Grupper

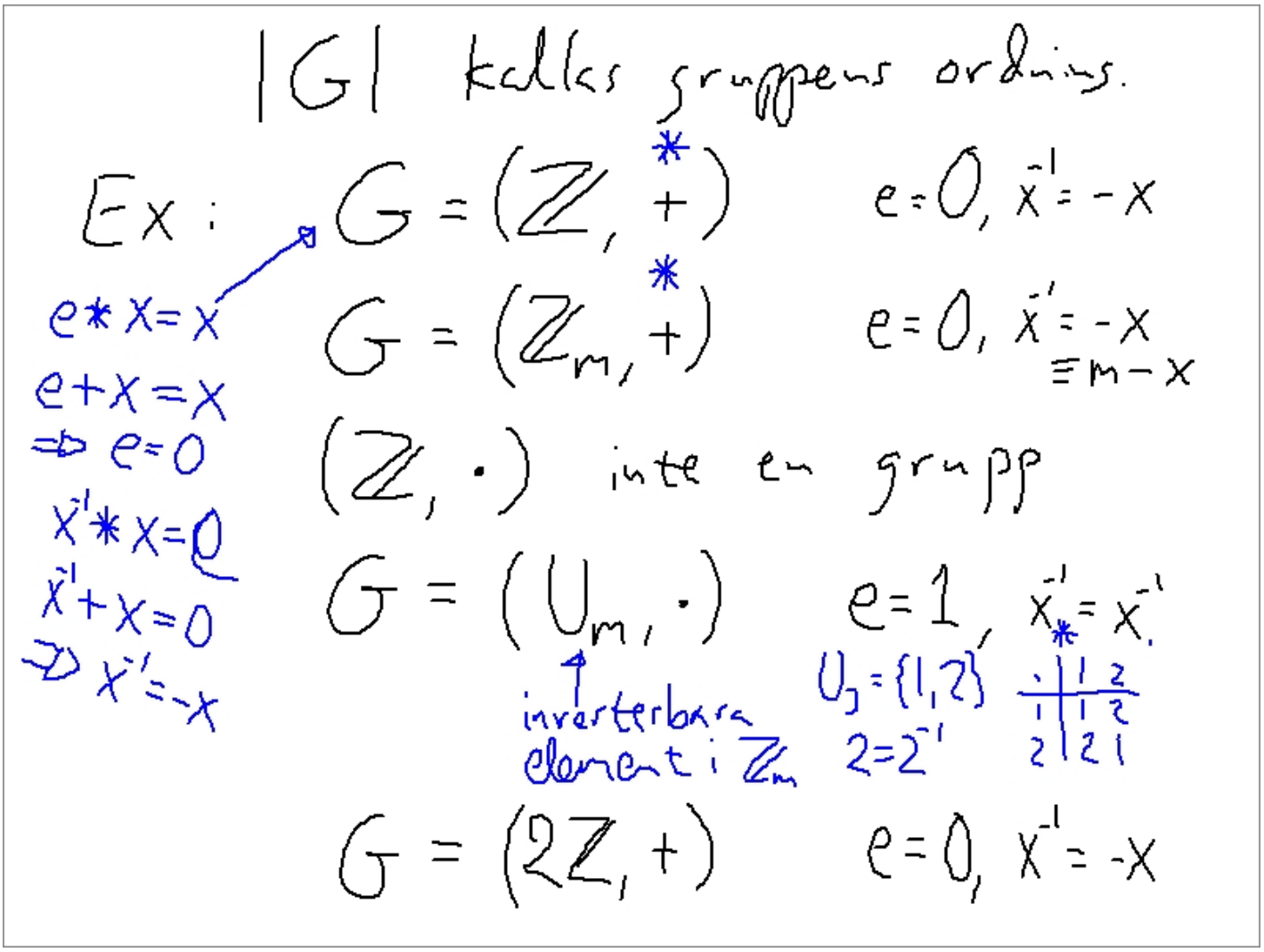
Def: En grupp är en mängd med en operation, $*$, som uppfyller axiomen:

G1: $\forall x, y \in G$ så $x * y \in G$

G2: $(x * y) * z = x * (y * z)$

G3: Det finns ett element, $e \in G$ så att $e * x = x * e = x$ för alla $x \in G$

G4: Till varje $x \in G$ så finns $x^{-1} \in G$ så att $x^{-1} * x = x * x^{-1} = e$.


|G| kallas gruppens ordning.
Ex:
$G = (\mathbb{Z}, *, +)$ $e = 0$, $x^{-1} = -x$
$G = (\mathbb{Z}_m, *, +)$ $e = 0$, $x^{-1} = -x \equiv m - x$
$e * x = x$
$e + x = x$
$\Rightarrow e = 0$
$x^{-1} * x = 0$
$x^{-1} + x = 0$
$\Rightarrow x^{-1} = -x$
$(\mathbb{Z}, \cdot)$ inte en grupp
$G = (U_m, \cdot)$ $e = 1$, $x^{-1}_* = x^{-1}$
inverterbara element i $\mathbb{Z}_m$
$U_3 = \{1, 2\}$
$2 = 2^{-1}$
$G = (2\mathbb{Z}, +)$ $e = 0$, $x^{-1} = -x$

Ex: Symmetriska gruppen, S_n

Mängden av permutationer av $1, \dots, n$ har vi betecknat S_n och med operationen sammansättning utgör den en grupp. $\pi\sigma$

G1 svarar precis mot egenskap i) i sats 3.6. $\pi, \sigma \in S_n \Rightarrow \pi\sigma \in S_n$

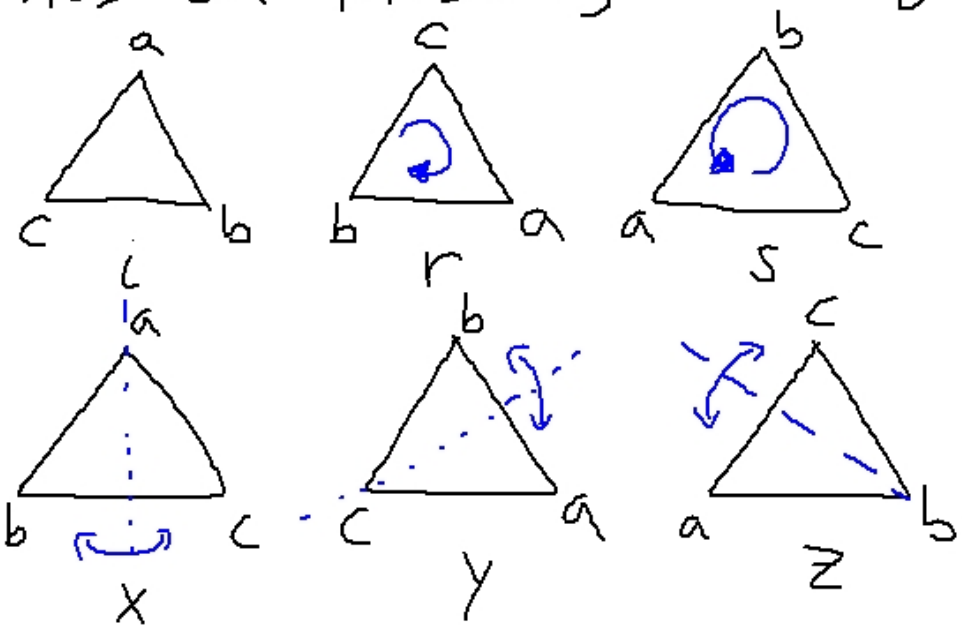
G2 $\leftrightarrow$ ii) $(\pi\sigma)\tau = \pi(\sigma\tau)$

