# 5

Aufgabentyp: $R_{63}(100^{1207})$ (Hint: Di find $R_7(100^{1207})$ and $R_9(100^{1207}) \Rightarrow 100^{1207} \equiv_7 2 \wedge 100^{1207} \equiv_9 1$.
Since $\gcd(7,9)=1$, use CRT to find solution to $100^{1207} \equiv_{7\cdot 9=63} x$ with $m_1=9, m_2=7, a_1=1, a_2=2 \Rightarrow M=63, M_1=\frac{M}{m_1}=7, M_2=\frac{M}{m_2}=9, N_1 \cdot M_1 \equiv_9 1 \Rightarrow N_1=4, \ldots$

**If $R_m(a^c)=1$ then $R_m(a^n)=R_m(a^{R_c(n)})$**

**3.10:** Prove that the composition of relations is associative (Lem 3.5): $\rho(\sigma\phi)=(\rho\sigma)\phi$ states equality of sets. Suppose any $(a,d) \in \rho(\sigma\phi) \Rightarrow \exists b((a,b)\in\rho \wedge (b,d)\in\sigma\phi)$
$\Rightarrow \exists b(\exists c((a,b)\in\rho \wedge (b,c)\in\sigma) \wedge (c,d)\in\phi) \Rightarrow \exists b\exists c((a,b)\in\rho \wedge ((b,c)\in\sigma \wedge (c,d)\in\phi))$
$\Rightarrow \exists b\exists c((\exists c((a,b)\in\rho \wedge (b,c)\in\sigma) \wedge (c,d)\in\phi)) \Rightarrow \exists c\exists b((\exists b((a,b)\in\rho \wedge (b,c)\in\sigma) \wedge (c,d)\in\phi))$
$\Rightarrow \exists c(\exists b((a,b)\in\rho \wedge (b,c)\in\sigma) \wedge (c,d)\in\phi) \Rightarrow \exists c((a,c)\in\rho\sigma \wedge (c,d)\in\phi) \Rightarrow (a,d)\in(\rho\sigma)\phi$ ■

**3.11:** A relation $\rho$ is transitive $\Leftrightarrow \rho^2 \subseteq \rho$: ($\Leftarrow$): If $apb \wedge bpc$ then $ap^2c$, thus for also $apc$ since we assume $\rho^2 \subseteq \rho$. this means transitivity. ($\Rightarrow$) assume $ap^2b$ for some $a,b$. The Def. of $\rho^2$ ($=\rho\cdot\rho$) implies that exists $a\,c$ s.t. $apc$ and $cpb$, the assumed trans. of $\rho$ thus implies that $apb$ which concludes the proof ■

**3.12:** Intersection of two equivalence rel. is equiv. rel.: Suppose $\rho,\sigma$ are equiv. rel. on set $A$. $\rho \in A\times A$, $\sigma \subseteq A\times A \Rightarrow \rho\cap\sigma \subseteq A\times A$ (is also rel. on $A$!) (Refl.): Let $a\in A$, since $\rho,\sigma$ are equiv. rel., we have $\forall a((a,a)\in\rho \wedge (a,a)\in\sigma) \Rightarrow \forall a((a,a)\in(\rho\cap\sigma))$ (Def. of $\cap$) (Sym.): Let $a,b\in A$, s.t $(a,b)\in\rho\cap\sigma$
$\Rightarrow (a,b)\in\rho \wedge (a,b)\in\sigma \Rightarrow (b,a)\in\rho \wedge (b,a)\in\sigma$ ($\rho,\sigma$ are sym.) $\Rightarrow (b,a)\in\rho\cap\sigma$ (trans.): Let $a,b,c\in A$, s.t. $(a,b)\in\rho\cap\sigma \wedge (b,c)\in\rho\cap\sigma \Rightarrow (a,b)\in\rho \wedge (b,c)\in\rho$ and $(a,b)\in\sigma \wedge (b,c)\in\sigma \Rightarrow (a,c)\in\rho \wedge (a,c)\in\sigma$
$\Rightarrow (a,c)\in\rho\cap\sigma$. Hence we have shown that if $\rho,\sigma$ are equiv. rel., so is $\rho\cap\sigma$ ■

**3.13:** $f(A\cap B)=f(A)\cap f(B) \Leftrightarrow f$ is injective: ($\Rightarrow$): Let arb. $a,b\in X$, $a\neq b$. We define $\{a\}=A$, $\{b\}=B$
$\Rightarrow \{a\}\cap\{b\}=\emptyset \Rightarrow f(\{a\}\cap\{b\})=\emptyset \Rightarrow$ (we assume: $f(A\cap B)=f(A)\cap f(B)$) $f(\{a\})\cap f(\{b\})=\emptyset$
$\Leftrightarrow f(a)\neq f(b) \Rightarrow f$ is injective ($\Leftarrow$): Let $A\cap B\neq\emptyset$, $x\in f(A\cap B)$, $f(y)=x$, $y\in A\cap B \Rightarrow y\in A \wedge y\in B$
$\Rightarrow f(y)\in f(A)\cap f(y)\in f(B) \Rightarrow x\in f(A)\cap x\in f(B) \Rightarrow x\in f(A)\cap f(B)$ (noch umkehr zeigen) ■

**3.14:** If $g\circ f$ is injective and $f$ is surjective then $g$ is injective: Let $f:A\to B$, $g:B\to C$ be functions. Let $x,y\in B$ s.t. $g(x)=g(y)$. Since $f$ is surjective there exists two $a,b\in A$, s.t. $f(a)=x$, $f(b)=y \Rightarrow g(f(a))=g(f(b)) \Rightarrow g\circ f(a)=g\circ f(b)$
$\Rightarrow a=b$ (since $g$ injective) $\Rightarrow f(a)=f(b) \Rightarrow x=y$ Hence $g$ is injective ■

**3.15:** $g:B\to A$ is surjective $\Leftrightarrow f:A\to B$ is injective: ($\Rightarrow$): $g$ is totally and well defined. Since it is surjective, $\forall a\in A\exists b\in B(g(b)=a \Rightarrow |g^{-1}(\{a\})|\geq 1$ (Every element $a$ in $A$ has a pre-Image of cardinality $\geq 1$, spricht mehrere elemente könnten auf das gleiche Bildelement zeigen) Just taking the inverse would destroy the "well-definedness" (one element might target multiple values), hence, if $|g^{-1}(\{a\})|>1$ we define $f:A\to B$ with $a\mapsto b$, $b$ is one arb. element with $b=g^{-1}(a)$. $|g^{-1}(\{a\})|>1$. The function $f$ is totally (1) and well (2) defined. Since $g$ was well-defined, $a\neq a' \Rightarrow g^{-1}(\{a\})\cap g^{-1}(\{a'\})=\emptyset$, hence $f$ is injective. ($\Leftarrow$): $f$ is totally and well defined. We divide $B$ into 2 subgroups: $\mathrm{Im}(f(a))$ and $\overline{\mathrm{Im}(f(a))}$. As $f$ is injective, it is bijective onto $\mathrm{Im}(f(a))$ and $f^{-1}(\mathrm{Im}(f(A)))$ is also bijective from $\mathrm{Im}(f(A))\to A$. We use this implied surject. and define $g:B\to A$: $b\mapsto a \begin{cases} a=f^{-1}(b) \text{ if } b\in\mathrm{Im}(f(a)) \\ a=0 \text{ if } b\notin\mathrm{Im}(f(a)) \end{cases}$. As $\mathrm{Im}(f(A))\subseteq B$, $g$ is surjective, well and totally defined (Dieser proof nützlich, um funkt. zu konstr.) ■

