common multiple (lcm):  $L$  of two positive integers  $a, b$  is the common multiple of  $a$  and  $b$ , which divides every common multiple of  $a$  and  $b$ :  $\text{lcm}(a, b) \Leftrightarrow a|L \wedge b|L \wedge \forall m \ (a|m \wedge b|m) \Rightarrow L|m$

Primes

- D.4.6 Int  $p > 1$  is prime if the only positive divisors are  $p$  and 1. Else composite
- T.4.6 Every int  $> 0$  can be written uniquely as the products of primes
- L.4.7 If  $p$  is prime and  $p \mid x_1 x_2 \dots x_n$  ( $x_i = \text{int}$ ) then  $p \mid x_i$  for some  $i \in \{1, \dots, n\}$
- Note We can write  $a = \prod p_i^{e_i}$  and  $b = \prod p_i^{f_i} \Rightarrow \text{gcd}(a, b) = \prod p_i^{\min(e_i, f_i)}$   
From that follows:  $\text{gcd}(a, b) = \text{lcm}(a, b) = a \cdot b$  since  $\min(e_i, f_i) + \max(e_i, f_i) = e_i + f_i$

Congruence and modular arithmetic

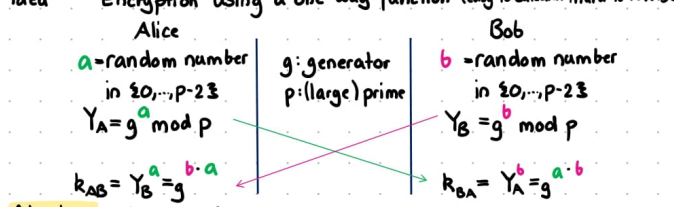
- D.4.8  $a$  is congruent to  $b$  modulo  $m$ :  $a \equiv b \pmod{m} \Leftrightarrow a - b \stackrel{\text{def}}{=} m \mid (a - b)$
- L.4.13 For any  $m \geq 1, \equiv_m$  is an equivalence relation on  $\mathbb{Z}$
- L.4.14  $a \equiv_m b$  and  $c \equiv_m d$  then  $a + c \equiv_m b + d$  and  $ac \equiv_m bd$  for cong. system
- C.4.15  $f(x_1, \dots, x_k)$  is multi-variate polynomial in  $k$  variables: If  $a_i \equiv_m b_i$  then  $f(a_1, \dots, a_k) \equiv_m f(b_1, \dots, b_k)$
- L.4.16 For any  $a, b, m \in \mathbb{Z}$  with  $m \geq 1$ : (i)  $a \equiv_m R_m(a)$  (ii)  $a \equiv_m b \Leftrightarrow R_m(a) = R_m(b)$
- C.4.17  $f(x_1, \dots, x_k)$  is multi-variate polynomial in  $k$  variables and  $m \geq 1$  Then:  
 $R_m(f(a_1, \dots, a_k)) = R_m(f(R_m(a_1), \dots, R_m(a_k)))$   $R_m(a^b) = R_m(R_m(a)^b)$ ,  
 $R_m(a \cdot b) = R_m(R_m(a) \cdot R_m(b))$ ,  $R_m(a + b) = R_m(R_m(a) + R_m(b))$ , ...
- Note if  $\text{gcd}(m, a) = 1$ , then  $R_m(a^b) = R_m(a^{R_m(b)})$ ,  $\forall n = \#$  coprime numbers  $< n$
- Ex Prove that if  $s(a) = s(2a) \Rightarrow 9|a$  ( $s$  = sum of digits)  
 $R_9(a) = R_9(s(a)) = R_9(s(2a)) = R_9(2a) = R_9(2) \cdot R_9(a)$   
 $\Rightarrow R_9(a) = 2 \cdot R_9(a)$   
 $\Rightarrow R_9(a) = 0$   $R_m(a^b) = R_m(a^{R_m(b)})$ ,  $R_{mn}(a) \Rightarrow \text{CRT}(R_m(a), R_n(a))$

- Ex Prove for all  $a, b \in \mathbb{Z}$  such that  $a^2 + b^2 = 0$  it holds:  $a^2 = 0$  and  $b^2 = 0$   
 $0 = R_2(a^2 + b^2) = R_2(R_2(a^2) + R_2(b^2))$  therefore  $R_2(a^2) + R_2(b^2) = 0$
- Ex Prove for all  $a, b, c \in \mathbb{Z} \setminus \{0\}$  if  $a|b$  and  $\text{gcd}(a, b) = 1$  then  $a|c$ :  $\text{gcd}(a, b) = 1 \Rightarrow ua + vb = 1$  for some  $u, v \in \mathbb{Z}$   
 $a|b \Rightarrow bc = ad, c = 1c = (ua + vb)c = uac + vbc = uac + vad = (u + v)a = a|c$
- Ex Prove for all  $n \geq 2$  if  $3 \nmid n$ , then  $n^2 + 2^n$  is not prime  
Case:  $n = 2k$  (even),  $(2k)^2 + 2^n = 4 \cdot k^2 + 2 \cdot 2^{n-1} \Rightarrow 2 \mid (n^2 + 2^n)$   
Case:  $n$  is odd,  $R_3(n^2) = R_3(R_3(n) \cdot R_3(n)) = R_3(1 + 2^{R_3(n)}) = R_3(2 + 1) = 0 \Rightarrow 3 \mid (n^2 + 2^n)$

Multiplicative inverse

- L.4.18  $ax \equiv_m 1$  has a unique solution  $x \in \mathbb{Z}_m \Leftrightarrow \text{gcd}(a, m) = 1$
- D.4.9 Multiplicative inverse: solution of L.4.18 denoted:  $x \equiv_m a^{-1}$
- Chinese Remainder Theorem (CRT)
- T.4.19 Let  $m_1, m_2, \dots, m_r$  be pairwise relatively prime and let  $M = \prod_{i=1}^r m_i$   
For every list  $a_1, \dots, a_r$  with  $0 \leq a_i \leq m_i$  for  $i = 1, \dots, r$  has  $x \equiv_m a_i$  a unique solution  $x$ , with  $0 \leq x \leq M$
- Ex  $x \equiv_3 2 \quad 1) M_i = \frac{M}{m_i} \quad 2) M_i M_i^{-1} \equiv_m 1$   
 $x \equiv_4 1 \quad M_1 = 20 \quad N_1 \cdot 20 \equiv_3 \Rightarrow N_1 = 2$   
 $x \equiv_5 4 \quad M_2 = 15 \quad N_2 \cdot 15 \equiv_4 \Rightarrow N_2 = 3$   
 $M = 60 \quad M_3 = 12 \quad N_3 \cdot 12 \equiv_5 \Rightarrow N_3 = 3$   
 $3) \sum_{i=1}^r a_i \cdot M_i \cdot M_i^{-1} = 2 \cdot 20 \cdot 2 + 1 \cdot 15 \cdot 3 + 4 \cdot 12 \cdot 3 = 23$   
If  $\text{gcd}(m_i, m_j) \neq 1$  for  $i \neq j \Rightarrow$  decompose: i.e.  
 $x \equiv_{12} 8, x \equiv_{15} 2 \Rightarrow x \equiv_{32} 2, x \equiv_3 0$  and  $x \equiv_{32} 2, x \equiv_5 2$   
must be equal, else no solution