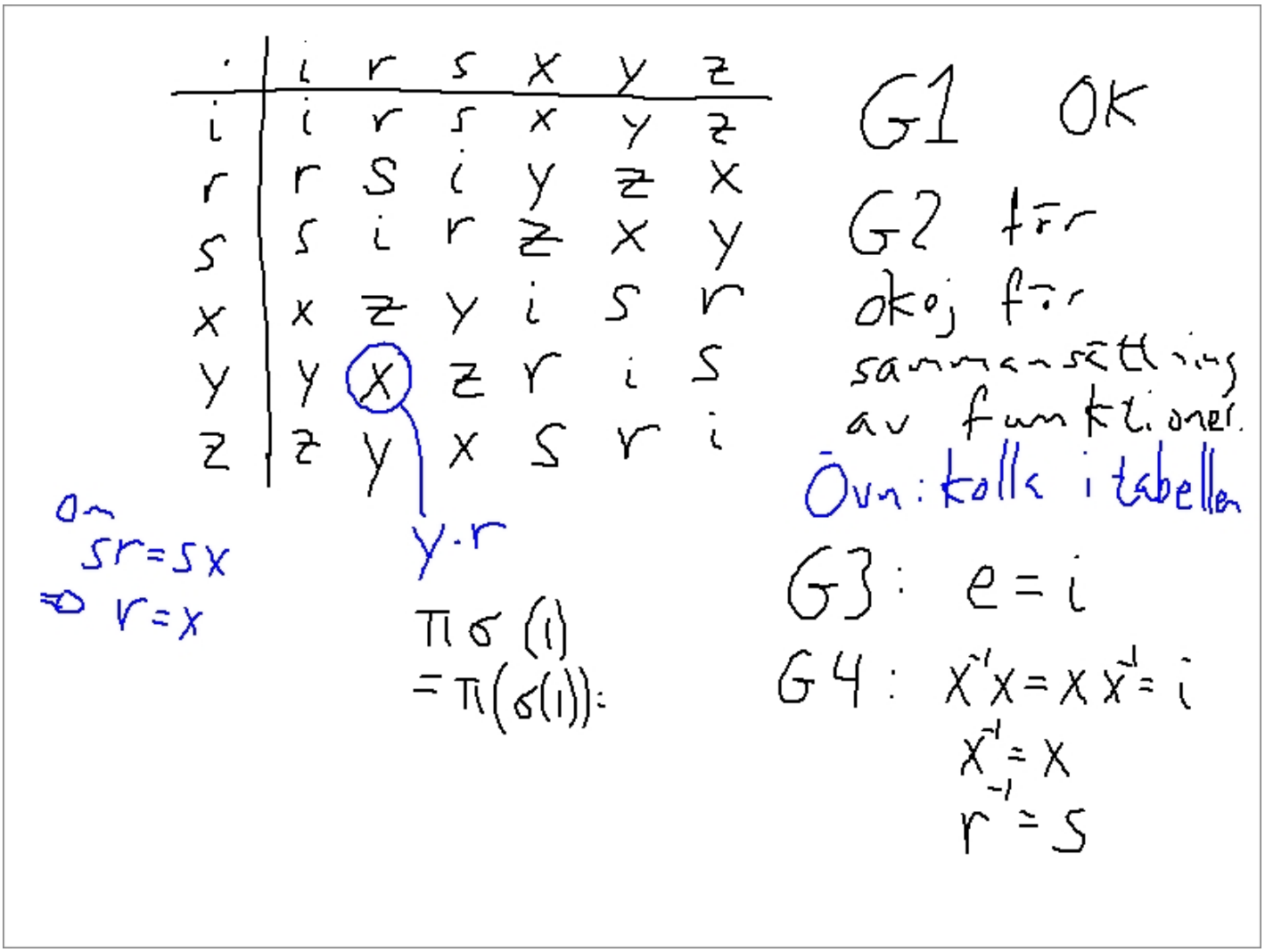
G3 $\leftrightarrow$ iii) $\mathrm{id}\,\pi = \pi\,\mathrm{id} = \pi$