**3.16:** (I) If $g\circ f$ are inj, so is $f\circ g$: Let $a,b\in A$. If $(f\circ g)(a)=(f\circ g)(b)$ then $f(g(a))=f(g(b))$. Since $f$ inj.
$\Rightarrow g(a)=g(b)$. Since $g$ inj. $\Rightarrow a=b \Rightarrow f\circ g$ is inj. ■ (II) If $g\circ f$ is inj., then $g$ is inj.? This is false: Let $A=\{1\}$, $B=\{1,2\}$, $C=\{1\}$. Define $f(1)=1$ and $g(1)=g(2)=1$. Then $g\circ f$ is inj. but $g$ is not! (III) If $g\circ f$ is inj., then is $f$? This is true: Let $a,b\in A$ with $a\neq b$ If $(g\circ f)(a)\neq(g\circ f)(b)$ then $g(f(a))\neq g(f(b)) \Rightarrow f(a)\neq f(b) \Rightarrow f$ inj. ■ (IV) If $g\circ f$ is surj., then $f$ is? Use (II), false (IV) If $g\circ f$ is surj., then is $g$? Correct: Since $g\circ f$ surj., $\forall c\in C\exists a\in A(g(f(a))=c)$. Let $b=f(a) \Rightarrow b\in B$ and $g(b)=g(f(a))=c$. Thus $g(b)=c$. Hence $g$ is surjective ■

**3.17:** For each $a,b\in A$, $[a]=[b]$ or $[a]\cap[b]=\emptyset$: case 1: $[a]\cap[b]=\emptyset$ case 2: $[a]\cap[b]\neq\emptyset$
If $[a]\cap[b]=\emptyset$, the first part of the disjunc. is true. Hence we only need to show $[a]\cap[b]\neq\emptyset \Rightarrow [a]=[b]$. Since $[a]\cap[b]\neq\emptyset$, there is $x$ in $A$, s.t. $x\in([a]\cap[b])$
$\Rightarrow x\in[a] \wedge x\in[b] \Rightarrow [x]=[a]\cap[x]=[b] \Rightarrow [a]=[b]$. Hence $[a]=[b]$ or $[a]\cap[b]=\emptyset$ ■

**3.18:** Let $\theta$ equiv. rel. on $A$. Prove that collection $A/\theta$ of all equiv. classes by $\theta$ is partition of $A$.
Since $\forall a\in A(a\in[a])$, $\bigcup_{i\in I}[a_i]=A$. It remains to prove that the equiv. classes are disjoint:
For any $a,b\in A$, $a\theta b \Rightarrow [a]=[b]$ and $a\not\theta b \Rightarrow [a]\cap[b]=\emptyset$. Prove that $a\theta b \Rightarrow [a]=[b]$
Consider arb. $c\in[a] \Leftrightarrow c\theta a$ (def. of $[a]$) $\Rightarrow c\theta b$ (transitivity of $\theta$) $\Leftrightarrow c\in[b] \Rightarrow [a]\subseteq[b]$
Now consider $d\in[b] \Leftrightarrow d\theta b \Rightarrow d\theta b\wedge a\theta b \Leftrightarrow d\theta b\wedge b\theta a$ (symmetry of $\theta$) $\Rightarrow d\theta a$
$\Rightarrow d\in[a] \Rightarrow [b]\subseteq[a] \Rightarrow [a]=[b]$. Now we prove $a\not\theta b \Rightarrow [a]\cap[b]=\emptyset$. (Contrad.):
Suppose $a\not\theta b \wedge [a]\cap[b]\neq\emptyset \Rightarrow \exists c(c\in[a]\cap[b]) \Rightarrow c\theta a\wedge c\theta b \Rightarrow a\theta c\wedge c\theta b$
$\Rightarrow a\theta b$ ↯ Contradiction, hence $a\not\theta b \Rightarrow [a]\cap[b]=\emptyset$ and hence $A/\theta$ is partition ■

**3.19:** Prove that the lexicographic order $\leq_{lex}$ is a partial order rel.: (I, refl.): Let arb. $(a_1,b_1)\in A\times B$
Since $\subseteq$ is reflex, we have $b_1\subseteq b_1$. Hence we get $(a_1=a_1\wedge b_1\subseteq b_1)$ and thus, $(a_1,b_1)\leq_{lex}(a_1,b_1)$ (II, antisym.): Take any $(a_1,b_1),(a_2,b_2)\in A\times B$, s.t. $(a_1,b_1)\leq_{lex}(a_2,b_2)$ and $(a_2,b_2)\leq_{lex}(a_1,b_1)$. This means that: $a_1\prec a_2$ (1) $\vee$ $(a_1=a_2\wedge b_1\subseteq b_2)$ (2) and $a_2\prec a_1$ (3) $\vee$ $(a_2=a_1\wedge b_2\subseteq b_1)$ (4)
By case dist., we show $(a_1,b_1)=(a_2,b_2)$: (1) and (3): $a_1\preceq a_2\wedge a_1\neq a_2$ and $a_2\preceq a_1\wedge a_2\neq a_1$. But since $\preceq$ is antisymmetric, we have $a_1=a_2$ which is contradiction with $a_1\neq a_2 \Rightarrow$ Illegal case (1), (4): $a_1\prec a_2 \wedge a_1\neq a_2$ and $(a_1=a_2\wedge b_2\subseteq b_2) \Rightarrow$ contradiction, illegal case (2), (3) same as 1.4 (2), (4): $(a_1=a_2\wedge b_1\subseteq b_2)$ and $(a_2=a_1\wedge b_2\subseteq b_1) \Rightarrow a_1=a_2$ and $(b_1\subseteq b_2\wedge b_2\subseteq b_1) \Rightarrow$ ($\subseteq$ is antisym.) $a_1=a_2$ and $b_1=b_2 \Rightarrow (a_1,b_1)=(a_2,b_2)$ (III, trans.): Let arb. $(a_1,b_1),(a_2,b_2),(a_3,b_3)\in A\times B$, s.t $(a_1,b_1)\leq_{lex}(a_2,b_2)$ and $(a_2,b_2)\leq_{lex}(a_3,b_3)$. That is: $a_1\prec a_2$ (1) $\vee$ $(a_1=a_2\wedge b_1\subseteq b_2)$ (2) and $a_2\prec a_3$ (3) $\vee$ $(a_2=a_3\wedge b_2\subseteq b_3)$ (4). By case dist., we show $(a_1,b_1)\leq_{lex}(a_3,b_3)$ (1), (3) $a_1\prec a_2$ and $a_2\prec a_3$ ($\prec$ is trans.) $\Rightarrow (a_1,b_1)\leq_{lex}(a_3,b_3)$ (1), (4) $a_1\prec a_2$ and $(a_2=a_3\wedge b_2\subseteq b_3) \Rightarrow (a_1,b_1)\leq_{lex}(a_3,b_3)$ (2), (3) $(a_1=a_2\wedge b_1\subseteq b_2)$ and $(a_2\prec a_3) \Rightarrow a_1\prec a_3 \Rightarrow (a_1,b_1)\leq_{lex}(a_3,b_3)$
(2), (4) $a_1=a_2\wedge b_1\subseteq b_2$ and $a_2=a_3\wedge b_2\subseteq b_3 \Rightarrow a_1=a_3\wedge b_1\subseteq b_2\wedge b_2\subseteq b_3$
$\Rightarrow a_1=a_3\wedge b_1\subseteq b_3$ (trans. of $\subseteq$) $\Rightarrow (a_1,b_1)\leq_{lex}(a_3,b_3)$, Hence its partial ord. rel. ■