Diffie-Hellman



Algebra

- $ab \stackrel{\text{ord}(g)}{=} 1$
- D.5.1 Operation on a set  $S$  is a function  $S^n \rightarrow S$ , where  $n \geq 0$  is arity
- D.5.2 Algebra is a pair  $\langle S; \mathcal{R} \rangle$  with a set  $S$ , called carrier and  $\mathcal{R}$  = list of operations on  $S$
- Monoids and Groups
- D.5.3 left/right neutral element is an element  $e \in S$  such that  $\forall a \in S \ e * a = a / a * e = a$ . If both then simply neutral element
- L.5.1 If  $\langle S; \mathcal{R} \rangle$  has both left/right NE then they're equal.  $\langle S; \mathcal{R} \rangle$  has max 1 NE
- D.5.4 Associative binary operation  $*$  on a set if  $a * (b * c) = (a * b) * c$
- D.5.5 Monoid is an algebra  $\langle M; *, e \rangle$ ,  $*$  = associative,  $e$  = NE
- D.5.6 left/right inverse of an element  $a \in S$ , is a  $b \in S$  such that  $b * a = e / a * b = e$ . If both then it is simply called inverse of  $a$
- D.5.7 Group is an algebra  $\langle G; *, ^{-1}, e \rangle$  satisfying the axioms:
  - g1  $*$  is associative
  - g2  $e$  is NE,  $a * e = e * a = a$
  - g3  $\forall a \in G \exists a^{-1} \ a * a^{-1} = a^{-1} * a = e$
- D.5.8 Commutative/abelian group/monoid if:  $a * b = b * a, a, b \in G$
- L.5.2 If monoid has both left/right inv then they're equal. Monoid has at most 1. inverse

**L.5.3** For groups holds:

- (i)  $(\hat{a})^n = a$   
Proof: start:  $(\hat{a})^n = e$ ; apply:  $x \hat{a}, g_2, x a, g_4, g_2, g_2$
- (ii)  $\hat{a+b} = \hat{b+a}$   
Proof: start:  $(\hat{a+b}) = (a+b) = e$ ; apply:  $g_3, x \hat{b}, g_2, g_4, g_3, g_2, x \hat{a}, g_4, g_3, g_2$
- (iii)  $a \cdot b = a \cdot c \Rightarrow b = c$   
Proof: start:  $ba = ca$ ; apply:  $x \hat{a}, g_3, g_3$
- (iv)  $b \cdot a = c \cdot a \Rightarrow b = c$   
Proof: start:  $ba = ca$ ; apply:  $x \hat{a}, g_3, g_3$
- (v)  $a \cdot x = b$  has a unique solution, so does  $x \cdot a = b$   
Proof: for  $a \cdot x = b$ : show solution exists, namely  $x = (\hat{a} \cdot b)$ ; insert; apply  $g_4, g_3$ ; assume two  $x$  exists:  $a \cdot x_1 = b$  and  $a \cdot x_2 = b \Rightarrow x_1 = x_2$

**D.5.7** can be simplified to:  $g_2 \Rightarrow g_2^2: a \cdot e = a, g_3 \Rightarrow g_3^2: a \cdot \hat{a} = e$  from this the other sides follow: Proof: start:  $\hat{a} \cdot a = (\hat{a} \cdot a)$  apply:  $(x \cdot e, g_2^2), (e = (\hat{a} \cdot \hat{a}), g_3^2), g_4, g_4, g_3, g_4, g_2^2, g_3^2$

**Structure of groups** order is  $(\mathbb{Z}_m, \mathbb{Z}_n)$

**D.5.9** direct product of  $n$  groups is the algebra  $\langle g_1 x \dots g_n, + \rangle$  where  $+$  is a component wise operation

**L.5.4**  $\langle g_1 x \dots g_n, + \rangle$  is a group in which the NE/INV are component wise

**D.5.10** A function  $\Psi$  from group  $G$  to group  $H$  is a **group homomorphism** if for all  $(a,b) \Psi(a \cdot b) = \Psi(a) \cdot \Psi(b)$ . If  $\Psi$  is bijective it is a **isomorphism**:  $G \cong H$  to prove only (1)  $\Rightarrow$  L.5.5 follows

**L.5.5** A group homomorphism  $\Psi$  satisfies:  $\Psi(e) = e' \cdot \Psi(a) = \Psi(a)$   
Proof: start:  $\Psi(e) = \Psi(e \cdot e)$ ; apply: **D.5.10**,  $\Psi(e), g_3, g_3, g_2$

**Note** When proving that  $f$  is isomorphism one needs to prove:  
•  $f$  is homomorphism •  $f$  is bijective

**D.5.11** A subset  $H \subseteq G$  is **subgroup** if  $H$  is a group, meaning closed under all operations: (1)  $a \cdot b \in H$  (2)  $e \in H$  (3)  $\hat{a} \in H$

**D.5.12** Order of  $a \in G  $ord(a)$  is least  $m \geq 1$  s.t.  $a^m = e$ : if not  $ord(a) = \infty$$

**D.5.13** Order of a finite group  $G$ :  $|G|$

**L.5.6** In a finite group, every element has finite order

**Ex** Prove for any  $a, b \in G$ :  $ord(a \cdot b) = ord(b \cdot a)$ : Lets denote  $n = ord(a)$   
 $(a \cdot b)^n = e \Leftrightarrow (a \cdot b)(a \cdot b) \dots = e \Rightarrow b \cdot (a \cdot b) \dots = b \cdot e = b$   
 $(b \cdot a)(b \cdot a) \dots = b \cdot a \Rightarrow \hat{a} \cdot b \cdot b \cdot a \cdot (b \cdot a) \dots = \hat{a} \cdot b \cdot b \cdot a$   
 $\Leftrightarrow (b \cdot a)^n = e$ , proves  $ord(a \cdot b) \geq ord(b \cdot a)$ , do for both sides

**D.5.14** For  $a \in G$ , the group generated by  $a$ :  $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$

**D.5.15** A group  $G = \langle g \rangle$  is called **cyclic** and  $g$  is called a **generator** of  $G$   
 $\langle g^{-1} \rangle$  is also a generator

**Finding generators**

$\langle \mathbb{Z}_m, \oplus \rangle$  all elements with  $gcd(a, m) = 1$

$\langle \mathbb{Z}_n, \odot \rangle$  calculate order of group; for  $d \mid$  order, check if  $a^d = 1$ , if not  $a = \text{gen}$   
 $\rightarrow$  Check: # generators =  $\varphi(\text{order})$

**T.5.7** A cyclic group of order  $n$  is isomorphic to  $\langle \mathbb{Z}_n, \oplus \rangle$  and therefore commutative. All groups of prime order are comm.