G4 $\leftrightarrow$ iv) finns π^{-1}

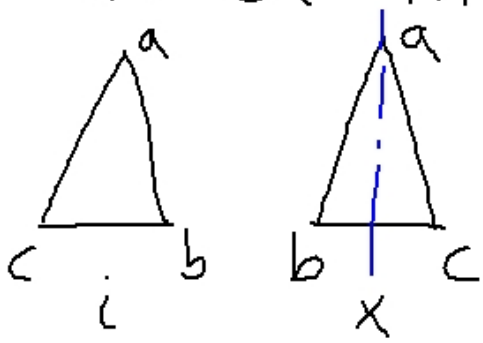
$|S_n| = n!$

Ex: G_Δ, gruppen av symmetrier hos en liksidig triangel.




·
i r s x y z
i i r s x y z
r r s i y z x
s s i r z x y
x x z y i s r
y y x z r i s
z z y x s r i
y·r
Om
sr = sx
⇒ r = x
π σ (1)
= π(σ(1))
G1 OK
G2 för
okej för
sammansättning
av funktioner.
Övn: kolla i tabellen
G3: e = i
G4: x⁻¹x = x x⁻¹ = i
x⁻¹ = x
r⁻¹ = s

Ex: Gruppen av symmetrier hos en liktbent triangel.



	i	x
i	i	x
x	x	i

isomorfa

$\cdot$	1	-1
1	1	-1
-1	-1	1

$(\{1,-1\}, \cdot)$

$\alpha(i) = 1$

$\alpha(x) = -1$

$\alpha(g \circ h) = \alpha(g) \cdot \alpha(h)$

α bijektion: $G \to H$

$g, h \in G \quad \alpha(g *_G h) = \alpha(g) *_H \alpha(h)$

Det behöver inte vara så att $x*y = y*x$, tex

$(12)(132) = (13)$

$(132)(12) = (23)$

Abelska grupper (Kommutativa grupper) är sådana där $x*y = y*x$.

Ex: $(\mathbb{Z}, +)$. I en grupp G gäller

Sats: i) $xy = xz \Rightarrow y = z$

ii) $yx = zx \Rightarrow y = z$

Bevis av i): $y = x^{-1}(xy) = x^{-1}(xz) = (x^{-1}x)z = ez = z$

$\Rightarrow$ Varje rad i en grupptabell innehåller elementen i G precis en gång och samma gäller varje kolumn.

Sats: Ekvationen $ax=b$ har en unik lösning i G. $(a,b \in G)$.