**4.1:** If $(a,b)=(d)$ then $d=\gcd(a,b)$: $(a\in(d)\wedge b\in(d)) \to (d|a\wedge d|b)$, If $(c|a\wedge c|b) \to c|(ua+vb)$ (i.e. every common divisor $c$ of $a,b$ divides every integer of form $ua+vb$, especially also $d=u_0a+v_0b) \Rightarrow c|d$ ■ (Lem 4.3)

**4.2:** For $a,b\in\mathbb{Z}$, there exists $d\in\mathbb{Z}$, such that $(a,b)=(d)$: Let $d$ be the smallest positive element in $(a,b)$. (Clearly, $(d)\subseteq(a,b)$. We need to show $(a,b)\subseteq(d)$: For any $c\in(a,b)$, $c=q\cdot d+r$
Since both $c,d\in(a,b)$, so is $(r=c-q\cdot d)\in(a,b)$ Since $0\leq r<d$ and $d$ (by assumption is the smallest positive int. in $(a,b)$, $r=0$, thus $c=q\cdot d$, hence $(a,b)\subseteq(d)$ ■ (Lem 4.4)

**4.3:** For all $a,b\in\mathbb{Z}$, there are $u,v$, s.t. $ua+vb=\gcd(a,b)$: Its the smallest positive element in $(a,b)=\{ua+vb \mid u,v\in\mathbb{Z}\}$ (weil $\gcd(a,b)=\min\{a\cdot s+b\cdot t \mid (s,t)\in\mathbb{Z}\times\mathbb{Z}\wedge(a\cdot s+b\cdot t)>0\}$ bzw. $(a,b)=\{ua+vb \mid u,v\in\mathbb{Z}\}=(\gcd(a,b))=\{u\cdot\gcd(a,b) \mid u\in\mathbb{Z}\}$, all this useful for proofs with $\gcd(a,b)=1$ ■

**4.4:** $\gcd(m,n)=\gcd(m-qn,n)$: Let $d=\gcd(m,n) \Rightarrow d|m\wedge d|n \Rightarrow \exists k(k\cdot d=m)\wedge\exists j(j\cdot d=n)$
$\Rightarrow \exists k,j(m-qn=k\cdot d-q\cdot j\cdot d) \Leftrightarrow \exists k,j(m-qn=d(k-q\cdot j) \Rightarrow d|m-qn\wedge d|n$. Let $c$ be a simple common divisor of $(m-qn,n) \Rightarrow \exists k,j(k\cdot c=m-qn) \Rightarrow \exists k,j(kc=m-q\cdot j\cdot c)$
$\Rightarrow \exists k,j(kc+q\cdot j\cdot c=m) \Rightarrow c|m \Rightarrow c|m\wedge c|n \Rightarrow c|d$ ■

**4.5:** $\gcd(xa,xb)=x\cdot\gcd(a,b)$: Let $d=\gcd(a,b) \Rightarrow (d|a\wedge d|b)\wedge\exists u,v(ua+vb=d)$. Let $d'$ be $\gcd(xa,xb) \Rightarrow d'|xa\wedge d'|xb \Rightarrow \exists u,v(d'|xua\wedge d'|xvb) \Rightarrow \exists u,v(d'|(xua+xvb))$
$\Leftrightarrow d'|x\cdot d$. z.z.: $xd|d'$: $\exists u,v(uxa+vxb=d')$, $d|a\wedge d|b \Rightarrow xd|xa\wedge xd|xb$
$\Rightarrow xd|xua\wedge xd|xvb \Rightarrow xd|(xua+xvb) \Leftrightarrow xd|d'$. $(x\cdot d|d'\wedge d'|x\cdot d) \Rightarrow d'=x\cdot d$ ■

**4.6:** $\gcd(a,b)=a \Leftrightarrow a|b$: ($\Rightarrow$): $a|a\wedge a|b \Rightarrow a|b$ ($\Leftarrow$): If $\exists c(c|a\wedge c|b)$, then $c|a, \gcd(a,b)=a$ ■

**4.7:** $\gcd(a,b)=1 \Leftrightarrow \exists u,v(ua+vb=1)$: See 4.2 ■

**4.8:** $ax\equiv_m b$ has 1 solution if $\gcd(a,m)=1$: Case dist.: (case I): $\gcd(a,m)=1$ and $b=1$ then $ax\equiv_m 1$ has exactly 1 sol mod $m$, since, if $ax\equiv_m ay$, then $m|a(x-y)$ and since $\gcd(a,m)=1$, $\Rightarrow m|(x-y)$, hence $x\equiv_m y$ and hence $x$ is unique (Case II): $\gcd(a,m)=1$ and $b=k$ ($k\in\mathbb{Z}$) then $ax\equiv_m 1$ has clearly sol. for $x=ky$. If $aw\equiv_m k$ is another sol., then $aw\equiv_m ax$ and since $\gcd(a,m)=1$, $m|w-x$, hence $w\equiv_m x$

**4.9:** If $\gcd(n,m)=1$, prove $a\equiv_{mn}b \Leftrightarrow a\equiv_n b\wedge a\equiv_m b$: ($\Rightarrow$) $a\equiv_{mn}b \Rightarrow a+n\cdot m\cdot k=b \Rightarrow \begin{matrix} a+n\cdot(m\cdot k)=b \text{ and} \\ a+m\cdot(n\cdot k)=b \end{matrix} \Rightarrow a\equiv_n b, a\equiv_m b$
($\Leftarrow$): $a\equiv_n b\wedge a\equiv_m b \Rightarrow n|a-b\wedge m|a-b \Rightarrow \exists k,j(k\cdot n=a-b\wedge j\cdot m=a-b) \Rightarrow \exists k,j(k\cdot n=j\cdot m) \Rightarrow n|j\cdot m$
$\Rightarrow$ (since $\gcd(n,m)=1$, hence) $n|j \Leftrightarrow \exists v(v\cdot n=j) \Rightarrow \exists v(v\cdot n\cdot m=(a-b)) \Rightarrow nm|(a-b) \Rightarrow a\equiv_{mn}b$ ■
((Alternativer proof für $\Leftarrow$): Betrachte: $x\equiv_m R_m(b)$, $x\equiv_n R_n(b)$. Acc. to CRT, all sol. of this are congr. mod $m\cdot n$)