**Note**  $\mathbb{Z}_m \times \mathbb{Z}_n$  is cyclic if  $gcd(m, n) = 1 \mid \langle \mathbb{Z}_m, \oplus \rangle$  is not for cyclic group of order  $ln$

**T.5.8** Lagrange: If  $H \subseteq G \Rightarrow |H|$  divides  $|G|$

**C.5.9** For a finite group  $G$  and  $a \in G$ :  $ord(a)$  divides  $|G|$

**C.5.10** For a finite group  $G$  and  $a \in G$ :  $a^{|G|} = e$

**C.5.11** Every group of prime order is cyclic. Every element, except the neutral element is a generator

**D.5.16** Multiplicative group:  $\mathbb{Z}_m^* = \{a \in \mathbb{Z}_m \mid gcd(a, m) = 1\}$   
 Structure of groups - finding generators - RSA - Rings

**D.5.7** Euler Function:  $\varphi(m) = |\mathbb{Z}_m^*|$  if  $m = \text{prime}$ :  $\mathbb{Z}_p^* = \mathbb{Z}_p \Rightarrow |\mathbb{Z}_p| = p - 1$

**L.5.12** If  $\prod p_i^{e_i}$  is the prime factorization of  $m$ , then  $\varphi(m) = \prod (p_i - 1) p_i^{e_i - 1}$   
 Proof:  $\varphi(p^e) = p^e - p^{e-1} \Rightarrow gcd(a, p) = 1 \Rightarrow gcd(a, p_i^{e_i}) \Rightarrow \text{CRT}$

**T.5.13**  $\langle \mathbb{Z}_m^*, \odot \rangle$  is a group

**C.5.14** For all  $m \geq 2$  and  $gcd(a, m) = 1$ :  $a^{\varphi(m)} \equiv 1$  and for  $p = \text{prime}$ :  $p \nmid a \Rightarrow a^{p-1} \equiv 1$

**T.5.15**  $\mathbb{Z}_m^*$  is cyclic  $\Leftrightarrow m = 2, m = 4, m = p^e$  or  $m = 2p^e$ , where  $p$  is an odd prime and  $e \geq 1$   
 Inverse of  $a$ :  $a^{\varphi(m)-1} = \hat{a}$

**Ex** Claim: for  $gcd(m, n) = 1, \Psi: \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n, x \mapsto (R_m(x), R_n(x))$  is an isomorphism:  
 Computes number of isomorphisms of two groups of the same order. Homomorphism:  $\Psi(x+y) = (R_m(x+y), R_n(x+y)) = (R_m(x) + R_m(y), R_n(x) + R_n(y)) = (R_m(R_m(x) + R_m(y)), R_n(R_n(x) + R_n(y))) = (R_m(x) + R_n(x)) + (R_m(y) + R_n(y)) = \Psi(x) + \Psi(y)$

• We'll show that  $\Psi$  is injective: Assume  $x \neq y$  and  $\Psi(x) = \Psi(y)$ . Followed by the fact that  $x \cdot y$ :  $a \equiv_m \Psi(x)$  and  $a \equiv_n \Psi(y)$  Given by  $x \cdot y \in m \cdot n$  and  $\Psi(x) \in m, \Psi(y) \in n$  we have by CRT that  $a$  is unique, therefore  $x = y$ . Hence it is injective. Since  $|\mathbb{Z}_{mn}| = |\mathbb{Z}_m \times \mathbb{Z}_n|$  it is also surjective

**Ex** Let  $G$  be a finite, non-empty set and  $\cdot$  a binary operation on  $G$ . Let  $\cdot$  be associative and commutative. Let  $\forall a, b, c \in G: a \cdot b = a \cdot c \Rightarrow b = c$ . Prove that  $G$  is a group

We know  $\forall a \in G \exists n, m \in \mathbb{N} (n < m \wedge a^n = a^m)$ , since  $G$  is finite

1)  $e \in G$ :  $z = m - n \Rightarrow a^z = a^n = a^{(m-n)+n} = a^m = a^n \Rightarrow a^z = e$   
 Show  $a^z = e$  for all  $b \in G$ :  $(a \cdot e) \cdot b = a \cdot (e \cdot b)$   
 $\Rightarrow b = (e \cdot b) = (b \cdot e)$

2)  $\hat{a} \in G$ :  $\forall a \in G a^z = e, e = a^{m-n}$  then  $\hat{a} = a^{m-n-1}$   
 since  $a^{m-n-1} \cdot a = a^{m-n} = e$

**Ex** group Prove that if  $G \subseteq \langle \mathbb{Z}; + \rangle$  then  $G = \mathbb{Z} \cdot d \mid n \in \mathbb{Z}$  for some  $d \in \mathbb{Z}$

Proof by contradiction. Let  $d$  be the smallest element in  $G$ . We assume  $\nexists d' \in \mathbb{Z} \cdot d' \mid n \in \mathbb{Z}$ . If we set  $d' = d$  we have that  $\exists g \in G$  for which  $d \nmid g$ . Let  $g > 0$ , then  $g = k \cdot d + r$  with  $0 < r < d$ . But because  $G$  is closed under  $+$  and  $-$  we have  $r = g - k \cdot d \in G$ . But we assumed  $d$  is the smallest element which is a contradiction. Therefore  $G$  is in the form  $\mathbb{Z} \cdot d \mid n \in \mathbb{Z}$

**RSA**

**T.5.16** Let  $G$  be a finite group and  $e \in \mathbb{Z}$  with  $gcd(e, |G|) = 1$ . Then  $x \mapsto x^e$  is a bijection and  $x$  is the  $e$ -th root of  $y \in G, y = x^e$   
 $x = y^d$  where  $d$  is the multiplicative inverse of  $e \bmod |G|, e \cdot d \equiv 1 \bmod |G|$

Alice Bob

$p, q$  large primes  
 $n = p \cdot q$   
 $f = (p-1)(q-1) = \varphi(n)$   
 Select  $e \in \mathbb{Z}_n^*$   
 $d \equiv e^{-1} \Rightarrow e \cdot d \equiv 1$   
 $m = R_n(y^d)$

insecure channel

$n, e$   $m = \text{message}$

$y = R_n(m^e)$

**Ex** Prove that for all  $m \in \mathbb{Z}_n$ , we have  $m^{de} \equiv_p m$  where  $n = p \cdot q$  and  $de \equiv_{\varphi(n)} 1$ :  $de - 1 = (p-1)(q-1) \cdot k$ ;  $de = (p-1)(q-1) \cdot k + 1$   
 case 1:  $m = k \cdot p \Rightarrow m^{de} \equiv_p 0 \equiv_p m$ ; Case 2:  $m \neq k \cdot p$ :  $m^{(p-1)(q-1) \cdot k + 1} \equiv_p m$   
 $m = m^{(p-1)(q-1) \cdot k} \cdot m \equiv_p 1 \cdot m$  by **C.5.14**

**Ex** Prove that if  $m^{de} \equiv_p m$  and  $m^{de} \equiv_q m$  then  $m^{de} \equiv_{p \cdot q} m$   
 Define  $x \equiv_p m$ :  $m^{de}$  and  $m$  are two solutions, by CRT, all solutions are congruent modulo  $p \cdot q = n$ , hence  $m^{de} \equiv_n m$

**Rings**

**D.5.18** Ring is an algebra  $\langle R; +, -, \cdot, 1 \rangle$  for which

- (i)  $\langle R; +, 0 \rangle$  is a commutative group
- (ii)  $\langle R; \cdot, 1 \rangle$  is a monoid
- (iii)  $a(b+c) = ab+ac$  and  $(b+c)a = ba+ca$