**4.10:** If $\gcd(n,m)=1$, prove $n|y\cdot m \to n|y$: $\gcd(u,m)=1 \Rightarrow \exists u,v(un+vm=1) \Leftrightarrow \exists v(v\cdot m\equiv_n 1\equiv R_n(v\cdot m)=1)$
$n|y\cdot m \Rightarrow \forall v(n|y\cdot v\cdot m) \Rightarrow R_n(y\cdot v\cdot m)=0 \Leftrightarrow R_n(R_n(y)\cdot R_n(v\cdot m))=0 \Rightarrow R_n(R_n(y)\cdot 1) \Rightarrow R_n(R_n(y))$
$=R_n(y)=0 \Leftrightarrow n|y$ ■

**4.11:** $R_m(a+b)=R_m(R_m(a)+R_m(b))$: $a=k\cdot m+r_a$, $b=k'\cdot m+r_b \Rightarrow R_m(a)=r_a$, $R_m(b)=r_b \Rightarrow r_a+r_b=k''\cdot m+r_{a+b}$
$\Rightarrow R_m(R_m(a)+R_m(b))=R_m(k''\cdot m+r_{a+b})=r_{a+b}$. $R_m(a+b)=R_m((k'+k)\cdot m+k''\cdot m+r_{a+b})=r_{a+b}$ ■

**4.12:** $R_x(R_{x\cdot k}(a))=R_x(a)$: Write $a$ as $a=v\cdot x\cdot k+r \Rightarrow R_x(R_{x\cdot k}(a))=R_x(R_{x\cdot k}(v\cdot x\cdot k+r))=R_x(R_{x\cdot k}(vxk$
$+R_{xk}(r)))=R_x(R_{xk}(r))=R_x(R_{xk}(r))=R_x(r)$, $R_x(a)=R_x(v\cdot x\cdot k+r)=$ (step needed) $=R_x(r)$ ■

**4.13:** Prove $913'406 \equiv_9 247\cdot 3'698$: $R_9(913406)=R_9(23)=5$, $R_9(247\cdot 3698)=R_9(R_9(247)$
$\cdot R_9(3698))=R_9(R_9(13)\cdot R_9(26))=R_9(4\cdot 8)=R_9(32)=5=R_9(913406)$ ■

**4.14:** Calculate all sol. $0\leq x<195$ for $\begin{matrix} \text{I } 2x^2+8\equiv_{13}6 \\ \text{II } x\equiv_{15}2 \end{matrix}$: First, we transform I: $2x^2\equiv_{13}11$ ($6\ominus_{13}8=11$)
then we get rid of coeff. 2 by multiplying both sides with the mult. inv of 2 ($\mathrm{inv}(2)=7$)
$x^2\equiv_{13}12$ Then decompose $x^2\equiv_{13}12$: Trick: add $m$ (von $\equiv_m$, also 13) to 6 until its a quadratic numb: $12+0\cdot 13=12$, $12+1\cdot 13=\underline{25}$! $25=5^2$ Hence, 5 and $-5$ ($\equiv_{13}8$) are two solutions. Hence we split the whole system into $\text{I}\ x\equiv_{13}5$ $\text{II}\ x\equiv_{15}2$ and $\text{III}\ x\equiv_{13}8$ $\text{IV}\ x\equiv_{15}2$
Solving I, II: $M=13\cdot 15=195$, $N_1=15\cdot N_1\equiv_{13}1 \Rightarrow N_1=7$ (calc. the mult. inv. of 15 mod 13 to get $N_i$)
$N_2=13\cdot N_2\equiv_{15}1 \Rightarrow N_2=7$, $x=R_{195}(5\cdot 15\cdot 7+2\cdot 13\cdot 7)=122$, equivalently, for III, IV, we get $x_2=47$. There are unique in $0\leq x<195$, hence, we have computed all solutions to the system ■

**4.15:** Why is $n$ divisible by 3 if its cross sum is? (consider 4 digit number $abcd$. We have: $abcd=10^3a+10^2b+10c+d=(999+1)a+(99+1)b+(9+1)c+d=3(333a+33b+3c)+(a+b+c+d)=x\cdot R_3(x)=R_3(a+b+c+d)$ ■

**4.16:** ((Unsatisfiability of equations) Prove $\neg\exists m,n\in\mathbb{Z}(n^5+7=m^2)$: Case dist: (If $m$ odd, then $n$ even, if $m$ even, then $n$ odd) (case I, $m$ odd): $(2k)^5+7=(2c+1)^2 \Leftrightarrow 32k^5+7=4c^2+4c+1 \Leftrightarrow 32k^5+6=4c^2+4c$
$\Rightarrow$ no sol., since $32k^5+6\equiv_4 2$ and $4c^2+4c\equiv_4 0$ and we know that $a\neq m\,b \Rightarrow a\neq b$ (case II, $m$ even):
$(2k+1)^5+7=(2c)^2 \Leftrightarrow 32k^5+80k^4+80k^3+40k^2+10k+8=4c^2 \Leftrightarrow 4(8k^5+20(k^4+k^3)+10k^2+2)+10k=4c^2$
$\Rightarrow$ no sol., since $4(8k^5+20(k^4+k^3)+10k^2+2)+10k\equiv_4 2$ but $4c^2\equiv_4 0$ since $4(\cdots)\equiv_4 0$ but $10k\equiv_4 2$ ■

**4.17:** Prove CRT uniqueness (Use 4.8 technique): Assume $x_1,x_2$ are two sol. Hence for arb $a_i$, we have $x_1\equiv_{m_i}x_2\equiv_{m_i}a_i \Rightarrow m_i|x_1-x_2$ Since $[m_1,\ldots,m_n]$ are pairwise rel. prime, we have $m_1\cdot\ldots\cdot m_n|x_1-x_2$
$\Rightarrow x_1\equiv_{m_1\cdot\ldots\cdot m_n}x_2$ ■ (In CRT, $m_1\cdot\ldots\cdot m_n$ is often denot. as "$M$") (This proves, CRT has 1 sol. mod $M$. One can add further sol. by $x_i=x_1+M\cdot n$, $n\in\mathbb{N}^+$)

# 6 gcd of polynomials. Extended euclid:

Let $f(x)=x^3+x^2+x+1$, $g(x)=x^3+1$ in $\mathbb{Q}[x]$. Then: $f(x)/g(x)=x^2+x \Rightarrow (x^3+x^2+x+1)=(x^2+1)\cdot 1+(x^2+x)$. Then: $(x^3+1)/(x^2+x) \Rightarrow x^3+1=(x^2+x)\cdot x+(-x^2+1)$. Then: $(x^2+x)/(-x^2+1) \Rightarrow x^2+x=(-x^2+1)\cdot(-1)+(x+1)$
Then: $(-x^2+1)/(x+1) \Rightarrow -x^2+1=(x+1)(-x+1) \Rightarrow \gcd(f(x),g(x))=(x+1)$ and: $\operatorname{lcm}(f(x),g(x))=\frac{f(x)\cdot g(x)}{\gcd(f(x),g(x))}$ proved in 5.13 see 5.13

**5.1:** Only one neutral element: Let $e,e'$ be neutral elements. Then $e=e*e'=e'$ ■

**5.2:** Only one inverse element: Let $b,c$ be inverses of $a$, $b$ is left-an $c$ right-inverse. Then $b \overset{E2}{=} b*e \overset{E3}{=} b*(a*c) \overset{E1}{=} (b*a)*c \overset{E3}{=} e*c \overset{E2}{=} c$ ■

**5.3:** $\widehat{a*b}=\hat{b}*\hat{a}$: (We need to show that $(a*b)*(\hat{b}*\hat{a})=(\hat{b}*\hat{a})*(a*b)=e$): I $(a*b)*(\hat{b}*\hat{a}) \overset{E1}{=} a*(b*\hat{b})*\hat{a} \overset{E3}{=} a*(e)*\hat{a} \overset{E1}{=} (a*e)*\hat{a} \overset{E2}{=} a*\hat{a} \overset{E3}{=} e$ (same for vice versa) ■

**5.4:** $a*b=a*c \Rightarrow b=c$: Take $a*b=a*b$, apply $\hat{a}$: $\hat{a}*(a*b)=\hat{a}*(a*b) \Leftrightarrow b=c$ ■

**5.5:** $a*x=b$ has unique sol.: add $\hat{a}$: $(\hat{a}*a)*x=\hat{a}*b \Rightarrow x=\hat{a}*b$ Now we need to show that this is true: $a*x=b \overset{\text{einsetzen}}{\Leftrightarrow} a*(\hat{a}*b)=b \overset{E1}{\Leftrightarrow} (a*\hat{a})*b=b \overset{E3}{\Leftrightarrow} e*b=b \overset{E2}{\Leftrightarrow} b=b$ ■

**5.6:** Let $G$ be finite set and $*$ operation with $*$ associative and commut. and with $\forall a,b,c\in G\,(a*b=a*c \to b=c)$
I: Let $a\in G$ be arb. $\exists m,n\in\mathbb{N}(n<m \wedge a^n=a^m) \Rightarrow$ let $z=m-n \Rightarrow a^z*a^n=a^m$, Thus $a^z$ is neutral elmnt.
II: Let $k\in G$ be arb. For the inv. of $a$ we simply compute $e=a^{(m-n)}$ and then $\hat{a}=a^{(m-n)-1}$ as now $a*\hat{a}=a^{m-n}=e$ ■

**5.7:** Let $G$ be a group and let $a\in G$. Prov $\langle a\rangle=\langle a^{-1}\rangle$: Approach: show $a\in\langle a\rangle$ and $a\in\langle a^{-1}\rangle$ because $\langle a\rangle$ is the smallest subgroup of $G$ that contains $a$, Hence if $a\in H$ for any $H\leq G$, then $\langle a\rangle\subseteq H$. This implies if $a\in\langle a^{-1}\rangle$ then $\langle a\rangle\subseteq\langle a^{-1}\rangle$. (Also need to show $a^{-1}\in\langle a\rangle$). By Def. 5.14, $a^{-1}\in\langle a\rangle$ and $(a^{-1})^{-1}$ $(=a)\in\langle a^{-1}\rangle$ Hence $\langle a\rangle=\langle a^{-1}\rangle$ ■

**5.8:** Prove that a subgroup of a cyclic group is cyclic: Take an arb. cyclic group $\langle G;*;^{-1};e\rangle$ with generator $g$ and any subgroup $H$. If $H=\{e\}$, its trivially cyclic. Else, let $n>0$ be the smallest Integer, s.t. $g^n\in H$. We show that $H$ is generated by $h=g^n$: Take any $a\in H$. We show $\exists q\in\mathbb{Z}\,(a=h^q)$. Since $g$ is generator of $G$, $\exists m\in\mathbb{Z}\,(a=g^m)$ let $q$ and $0\leq r<n$ be such that $m=q\cdot n+r$. Hence, we have $a=g^m=g^{n\cdot q+r}=(g^n)^q g^r=h^q g^r$. Hence $g^r=(h^q)^{-1}*a=(a)^{-1}*a$ Since $H$ is closed under inverses and the group operation $*$, $g^r\in H$. But since $0\leq r<n$ and $n$ was the smallest positive integer, s.t. $g^n\in H$, we must have $r=0$. Hence $a=h^q$ ■

**5.9:** List all subgroups of $\langle\mathbb{Z}_4;\oplus\rangle\times\langle\mathbb{Z}_5;\oplus\rangle$: $\{(0,0)\}$, $\{0,2\}\times\{0\}$, $\mathbb{Z}_4\times\{0\}$, $\{0\}\times\mathbb{Z}_5$, $\{0,2\}\times\mathbb{Z}_5$, $\mathbb{Z}_4\times\mathbb{Z}_5$
Begründung: Lagrange, $|H|\,|G|$ so $H\leq G$ and the subsets must be closed under $\oplus$, contain the neutral element $(0,0)$ and an inverse, e.g., in $\{0,2\}\times\mathbb{Z}_5$, $\operatorname{inv}((2,1))$ is $(2,4)$, thats why $\{0,3\}\times\mathbb{Z}_5$ is not, since $\oplus$ isn't closed, i.e. $(3,n\in\mathbb{Z}_5)\oplus(3,k\in\mathbb{Z}_5)$ does not exist!

**5.10:** Let $G$ be a group, s.t. $a*a=e$. Prove that $G$ is commut.: $a*a=e\Rightarrow a=\hat{a}$ and $a*b=\widehat{a*b}=\hat{b}*\hat{a}=b*a$, hence it is commutative ■

**5.11:** Let $G$ be a group. Prove $H=\{a\in G\mid\forall b\in G(a*b=b*a)\}$ is a Subgroup: (I is closed, i.e $(a_1*a_2)*b=b*(a_1*a_2)$): $(a_1*a_2)*b=a_1*(a_2*b)=a_1*(b*a_2)=\ldots=b*(a_1*a_2)$. (II, $e\in H$) $e*b=b*e$ (G2) (III, $\hat{a}\in H$ for all $a$, i.e, need to show $\hat{a}*b=b*\hat{a}$): $\hat{a}*b=\hat{b}*a$ (since $b\in H$, $\hat{b}\in H$, hence $\hat{b}*a=a*\hat{b}=\widehat{a*b}=b*\hat{a}$. Hence $H$ is a subgroup of $G$ ■

**5.12:** Elements in finite groups have finite order: Suppose not: Consider any element $g$ of any group $G$. If $|g|$ is not finite, then there exists a bijection from $\mathbb{N}$ to the set $X$ of all powers of $g$. But since $G$ is finite, all these powers of $g$ cannot be all distinct: Let $g^m=g^{m+k}$ with $k$ is the smallest pos. Int. for which this property holds: Then $g^m=g^{k+m}\Rightarrow g^{-m}g^m=g^{-m}g^{k+m}\Rightarrow g^0=g^k\Rightarrow e=g^k$. Hence $|g|=k<\infty$ and it is proven ■