Ring is commutative if  $\cdot$  is commutative

**of fields:**  
 - find root of poly  
 - get multiple of root  
 Find  $n(b)$  s.t. field has  $n$  elements  
 - find deg.  $d \Rightarrow$  L.5.34  
 $\rightarrow$  choose irr. poly from list

**L.5.17** For any ring and for any  $a, b \in R$  we have

- (i)  $0a = a0 = 0$
- (ii)  $(-a)b = -(ab)$
- (iii)  $(-a) \cdot (-b) = ab$
- (iv) if  $R$  is non-trivial  $\Rightarrow 1 \neq 0$
- (v)  $(-a)b = 0 \wedge (-a)b = a0 \wedge (-a)b = a(b \cdot (-1)) = (-a)b$

**D.5.19** Characteristic of a ring: order of 1 in the additive group. For infinite groups it's defined to be 0

**D.5.20** Unit is an element  $u$  of a ring  $R$  such that  $u$  is invertible  $uv = vu = 1$  for some  $v \in R$ . Set of units is denoted by  $R^*$

**L.5.18** For a ring  $R, R^*$  is a multiplicative group unit  $\neq$  zero divisor  
 Find units: all elements s.t.  $gcd(a, m) = 1$

**D.5.21** a divides  $b$ ,  $a \mid b$  if  $\exists c \in R$  such that  $b = ac \quad \forall a \in R \exists 1 \exists 0$  a.o.

**L.5.19** (i) if  $a \mid b$  and  $b \mid c$  then  $a \mid c$ ,  $\mid$  is transitive  
 (ii) if  $a \mid b$  then  $a \mid b \cdot c \quad \forall c \in R$   
 (iii) if  $a \mid b$  and  $a \mid c$  then  $a \mid (b+c)$

**D.5.22** gcd for rings  $gcd(a, b) \nmid a \wedge a \mid b \wedge \forall c ((c \mid a \wedge c \mid b) \Rightarrow c \mid d)$

**D.5.23** zerodivisor is an element  $a \neq 0$  which gives with  $b \neq 0: ab = 0$ .  
 Find zerodivisor:  $\forall a \in \mathbb{Z}_m$  such that  $gcd(a, m) \neq 1$

**Note**  $\langle \mathbb{Z}_n; + \rangle$  is isomorphic to  $\langle \mathbb{Z}_p; + \rangle \times \langle \mathbb{Z}_q; + \rangle \Leftrightarrow n = p \cdot q$  and  $gcd(p, q) = 1$ , follows from CRT

**D.5.24** Integral domain is a non-trivial commutative ring without zerodivisors:  $\forall a \forall b (ab = 0 \Rightarrow a = 0 \vee b = 0)$

**note**  $\mathbb{Z}_m$  can only be Integral domain if  $m$  is prime

**L.5.20** In an integral domain  $a \mid b \Rightarrow c$  is unique s.t.  $b = ac$ .  $c$  is quotient

**D.5.25** Polynomial  $a(x)$  over  $R$  is  $a(x) = \sum a_i x^i$  for some  $d \geq 0$  and  $a \in R$ .  $deg(a(x))$  is largest  $i$  for  $a_i \neq 0$   
 if  $\forall i a_i = 0 \Rightarrow deg(a(x)) = -\infty$ .  $\mathbb{R}[x]$  denotes the set of polynomials over  $R$

**T.5.21** For any commutative ring  $R, R[x]$  is commutative ring

**L.5.22** (i) if  $D$  is integral domain, then so is  $D[x]$   
 (ii) The units of  $D[x]$  are the constant polynomials that are units in  $D$ :  $D[x]^* = D^*$

**Ex** Let  $\langle R; +, -, \cdot, 1 \rangle$  be any ring such that  $a^2 = a$  prove  $a + a = 0$   
 prove  $a + a = 0$ :  $(a + a) = (a + a)(a + a)$   
 $= aa + aa + aa + aa$   
 $= a + a + a + a$   
 $= a + a$   
 $\Rightarrow 0 = a + a$

prove commutativity:  
 $a + b + (-a) + (-b) = ab + ba$   
 $0 = ab + ba$   
 $-(ab) = ba \Rightarrow ab = ba$

Ex List all elements  $R \setminus R^*$  with  $R = \mathbb{Z}_7[x]_{x^2+x+1}$   
 We have to remove all units:  $x^2+x+1 = (x+3)(x+5)$   
 all elements which are a linear combination of these factors are units. Therefore  $R \setminus R^*$  all multiples of  $(x+3)$  and  $(x+5)$

Ex Let  $R$  be a ring. Prove that if  $1-ab$  has a multiplicative inverse  $c$ , then  $1-ba$  has the multiplicative inverse  $1+bca$ : Assume:  $(1-ab) \cdot c = 1$

Show  $\mathbb{Z}_n[x]$  is a field (1.2.23, if  $n$  prime)  
 1.  $\mathbb{Z}_n$  field T.5.23, if  $n$  prime  
 2.  $\mathbb{Z}_n[x]$  is ring L.5.35  
 3. If  $u(x)$  irr, then from T.5.37  
 $\mathbb{Z}_n[x]$  is field  
 Show irr  $\Rightarrow$  C.5.30, if no roots  $\Rightarrow$  input all  $x \in \mathbb{Z}_n$

D.5.26 Field is a nontrivial commutative ring  $F$  in which every nonzero element is a unit:  $F^* = F \setminus \{0\}$   
 $\mathbb{Z}_p$  is a field  $\Leftrightarrow p$  is prime  $\mathbb{Z}_p = GF(p)$   
 A field is an integral domain

Proof: D.5.26, D.5.24  $\Rightarrow$  suffices to show that in any comm. ring a unit  $u \in R$  is not a zero-divisor  
 Assume  $uv=0$ :  $v = 1v = u^{-1}uv = u^{-1} \cdot 0 = 0$

D.5.27 Monic polynomial  $a(x) \in F[x]$  if leading coefficient is 1  
 D.5.28 Irreducible polynomials  $a(x) \in F[x]$  with degree  $\geq 1$  if it's divisible only by a constant poly. or const. mult. of  $a(x)$

D.5.29 gcd of  $a(x)$  and  $b(x)$  is a monic polynomial with the largest degree such that  $g(x) | a(x)$  and  $g(x) | b(x)$   
 T.5.25 For any  $a(x)$  and  $b(x) \neq 0$  in  $F[x]$ , there exists a unique monic  $q(x)$  and a unique  $r(x)$  such that:  
 $a(x) = q(x) \cdot b(x) + r(x)$  and  $\deg(b(x)) \geq \deg(r(x))$

D.5.30 Associates are two elements,  $a, b$  in an integral domain if  $a = ub$  for some unit  $u$ . Denoted as  $a \sim b$

D.5.31 In an integral domain, a non-unit  $p \in D \setminus \{0\}$  is irreducible if  $p=ab$ , then either  $a$  or  $b$  is a unit