**5.13:** (Ring): $a\cdot 0=0$: $a\cdot 0=0\Leftrightarrow a\cdot 0=a\cdot(0+0)\Leftrightarrow a\cdot 0=a\cdot 0+a\cdot 0 \overset{-(a\cdot 0)}{\Leftrightarrow} 0=a\cdot 0$ ■
(Ring): $(-a)\cdot b=-(a\cdot b)$: $(-a)\cdot b+a\cdot b=((-a)+a)\cdot b=0\cdot b=0$. Since $\exists$ only one inverse, $(-a)b=-(ab)$

**5.14:** (Ring): $(-a)(-b)=a\cdot b$: $-(a\cdot b)+(-a)(-b)=(-a)\cdot b+(-a)(-b)=(-a)(b+(-b))=(-a)\cdot 0=0$, only one inv. ■

**5.15:** (Ring): $-(-a)=a$: Since Ring consists of group, a "-" are part of group, we have $(\hat{a})=a$, $-(-a)=a$ ■

**5.16:** (Ring). $1\,!=0$: Let $a\neq 0$ be $\in R$. Suppose $0=1\Rightarrow a=a\cdot 1=a\cdot 0=0$ ↯ since $a\neq 0$. Hence, $1\neq 0$ ■

**5.17:** Prove the image of a group homo is a subgroup of the codomain: We use the fact $\psi(a*b)=\psi(a)\circ\psi(b)$
(I) $\psi(a)\circ\psi(b)\in\operatorname{Im}(\psi)$?: $\psi(a)\circ\psi(b)=\psi(a*b)$ and $\psi(a*b)\in\operatorname{Im}(\psi)$. (II) $\psi(e)\circ\psi(a)=\psi(a)\circ\psi(e)=\psi(a)$: $\psi(e)\circ\psi(a)=\psi(e*a)=\psi(a)\wedge\psi(a)\circ\psi(e)=\psi(a*e)=\psi(a)$ for all $a\in G$, (III) $\psi(a)^{-1}\circ\psi(a)$ $=\psi(a)\circ\psi(a)^{-1}=\psi(e)$ for all $a\in G$ with $\psi(a)^{-1}$ existing for each $\psi(a)$? For arb. $a$, $\psi(a)^{-1}=\psi(\hat{a})\Rightarrow$ $\psi(a)^{-1}\circ\psi(a)=\psi(\hat{a}*a)=\psi(e)\wedge\psi(a)\circ\psi(a)^{-1}=\psi(a*\hat{a})=\psi(e)$ ■ (This proof: $\psi(G)\leq H$)

**5.18:** Assume group homo $\psi:H\to G$. Prove $\psi(e_H)=e_G$: $\psi(e_H)=\psi(e_H)\circ e_G \overset{G2}{=}\psi(e_H)\circ(\psi(e_H)\circ\widehat{\psi(e_H)}) \overset{G3}{=}(\psi(e_H)\circ\psi(e_H))\circ\widehat{\psi(e_H)}$
$=(\psi(e_H*e_H))\circ\widehat{\psi(e_H)}=(\psi(e_H))\circ\widehat{\psi(e_H)}=e_G$ ■

**5.19:** group hom $\psi:H\to G$. Prove $\psi(h^n)=\psi(h)^n$ (Proof by Induct.) IH: $\psi(h^n)=\psi(h)^n$ Assume $\psi(h^n)=\psi(h)^n$ holds for $n$. IS $(n\to n+1)$: $\psi(h^{n+1})=\psi(h^n*h^1)=\psi(h^n)\circ\psi(h)=\psi(h)^n\circ\psi(h)=\psi(h)^{n+1}$ ■

**5.20:** $\psi(\hat{h})=\widehat{\psi(h)}$: $\psi(\hat{h})=\psi(\hat{h})\circ e_G=\psi(\hat{h})\circ(\psi(h)\circ\widehat{\psi(h)})=(\psi(\hat{h})\circ\psi(h))\circ\widehat{\psi(h)}=\psi(h*\hat{h})\circ\widehat{\psi(h)}$
$=\psi(e_H)\circ\widehat{\psi(h)}=e_G\circ\widehat{\psi(h)}=\widehat{\psi(h)}$ ■

**5.21:** Isomorphismen bilden generatoren auf generatoren ab: Let $\langle g\rangle=G$ and $\psi:G\to H$ isom. 1.: $H$ is closed, hence $\langle\psi(g)\rangle\leq H$ 2.: $\psi$ is bijective, hence, $\forall h\in H\,\exists b\in G(\psi(b)=h)$ 3.: $\langle g\rangle=G\Rightarrow b=g^m$ for some $m$.
$\Rightarrow\forall h\in H\,\exists m\in\mathbb{Z}\,(h=\psi(g^m)\overset{5.19}{=}\psi(g)^m)\Rightarrow H\subseteq\langle\psi(g)\rangle\Rightarrow H=\langle\psi(g)\rangle\Rightarrow\psi(g)$ is generator ■

**5.22:** Cyclic groups of same order are isomorph: Let $|G|=|H|$, $\psi:G\to H$ with $g\mapsto h$. $\langle g\rangle=G$, $\langle h\rangle=H$.
(I: Homomorphism): $\psi(a*b)=\psi(g^r*g^i)=\psi(g^{r+i})=\psi(g)^{r+i}=h^{r+i}=h^r\circ h^i=\psi(g^r)\circ\psi(h^i)=\psi(a)\circ\psi(b)$
(II: Bijective): Surj.: Let $h'\in H$ arb. $\Rightarrow h'=h^r$ for some $r\Rightarrow h'=\psi(g)^r=\psi(g^r)$, Inj.: $g'=g''\Rightarrow g'=g^r\wedge g''=g^r$
$\Rightarrow\psi(g')=\psi(g'')$ since $\psi(g')=\psi(g^r)=h^r\wedge\psi(g'')=\psi(g^r)=h^r$ ■ (shows neutral element, inv, closure in one step, just pick the corresponding $a,b$, e.g. $b=a$)

**5.23:** One-Step-Subgroup-Test: $H$ is subgroup of $G\Leftrightarrow$ (1) $H\neq\emptyset$ (2) $\forall a,b\in H(a*b^{-1}\in H)$

**5.24:** Isomorphisms map subgroups to subgroups: Let $\psi:G\to H$ Isom., $K\leq G$, $a,b\in K$. Let $\psi(a),\psi(b)$ be elements of $\psi(K)$ (Hence, $\psi(K)$ is not empty), We show that $\psi(a)\circ\psi(b)^{-1}\in\psi(K)$: $\psi(a)\circ\psi(b^{-1})$ $\overset{(5.23)}{=}\psi(a)\circ\psi(b^{-1})=\psi(a*b^{-1})$. Since $a*b^{-1}\in K$, $\psi(a*b^{-1})\in\psi(K)$ and hence by one-step-test, it's true ■