L.5.26  $a \sim b \Leftrightarrow alb \wedge bla$

D.5.32 Euclidian domain is an integral domain  $D$  together with a degree-function  $d: D \setminus \{0\} \rightarrow \mathbb{N}$  such that:  
 (i)  $\forall a, b \neq 0 \in D \exists q, r$  such that  $a = bq + r$  and  $d(r) < d(b)$  or  $r = 0$   
 (ii)  $\forall a \neq 0, b \neq 0 \in D, d(a) \leq d(ab)$

T.5.27 In an euclidian domain every element can be factored uniquely (up to taking associates) into irreducible elements

D.5.33 Root is an element  $d \in R$  for which  $a(d)=0$  with  $a(x) \in R[x]$

L.5.28 Polynomial evaluation is compatible with ring operations:  
 • if  $c(x) = a(x) + b(x) \Rightarrow c(d) = a(d) + b(d)$   
 • if  $c(x) = a(x) \cdot b(x) \Rightarrow c(d) = a(d) \cdot b(d)$

L.5.29 For a field  $F$ ,  $h \in F$  is a root of  $a(x) \Leftrightarrow (x-a) | a(x)$

C.5.30 A polynomial  $a(x)$  of degree 2 or 3 over a field  $F$  is irreducible  $\Leftrightarrow a(x)$  has no roots

T.5.30 For a field  $F$  a non-zero polynomial  $a(x) \in F[x]$  of degree  $d$  has at most  $d$  roots

L.5.32 A polynomial  $a(x) \in F[x]$  of degree at most  $d$  is uniquely determined by any  $(d+1)$  values, i.e by  $a(d_1), \dots, a(d_{d+1})$  for any distinct  $d_1, \dots, d_{d+1} \in F$   
 Note Lagrange's interpolation formula:  

$$a(x) = \sum_{i=1}^{d+1} \beta_i u_i(x)$$
 where  $u_i = \frac{(x-d_1) \dots (x-d_{i-1})(x-d_{i+1}) \dots (x-d_{d+1})}{(d_i-d_1) \dots (d_i-d_{i-1})(d_i-d_{i+1}) \dots (d_i-d_{d+1})}$

gcd of two polynomials  
 Ex Find  $\gcd(x^3+x+2, x^2+x+1)$   
 Apply euclids algorithm: divide by smaller polynomial, keep remainder  
 $\gcd(x^3+x+2, x^2+x+1) = \gcd(x^2+x+1, x+3) = \gcd(x+3, 0) = x+3$

Ex Find the multiplicative inverse of  $x \in \mathbb{Z}_5[x]_{x^2+1}$   
 $(x)(ax+b) = (a)x^2 + (b)x + (0) \cdot 1 \Rightarrow a=k, b=0 \Rightarrow \hat{x} = 4x$   
 $k(x^2+1)+1 = (k)x^2 + (0)x + (k+1) \cdot 1 \Rightarrow k+1=0, k=4$

Irreducibility of  $a(x)$   
 • deg 1 always irreducible  
 • deg 2/3 irreducible if  $a(x)$  has no roots C.5.30  
 • deg 4 irreducible if  $a(x)$  has no root or factor deg 2  
 • deg 5 irreducible if  $a(x)$  has no root or factor deg 2/3

Irreducible polynomial e.g. "1234"  $= 1 \cdot x^3 + 2 \cdot x^2 + 3 \cdot x + 4$ , "12"  $= 1 \cdot x + 2$ , "1"  $= 1$

|            |         |         |         |         |         |         |         |         |        |
|------------|---------|---------|---------|---------|---------|---------|---------|---------|--------|
| $GF(2)[x]$ | 10      | 11      | 111     | 1011    | 1101    | 10011   | 11001   | 11111   | 100101 |
|            | 101001  | 101111  | 110111  | 111011  | 111011  | 111011  | 111101  | 1000011 |        |
|            | 1001001 | 1010111 | 1011011 | 1100001 | 1100001 | 1100001 | 1100001 | 1001101 |        |
|            | 1110011 | 1110101 |         |         |         |         |         |         |        |

|            |       |       |       |       |       |       |       |       |      |      |
|------------|-------|-------|-------|-------|-------|-------|-------|-------|------|------|
| $GF(3)[x]$ | 10    | 11    | 12    | 101   | 112   | 122   | 1021  | 1022  | 1102 | 1112 |
|            | 1121  | 1201  | 1211  | 1222  | 10042 | 10022 | 10102 | 10111 |      |      |
|            | 10121 | 10202 | 11002 | 11021 | 11100 | 11111 | 11122 | 11222 |      |      |
|            | 12002 | 12011 | 12112 | 12121 | 12212 |       |       |       |      |      |

|            |       |      |      |      |      |      |      |      |      |      |      |
|------------|-------|------|------|------|------|------|------|------|------|------|------|
| $GF(6)[x]$ | 10    | 11   | 12   | 13   | 112  | 113  | 121  | 122  | 131  | 133  | 1002 |
|            | 1003  | 1011 | 1021 | 1031 | 1101 | 1112 | 1113 | 1113 | 1113 | 1123 |      |
|            | 11132 | 1201 | 1213 | 1222 | 1232 | 1233 | 1301 | 1312 |      |      |      |
|            | 1322  | 1323 | 1333 |      |      |      |      |      |      |      |      |

|            |      |      |      |      |      |      |      |      |      |     |     |     |
|------------|------|------|------|------|------|------|------|------|------|-----|-----|-----|
| $GF(3)[x]$ | 10   | 11   | 12   | 13   | 14   | 102  | 103  | 111  | 112  | 123 | 124 | 133 |
|            | 134  | 141  | 142  | 1011 | 1014 | 1021 | 1024 | 1032 | 1033 |     |     |     |
|            | 1042 | 1043 | 1101 | 1102 | 1113 | 1114 | 1131 | 1134 | 1134 |     |     |     |
|            | 1141 | 1143 | 1201 | 1203 | 1213 | 1214 | 1222 | 1223 |      |     |     |     |
|            | 1242 | 1244 | 1302 | 1304 | 1311 | 1312 | 1322 | 1323 |      |     |     |     |
|            | 1341 | 1343 | 1403 | 1404 | 1411 | 1412 | 1431 | 1434 |      |     |     |     |
|            | 1442 | 1444 |      |      |      |      |      |      |      |     |     |     |

|            |     |     |     |     |     |     |     |     |     |     |     |     |
|------------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| $GF(7)[x]$ | 10  | 11  | 12  | 13  | 14  | 15  | 16  | 101 | 102 | 104 | 113 | 114 |
|            | 116 | 122 | 123 | 125 | 131 | 135 | 136 | 141 | 145 | 146 | 152 | 153 |
|            | 155 | 163 | 166 |     |     |     |     |     |     |     |     |     |

Ex Solve  $y^2 + (x^2+1) \cdot y + (x^2+x+1) = 0$  for  $y \in A$   
 We have to find the root of the polynomial by inserting elements of  $A$  into the polynomial. One found we can divide by  $(y-r)$  to get  $(y-r')$  where  $r'$  is the second root  
 Algebras - Applications

Finite Fields  
 D.5.35 Let  $m(x)$  be a polynomial of deg  $d$  over  $F$ . Then  $|F[x]_m(x)| = \sum_{a(x) \in F[x]} \deg(a(x)) < d$   
 L.5.34 Let  $F$  be a finite field with  $q$ -elements and let  $m(x)$  be of degree  $d$  over  $F$ . Then  $|F[x]_m(x)| = q^d$   
 L.5.35  $F[x]_m(x)$  is a ring with respect to addition and multiplication modulo  $m(x)$   
 L.5.36  $F[x]_m(x) = \sum_{a(x) \in F[x]} \deg(a(x)) | \gcd(a(x), m(x)) = 1$   
 T.5.37 The ring  $F[x]_m(x)$  is a field  $\Leftrightarrow m(x)$  is irreducible  
 T.5.38  $|GF(q)| = q-1$  for  $q=p^e$ ,  $p$  prime,  $e \geq 1$   
 T.5.39 There exists a finite field with  $q$  elements  $\Leftrightarrow q$  is power of prime. Further, any two fields with the same size  $q$  are isomorphic

Note  $F$  is a field  $\Rightarrow F[x]$  can't be a field  
 Proof: At least one element in  $F[x]$  has no inverse given at least two elements we have  $0, 1 \in F$  and  $0 \neq 1$   
 Multiplying two polynomials of degree  $d, d'$  which will yield a polynomial of degree  $d+d' \geq d$  as  $a_d \cdot b_{d'} \neq 0$  (no zero divisor)  
 Multiplication only increases the degree it follows that a polynomial with  $d \geq 1$  does not have an inverse

Constructing finite fields with  $p^d$  elements  
 • pick  $GF(p)$   
 • pick  $m(x)$  of degree  $d$  in  $GF(p)$  that it is irreducible  $\Rightarrow GF(p)[x]_m(x)$

| Examples of algebras |                                                                      | cyclic, not commutative                      |                                                               |
|----------------------|----------------------------------------------------------------------|----------------------------------------------|---------------------------------------------------------------|
| monoid               | $\langle \mathbb{R}^n, +, 0 \rangle$                                 | $\langle \mathbb{N}^n, +, 0 \rangle$         | $\langle A^n, \cdot, id \rangle$                              |
| fin. monoid          | $\langle \mathbb{Z}_m, +, 0 \rangle$                                 | $\langle \mathbb{Z}_m, \cdot, 1 \rangle$     |                                                               |
| group                | $\langle \mathbb{R}, +, -, 0 \rangle$                                | $\langle \mathbb{N}, +, -, 0 \rangle$        | $\langle \mathbb{R} \setminus \{0\}, \cdot, ^{-1}, 1 \rangle$ |
| fin group            | $\langle \mathbb{Z}_m, +, 0 \rangle$                                 | $\langle \mathbb{Z}_p, \cdot, 1 \rangle$     |                                                               |
| ring                 | $\langle \mathbb{R}, +, \cdot, 0, 1 \rangle$                         | $\langle \mathbb{N}, +, \cdot, 0, 1 \rangle$ | $\mathbb{Z}_{prime}, \mathbb{Z}, \mathbb{Q}, \mathbb{C}$      |
| fin ring             | $\langle \mathbb{Z}_m, +, \cdot, 0, 1 \rangle$                       |                                              |                                                               |
| integral domain      | $\mathbb{Z}_{prime}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ | inverse only for +                           |                                                               |
| fields               | $\mathbb{Q}, \mathbb{R}, \mathbb{C}$                                 | inverse for + and $\cdot$                    |                                                               |
| fin fields           | $GF(x), \mathbb{Z}_{prime}, \mathbb{Z}_{prime}[x]_m(x)$              | $m(x)$ - irreducible                         |                                                               |

Ex Let  $F$  be a finite field, prove that there exists  $f(x) \in F[x]$  which has no roots  
 1) Let  $g(x) = \prod (x-a) \Rightarrow g(d)=0$  for all  $d \in F$   
 2) Let  $f(x) = g(x)^{def} + 1$ , since  $\forall d \in F g(d)=0$  it follows that  $\forall h \in F f(h)=1$

Application: Error correcting code (ECC)  
 D.5.36  $(n, k)$ -encoding function maps  $A^k$  to  $A^n$ , where  $n > k$ , the result is called a **codeword**  
 D.5.37  $(n, k)$ -ECC over  $A$  with  $|A|=q$  is a subset of  $A^n$  with cardinality  $q^k$   
 D.5.38 Hamming distance: number of positions in which two strings over  $A$  differ

Ex Compute all subgroups of the group  $\langle \mathbb{Z}_4, + \rangle$   $\mathbb{Z}_4 = \{0, 1, 2, 3\}$   
 we have by lagrange T.5.8 that  $|\text{subgroups}| \mid |\mathbb{Z}_4|$   
 $\Rightarrow x \mid 4 \quad x = 1, 2, 4 \Rightarrow \{0\}, \{0, 2\}, \{0, 1, 2, 3\}$   
 Compute amount of subgroups of  $\langle \mathbb{Z}_{60}, + \rangle$ :  $6 = 2^1 \cdot 3^1 \cdot 5^1$   
 Since  $|\mathbb{H}| \mid |\mathbb{G}| \Rightarrow$  exponent combination:  $\{0, 1, 2\}$  for 2,  $\{0, 1, 3\}$  for 3...  
 $\{0, 1\}$  for 5  $\Rightarrow 3 \cdot 2 \cdot 2 = 12$   
 Show that:  $11 \mid 2^{2016} + 3^{2016} - 1$

Ex  $R_n(2^{2016} + 3^{2016} - 1) = R_n(R_n(2^{2016}) + R_n(3^{2016}) + R_n(-1))$   
 $= R_n(R_n(2^{2016 \cdot 10 + 6}) + R_n(3^{5 \cdot 403 + 1}) + R_n(10))$   
 $= R_n(R_n(2^{20160} \cdot 2^6) + R_n(3^{2015} + 3) + R_n(10)) \dots$

Inverse mod b (a=b\*c)

| $\varphi$ | 0  | 1   | 2  | 3   | 4  | 5  | 6  | 7   | 8   | 9   |
|-----------|----|-----|----|-----|----|----|----|-----|-----|-----|
| 0         | x  | 1   | 1  | 2   | 2  | 4  | 2  | 6   | 4   | 6   |
| 10        | 4  | 10  | 4  | 12  | 6  | 8  | 8  | 16  | 6   | 18  |
| 20        | 8  | 12  | 10 | 22  | 8  | 20 | 12 | 18  | 12  | 28  |
| 30        | 8  | 30  | 16 | 20  | 16 | 24 | 12 | 36  | 18  | 24  |
| 40        | 16 | 40  | 12 | 42  | 20 | 24 | 22 | 46  | 16  | 42  |
| 50        | 20 | 32  | 24 | 52  | 18 | 40 | 24 | 36  | 28  | 58  |
| 60        | 16 | 60  | 30 | 36  | 32 | 48 | 20 | 66  | 32  | 44  |
| 70        | 24 | 70  | 24 | 72  | 36 | 40 | 36 | 60  | 24  | 78  |
| 80        | 32 | 54  | 40 | 82  | 24 | 64 | 42 | 56  | 40  | 88  |
| 90        | 24 | 72  | 44 | 60  | 46 | 72 | 32 | 96  | 42  | 60  |
| 100       | 40 | 100 | 32 | 102 | 48 | 48 | 52 | 106 | 306 | 108 |