**5.25:** $\psi:G\to H$ is Isomorphism. Prove if $G$ is abelian, so is $H$: $G$ is abelian $\Rightarrow$ Let $a,b\in H$. Since $\psi$ is surj. $\exists u,v\in G(\psi(u)=a\wedge\psi(v)=b)\Rightarrow a\circ b=\psi(u)\circ\psi(v)=\psi(u*v)=\psi(v*u)=\psi(v)\circ\psi(u)=b\circ a$ ■

**5.26:** Let $\langle g\rangle=G$ with $|G|=n$, $x\in G$. #sol. of $x^k=1$ is $\gcd(k,n)$: Since $x^n=1$, $x^k$ has precisely $d$ solutions if $d$ divides $n$: If some $d\,|\,n$, then $x=\frac{n}{d}$ is an Int. sol to $d\,x\equiv_n 0$, morover any multiple is also solution: $0\cdot\frac{n}{d},1\cdot\frac{n}{d},2\cdot\frac{n}{d},\ldots,(d-1)\cdot\frac{n}{d}$. Since the sol. $x$ needs to be $0\leq x<n$, $d\cdot\frac{n}{d}$ is too big. Since there is an isomorphism $\langle g\rangle$ to $\mathbb{Z}_n$, this means $x^k=1$ has $\gcd(k,n)=d$ solutions ■

**5.27:** The inv. of an Isom. ($\psi:G\to H$) is an Isom.: The bijectivity is trivial, hence, we only need to show $\psi^{-1}$ is an homomorphism: Let arb. $c,d\in H$, s.t. $\psi(a)=c$, $\psi(b)=d\Rightarrow\psi^{-1}(c\circ d)=\psi^{-1}(\psi(a)\circ\psi(b))=\psi^{-1}(\psi(a*b))$
$=a*b=\psi^{-1}(c)*\psi^{-1}(d)$ ■

**5.28:** Isomorphic groups have the same amount of generators: We know that Isomorphisms map generators onto generators. Let $G_G$ and $H_H$ be the sets of generators of $G$ (bzw. $H$). Da für jeden Generator aus $G$ ein einzigartiger Generator in $H$ existieren muss, gilt: $|G_G|\leq|H_H|$. Da $\psi^{-1}$ auch Isom. ist, gilt auch $|H_H|\leq|G_G|\Rightarrow|H_H|=|G_G|$ ■

**5.29:** Determine order: (of element): $\operatorname{ord}(a)\,|\,|G|$, hence: test for all $z\,|\,|G|$ if $a^z=e$ (mult. group): If $p$ prime, then $\varphi(p^c)=p^{c-1}(p-1)$

**5.30:** Isom. From cyclic group to $\langle\mathbb{Z}_n;\oplus\rangle$: $\psi:\langle g\rangle\to\langle\mathbb{Z}_n;\oplus\rangle$ has $g^i\mapsto i$, $\psi:\langle\mathbb{Z}_n;\oplus\rangle\to\langle g\rangle$ has $i\mapsto g^i$. Is Isomorphism. Since $i\oplus j=g^{i+j}=g^i*g^j$ ■

→ How many isomorphisms from $G$ to $H$? ⇒ #generators $=\varphi(n)$: We can map the first generator of $G$ to $\varphi(n)$ of $H$. While doing so, we also map all other generators of $G$ to generators of $H$, hence the same. So no function fulfills $\varphi(a\oplus_n b)$ $=\varphi(a)\oplus_m\varphi(b)$ since one can just set $a=0$ and $1\neq\varphi(a)\oplus_m\varphi(0)$

**5.31:** $\mathbb{Z}_{24}^*\not\cong\mathbb{Z}_{16}^*$: $|\mathbb{Z}_{24}^*|=\varphi(24)=2^2(1)\cdot 1^0(2)=8$, $|\mathbb{Z}_{16}^*|=\varphi(2^4)=2^3(1)=8$, hence $\exists$ bijection.
Bad, no homomorphism: $\mathbb{Z}_{24}^*\cong\mathbb{Z}_8^*\times\mathbb{Z}_3^*$ In $\mathbb{Z}_8^*$ & $\mathbb{Z}_3^*$ all a han $\operatorname{ord}(a)=2$, is true in $\mathbb{Z}_{24}^*$ $\cdot=\psi(a)\odot_m\psi(b)$ since one can then false

**5.32:** Let $G$ be abelian, finite, Let $n>0$, Define $\psi:G\to G$, $\psi(g)\mapsto g^n$ $(\forall g\in G)$. Find necessary & suffic. cond., s.t. $\psi$ is Isom.:
$\psi$ is Isom$\Leftrightarrow$ $G$ has no nontrivial element whose order is a divisor of $n$ ■

**5.33:** Finite Integral Domain is field: Its by Def. a commut. Ring, now we show $\forall v\in D\,\exists w(vw=wv=1)$: Take a func $\psi:D\to D$, $x\mapsto vx$ (and arb. $v\in D$, $v\neq 0$). It is injective, since if $\psi(x)=\psi(x')\Leftrightarrow vx=vx'\Leftrightarrow 0=vx-vx'\Leftrightarrow 0=v(x-x')$
Since $v\neq 0\Rightarrow x-x'=0\Rightarrow x=x'$. Since $D$ is finite, $\psi$ is also surj. $\Rightarrow\forall v\in D\,\exists w\in D\,(vw=\psi(v)=1)$, thus $v$ is unit ■

**5.34:** Find all irred. polyn in $G_7[2][x]$: (2): $111$ (3): $1101, 1011$ (4): $11111, 11001$ (5): $100101, 101111, 101001, 111011, 111101, 110111$

**5.35:** Tricks: (zerodivisors) all $a_i$ s.t. $\gcd(a_i,m)>1$ (units): all $a_i$ st. $\gcd(a_i,m)=1$ (Is Field?): check if $m(x)$ is reducible (Is irred?): If $\deg=2$ or 3, check if has roots (cor. 29), else check if divisible by polynomial of deg $\in[1,\frac{\deg}{2}]$ (Find zerodivisors with polynomials): Ex: $G_7[3]_{x^2+2x}$: Find factors (here of deg=1): $x, x+2$. Then all $ax,b(x+2)$ for $a,b\in\mathbb{Z}_7$ are sol.