110 - 209

| $\varphi$ | 0  | 1   | 2   | 3   | 4   | 5   | 6   | 7   | 8   | 9   |
|-----------|----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| 10        | 40 | 12  | 48  | 144 | 36  | 84  | 56  | 72  | 58  | 36  |
| 20        | 32 | 140 | 60  | 160 | 100 | 36  | 108 | 64  | 96  | 96  |
| 30        | 48 | 180 | 80  | 196 | 172 | 64  | 136 | 144 | 108 | 148 |
| 40        | 88 | 32  | 170 | 120 | 148 | 144 | 172 | 84  | 172 | 148 |
| 50        | 40 | 180 | 120 | 184 | 60  | 100 | 148 | 184 | 178 | 108 |
| 60        | 64 | 132 | 54  | 164 | 80  | 162 | 164 | 144 | 148 | 156 |
| 70        | 64 | 108 | 84  | 172 | 56  | 120 | 160 | 144 | 148 | 178 |
| 80        | 88 | 180 | 172 | 120 | 148 | 144 | 172 | 84  | 172 | 148 |
| 90        | 12 | 180 | 64  | 182 | 36  | 84  | 156 | 60  | 188 | 188 |
| 100       | 80 | 132 | 100 | 108 | 64  | 160 | 102 | 132 | 56  | 180 |
| 110       | 48 | 240 | 104 | 104 | 104 | 168 | 172 | 180 | 108 | 144 |

How many zero divisor has the ring  $\mathbb{Z}_{30}$ :  
 $30 = 2 \cdot 3 \cdot 5$ ,  $|\mathbb{Z}_{30}| = \varphi(30) = (2-1) \cdot (3-1) \cdot (5-1) = 8$   
 for:  $30 - 8 - 1 = 21$  Since:  $30 = 2^1 \cdot 3^1 \cdot 5^1$  L.5.12

Cardinality  
 $|\mathbb{Z}_n| = n$ ,  $|\mathbb{Z}_n^*| = \varphi(n)$ ,  $|\text{GF}(n)| = n$   
 $|\text{GF}(n)^*| = n-1$  (iff n is power of prime)  
 $|\text{F}[x]_m(x)| = |\text{F}[x]|^{\deg(m(x))}$   
 $|\text{F}[x]_m(x)| = \begin{cases} m(x) & \text{irreducible} \\ |\text{F}[x]_m(x)| - 1 & \text{else: } |\text{F}[x]_m(x)| - 1 \text{ - shared factors} \end{cases}$

Inverse - Cardinality - elements of multiplicative group

|            | NE  | ass | com | a <sup>-1</sup> | NE     | a   | s    | com | a <sup>-1</sup> | dist      |
|------------|-----|-----|-----|-----------------|--------|-----|------|-----|-----------------|-----------|
| monoids    | 0   | ✓   |     |                 |        |     |      |     |                 | Def. 5.5  |
| group      | g2  | g1  |     | g3              |        |     |      |     |                 | Def. 5.7  |
| com. group | g2  | g1  | ✓   | g3              |        |     |      |     |                 | Def. 5.8  |
| ring       | (i) | (i) | (i) | (i)             | 1 (ii) | (i) |      |     | (iii)           | Def. 5.18 |
| com ring   |     |     |     |                 |        |     | (iv) |     |                 | Def. 5.18 |
| field      |     |     |     |                 |        |     |      |     | only units      | Def. 5.26 |

↳ integral domain

Ex Prove that for all sets we have  $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$   
 Let  $(x, y)$  be arbitrary s.t.  $(x, y) \in (A \times B) \cup (C \times D)$   
 $\Rightarrow (x, y) \in (A \times B) \vee (x, y) \in (C \times D)$  (Def U)  
 $\Rightarrow (x \in A \wedge y \in B) \vee (x \in C \wedge y \in D)$  (Def x)  
 $\Rightarrow (x \in A \vee x \in C) \wedge (y \in B \vee y \in D)$  (Dist.)  
 $\Rightarrow (x \in A \vee x \in C) \wedge (y \in B \vee y \in D)$  (FAG)=F  
 $\Rightarrow x \in (A \cup C) \wedge y \in (B \cup D)$  (Def U)  
 $\Rightarrow (x, y) \in (A \cup C) \times (B \cup D)$  (Def x)

Gen Prove uncountability: create injection from  $\mathbb{Z}_0, 13^\infty \rightarrow X$ . Let  $s \in \mathbb{Z}_0, 13^\infty$   
 $X$  can be of the form:  $f(s) = x = \sum (a_i \cdot 13^i) \mid s_i = 13 \vee \sum (x_i) \mid x_i \in \mathbb{N}$   
 where  $s_i$  is the  $i$ -th bit of an arbitrary  $s$   
 Show  $f$  is injective: Let  $s, t \in \mathbb{Z}_0, 13^\infty$  with  $s \neq t$ . Let  $i \in \mathbb{N}$  be the smallest  $i$  such that  $s_i \neq t_i$ . Without loss of generality, assume  $s_i = 1$  and  $t_i = 0$ . It follows  $(i, i+1) \in f(s)$  but  $(i, i+1) \notin f(t)$   
 Thus  $f(s) \neq f(t)$ . Hence  $f$  is injective. Therefore D.3.9.2  $\mathbb{Z}_0, 13^\infty$  stats  $f$  dominates  $\mathbb{Z}_0, 13^\infty$  and D.3.3.4  $\mathbb{Z}_0, 13^\infty$  is uncountable

Fermat's little theorem: if  $p$  is prime and  $a$  is natural number:  
 (i)  $a^p \equiv a \pmod p$  (ii)  $p \nmid a \Rightarrow \exists d: a^d \equiv 1 \pmod p$  (iii)  $a^{p-1} \equiv 1 \pmod p$   
 group with  $n$  elements: cyclic  $\langle \mathbb{Z}_n, \oplus \rangle$ , acyclic:  $\langle \mathbb{Z}_{x_1}, \oplus \rangle \times \langle \mathbb{Z}_{x_2}, \oplus \rangle$  where  $x_1 x_2 = n$

Ex Prove that:  $f$  is surjective  $\Leftrightarrow \exists g$  such that  $fg = \text{id}$   
 $\Rightarrow$ : Let  $g(x) = a$  be defined as  $f(a) = x$ . Such  $g$  exists because  $f$  is surjective  
 In the case we have  $a_1 \neq a_2$ :  $f(a_1) = f(a_2)$ , we assign just one.  
 Then:  $f \circ g(x) = f(g(x)) = f(a) = x \Rightarrow fg = \text{id}$   
 $\Leftarrow$ : Assume  $g$  exists such that:  $fg = \text{id}$ ,  $\forall x f(g(x)) = x$  (1)  
 Let  $y$  be arbitrary. Let  $a \in A$  defined as  $a = g(x)$ . Then  $f(a) = f(g(x)) = x$   
 by def of  $a$  and (1): for any  $y \in A$  exists an  $a \in A$  s.t.  $f(a) = y$   $\Rightarrow f$  is surjective

Ex  $f: \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$  with  $f(x) = (R_m(x), R_n(x))$ . Prove  $f$  is injective  $\Rightarrow \gcd(m, n) = 1$   
 $|\mathbb{Z}_{mn}| = |\mathbb{Z}_m \times \mathbb{Z}_n|$  (for finite)  $\Rightarrow$  if  $f$  is injective  $\Rightarrow f$  is surjective. Hence,  $\exists x \in \mathbb{Z}_{mn}$  s.t.  
 $(R_m(x), R_n(x)) = (0, 1) \in \mathbb{Z}_m \times \mathbb{Z}_n$  (can be arbitrarily chosen):  $R_m(x) = 0, R_n(x) = 1$   
 As  $d \mid m$  and  $d \mid n \Rightarrow R_d(x) = R_d(R_m(x)) = R_d(0) = 0$  and  $R_d(x) = R_d(R_n(x)) = R_d(1) = 0$   
 which is the case for  $d = 1$

Ex Disprove:  $\forall x \exists y F \neq \exists y \forall x F$ : Counterexample:  $F = P(x, y)$ ,  $U^A = \mathbb{N}$ ,  $P^A(x, y) = 1 \Leftrightarrow y = x$   
 $A \models (\forall x \exists y F) = 1$  but  $A \models (\exists y \forall x F) = 0 \Rightarrow A \models (\exists y \forall x F) = 0$

Ex Prove:  $\forall x (F \Rightarrow G) \models (\forall x F) \Rightarrow (\forall x G)$ : Let  $A$  be arbitrary and suitable s.t.  $A \models (\forall x (F \Rightarrow G)) = 1$   
 1)  $A \models (\forall x F) = 0 \Rightarrow A \models (\neg(\forall x F)) = 1 \Rightarrow A \models (\neg(\forall x F) \vee (\forall x G)) = 1$   
 2)  $A \models (\forall x F) \Rightarrow A \models (\forall x G) = 1$  for arbitrary  $u \in U^A$ ,  $A \models (\forall x (F \Rightarrow G)) = 1 \Rightarrow A \models (\neg F \vee G) = 1$   
 $\Rightarrow A \models (\neg F) = 1$  or  $A \models G = 1 \Rightarrow A \models (\neg F \vee G) = 1$  or  $A \models G = 1$

Ex Prove:  $\forall x (F \wedge G) \models (\forall x F) \wedge G$ : Let  $A$  be any interpretation suitable for both  $\forall x (F \wedge G)$  and  $(\forall x F) \wedge G$  such that  $A \models (\forall x (F \wedge G)) = 1$ .  
 $\Rightarrow (\text{sem } V) A \models_{x \mapsto u} (F \wedge G) = 1$  for all  $u \in U^A \Rightarrow (\text{sem } V) A \models_{x \mapsto u} F = 1$  for all  $u \in U^A$   
 and  $A \models_{x \mapsto u} G = 1$  for all  $u \in U^A$ : (1)  $\Rightarrow A \models (\forall x F) = 1$  (3)  
 By sem of  $V$  if  $x$  appears free in  $G$ , so  $x$  does in  $(\forall x F) \wedge G$  and since  $A$  is suitable for  $(\forall x F) \wedge G$  it must assign a value to  $x$ .  
 def  $u^*$ :  $x$  free in  $G \Leftrightarrow u^*$  is value of  $x$  assigned by  $A$ . else  $u^*$  is arbitrary.  
 We have  $A \models_{x \mapsto u^*} G = 1$ , so by (2)  $\Rightarrow A \models G = 1$  (4): (3) and (4)  $\Rightarrow A \models ((\forall x F) \wedge G) = 1$

Ex Prove  $F \models \exists x F$ : Let  $A$  be a suitable interpretation of both  $F$  and  $\exists x F$ . Further let  $A$  be an arbitrary model for  $F$ . Case 1:  $F$  is independent from  $x$ : Then  $A \models F = 1$ ,  
 $\Rightarrow A \models_{x \mapsto u} F = 1$  for all  $u \in U^A$  ( $x$  independent)  
 $\Rightarrow A \models_{x \mapsto u} (F) = 1$  for some  $u \in U^A$  (instantiation)  $\Rightarrow A \models (\exists x F) = 1$   
 case 2:  $F$  is dependant:  $A \models F = 1 \Rightarrow A \models_{x \mapsto u} (F) = 1$   
 $\Rightarrow A \models_{x \mapsto u} (F) = 1$  for some  $u \in U^A \Rightarrow A \models (\exists x F) = 1$

Ex find a formula s.t.  $F$  is satisfiable but  $A \models F$  is unsatisfiable:  
 $F = P(x) \wedge \neg P(y)$   
 Ex Prove or disprove: If  $\Pi_3$  is complete  $\Rightarrow \Pi_1$  or  $\Pi_2$  is complete:  
 $\hookrightarrow$  indirect proof of an implication: 1. Assume  $\neg(\Pi_2 \text{ or } \Pi_3 \text{ is complete})$   
 $\Rightarrow$  both incomplete. It follows:  $\exists a, b \in S_1$  that is true but has no proof. (Same for  $b \in S_2$ )  $\Rightarrow (a, b) \in (S_1 \times S_2)$  and  $T_3(a, b) = 1$   
 $\Rightarrow \phi_3((a, b), (p_1, p_2)) = 0$  for all  $(p_1, p_2) \in (P_1 \times P_2)$   
 $\Rightarrow \phi_1(s_1, p_1) = \phi_2(s_2, p_2) = 1$  is always false since,  $a$  has no proof in  $P_1$  and  $b$  not in  $P_2 \Rightarrow \Pi_3$  is incomplete

Elements of multiplicative groups  $\mathbb{Z}_n^*$  and generators

| $\varphi$ | 0  | 1 | 2  | 3 | 4  | 5 | 6  | 7  | 8 | 9 |
|-----------|----|---|----|---|----|---|----|----|---|---|
| 0         | x  | 1 | 2  | 3 | 2  | 4 | 2  | 4  | 3 | 6 |
| 10        | 4  | 2 | 6  | 2 | 4  | 4 | 5  | 2  | 6 | 2 |
| 20        | 6  | 4 | 4  | 2 | 8  | 3 | 4  | 4  | 6 | 2 |
| 30        | 8  | 2 | 6  | 4 | 4  | 4 | 9  | 2  | 4 | 3 |
| 40        | 6  | 2 | 8  | 2 | 6  | 6 | 2  | 10 | 4 | 3 |
| 50        | 6  | 4 | 6  | 2 | 8  | 4 | 8  | 4  | 4 | 2 |
| 60        | 12 | 2 | 4  | 6 | 7  | 4 | 8  | 2  | 6 | 4 |
| 70        | 8  | 2 | 12 | 2 | 4  | 6 | 6  | 4  | 8 | 2 |
| 80        | 10 | 5 | 4  | 2 | 12 | 4 | 4  | 8  | 2 | 2 |
| 90        | 12 | 4 | 6  | 4 | 4  | 4 | 12 | 2  | 6 | 6 |

Prime in blue

DNF CNF

1) take rows = true false  
 2) write  $(x \vee y)$   
 3)  $x = (A \wedge B \wedge C)$   
 $A \wedge B \wedge C = 1$   
 $\neg A \vee \neg B \vee \neg C = 0$

| C | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
|---|---|---|---|---|---|---|---|---|
| B | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 |
| A | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 |

gen