**5.36:** Proof that polynomial of deg $t$ is uniquely defined by $d+1$ values of $a(x)$: Lagrange Interpol, prove uniqueness: Suppose $\exists a'(x)$ of deg $d$, s.t. $\beta_i=a'(a_i)$. Then $a(x)-a'(x)$ is also Polynomial of deg at most $d$ with at most $d$ roots unless its 0. But $a(x)-a'(x)$ has $d+1$ roots, hence its $0\Rightarrow a(x)=a'(x)$

**5.37:** If $D$ is Integr. Dom., then so is $D[x]$: Let arb. $f(x)=a_n x^n+\ldots+a_0$ and $g(x)=b_m x^m+\ldots+b_0$ be in $D[x]$ with $a_n,b_m\neq 0$. Then $f(x)\cdot g(x)=a_n b_m x^{n+m}+\ldots+a_0 b_0$. As $D$ is Integr. dom & $a_n,b_m\neq 0$, so is $f(x)g(x)\neq 0$ ■

**5.38:** The units of $D[x]$ are the constant polyn. that are units of $D$ ($D[x]^*=D^*$): As proved in 5.37, $\deg(f(x)g(x))\neq 0$, but the units in $D$ have inverses ■

**6.1:** The res. calc. is sound: (Show $\{K_1,K_2\}\vdash_{\text{Res}}K\Rightarrow\{K_1,K_2\}\models K$) Let $A$ be Interpr. s.t. it is suitable for $K_1,K_2,K$:
If $A$ is model for $\{K_1,K_2\}$ it has to make at least one literal in $K_1$ and one in $K_2$ true ($K_2$ contains $L$, $K_2\setminus L$)
((case Dist.: ① $A(L)=1$: Then one literal in $K_2\setminus\{\neg L\}$ is true as $A(\neg L)=0$. ② $A(L)=0$: Then one literal in $K_1\setminus\{L\}$ is true) Since, for the Implic., in both cases we assume $A$ is model for $\{K_1,K_2\}\Rightarrow K=(K_1\setminus\{L\})\cup(K_2\setminus\{\overline{L}\})$ is true ■

**6.2:** The res. calc. is complete: (Induction proof, $n$- #atomic formulas) $K(M)\vdash_{\text{Res}}\emptyset\Leftrightarrow M\models\bot$: $\Rightarrow$ $K\not\vdash_{\text{Res}}\emptyset$ ↯ (IS: $A(A_{n+1})=1$ or $0$) $n=1$: $K$ unsatis. $\Leftrightarrow\exists[A_1]\exists[\neg A_1]\subseteq K$ ✓

**6.3:** $\exists x(P(x)\to\forall y(P(y)))$ is taut.: $\equiv\exists x(\neg P(x)\vee\forall y P(y))\equiv\exists x\neg P(x)\vee\forall y P(y)\equiv\neg\forall x P(x)\vee\forall y P(y)\equiv\neg\bot\vee\bot\equiv\top$ ■

**6.4:** There are $2^{(2^n)}$ different form. with $n$ atomic formulas: There are $2^n$ poss. truth assigm., formula can either evaluate to true ($\to$truth table) or false ($\to$ then false) ⇒ $2^{(2^n)}$ ■

**6.5:** $\neg\exists x\forall y(P(y,x)\leftrightarrow\neg P(y,y))$ is taut.: $\equiv\forall x\neg\forall y(P(y,x)\leftrightarrow\neg P(y,y))\equiv\forall x\exists y\neg(P(y,x)\leftrightarrow\neg P(y,y))\equiv$ (use $\neg(F\leftrightarrow G)\equiv(F\leftrightarrow G)$)
$\forall x\exists y(P(y,x)\leftrightarrow P(y,y))$, set $y=x$ and we get $F(x,x)=P(x,x)\leftrightarrow\neg P(x,x)$ since all $y$'s are $=x$, hence taut. ■

**6.6:** $(\forall xF)\wedge H\equiv\forall x(F\wedge H)$: We show $(\forall xF)\wedge H\models\forall x(F\wedge H)$ and vice versa: (1): Suppose $A$, s.t. $A((\forall xF)\wedge H)=1$
$\Rightarrow A(\forall xF)=1\wedge A(H)=1\Rightarrow A_{[x\to u]}(F)=1$ for all $u\in U$ and $A_{[x\to u]}(H)=1$ for all $u\in U\Rightarrow A_{[x\to u]}(F\wedge H)=1$ for all $u\in U\Rightarrow A(\forall x(F\wedge H))=1$ (2): Suppose $A$, s.t. $A(\forall x(F\wedge H))=1\Rightarrow A_{[x\to u]}(F\wedge H)=1$ for all $u\in U\Rightarrow A_{[x\to u]}(F)$ for all $u\in U$ and $A_{[x\to u]}(H)=1$ for all $u\in U$. Since $x$ doesn't occur free in $H\Rightarrow A_{[x\to u]}(H)=A(H)=1$ for all $u\in U\Rightarrow A\models H\Rightarrow A\models(\forall xF)\wedge H$ ■

**6.7:** $\neg(\forall xF)\equiv\exists x\neg F$: (1): Suppose $A$, s.t. $A(\neg(\forall xF))=1\Rightarrow A_{[x\to u]}(F)=1$ not for all $u\in U\Rightarrow A_{[x\to u]}(\neg F)=1$ for some $u\in U$
$\Rightarrow\exists x\neg F(x)\Rightarrow\neg(\forall xF)\models\exists x\neg F$ (2): Suppose $A(\exists x\neg F)=1\Rightarrow A_{[x\to u]}(F)=0$ for some $u\in U\Rightarrow A_{[x\to u]}(F)=1$ not for all $u\in U\Rightarrow A(\forall xF)=1$, $\not\models$

**6.8:** Replace sub-formula $G_i$ of $F$ by, to $G$ equiv. formula $H_i$ is equiv. to $F$: Argue with Interpretations $A(F)=1$

**6.9:** $\{\forall xF,\forall yG\}\models F\wedge G$?: True, suppose any $A$ suitable for $\forall xF,\forall yG$, $F\wedge G$ s.t. $A(\forall xF)=A(\forall yG)=1\Rightarrow A_{[x\to u]}(F)=A_{[y\to v]}(G)=1$ for all $u,v\in U\Rightarrow A(F)=1$ and $A(G)=1$ (since $x$ not free in $F$, $y$ not in $G$) $\Rightarrow A(F\wedge G)=1$ ■

C1: $A=\{f:\mathbb{N}\to\mathbb{N}\mid\forall n\in\mathbb{N}\,n\text{ even}\Rightarrow f(n)>f(n+1)\wedge n\text{ odd}\Rightarrow f(n)<f(n+1)\}$ countable?: If $S\subseteq A$ is uncountable, then $A$, too:
$A'\subseteq A=\{f\mid n\text{ odd}\Rightarrow f(n)=0\}$ (i.e., the functions that go back to 0 every 2nd step) For neven there funct. have $f(n)\geq 1$.
We create bijective mapping $\phi:A'\to\mathbb{N}_+^*$, $f\mapsto f(0)f(2)f(4)\ldots$ As $\phi$ is bijective, it suffices to show $\mathbb{N}_+^*$ is uncountable which can be proved with Cantor's diagonal (aka. 2nd) argument ■

C2: Set of all funct. $(0,1)\to\mathbb{N}$ is uncountable: There are uncountable $z\in(0,1)$, hence we have at least uncountable many functions $f(z)$ with $f:(0,1)\to\mathbb{N}$ $\{0,1\}\to\mathbb{N}$ countable: $f\in A$ has 2 values: $f(0)$, $f(1)$ and each of them is in $\mathbb{N}$, Hence $A\sim\mathbb{N}\times\mathbb{N}$ which is countable ■

Trick (C): If $B=A\cup C\Leftrightarrow A=B\setminus C$ and $B$ is uncountable, prove that $A$ is uncountable by showing that $C$ is countable.