bevis: Antag att vi har två lösningar

$ax'=b$, $ax''=b \Rightarrow ax'=ax''$ $(a=x,\ x'=y,\ x''=z)$

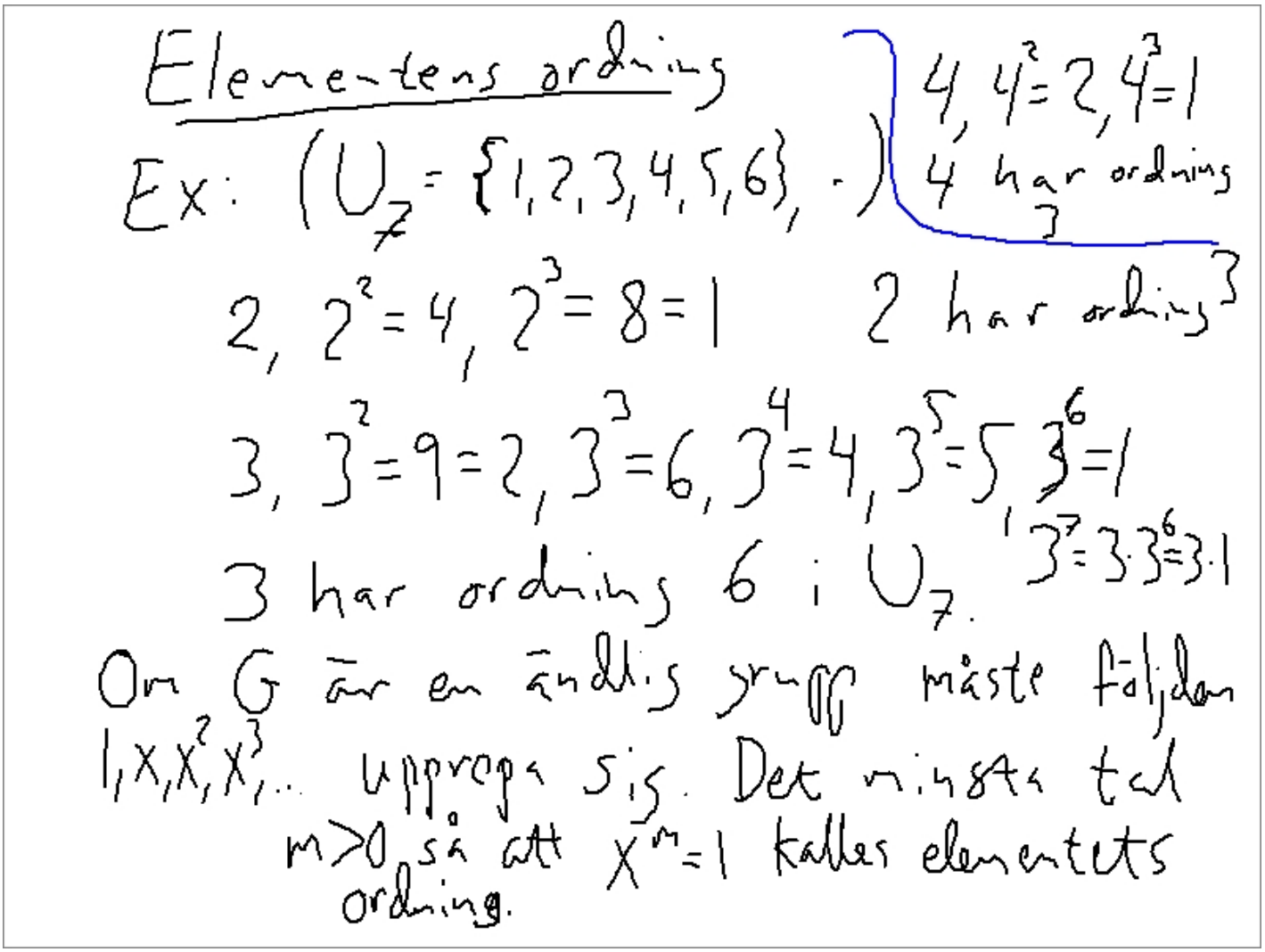
$\Rightarrow$ (enligt föregående sats) $x'=x''$

Så vi har högst en lösning. En lösning är $a^{-1}b$.

Följdsats: G har ett unikt enhetselement och varje element har en unik invers.

bevis: Sätt $b = a \Rightarrow ax = a$ har en unik lösning för alla a och e är den lösningen.

För att visa att a har en unik invers så sätter vi $b = e$. Ekvationen blir nu $ax = e$, som är precis ekvationen för inversen.


Elementens ordning
Ex: $(U_7 = \{1,2,3,4,5,6\}, \cdot)$
$4, 4^2 = 2, 4^3 = 1$
4 har ordning 3
$2, 2^2 = 4, 2^3 = 8 = 1$
2 har ordning 3
$3, 3^2 = 9 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5, 3^6 = 1$
$3^7 = 3 \cdot 3^6 = 3 \cdot 1$
3 har ordning 6 i U_7.
Om G är en ändlig grupp måste följden $1, x, x^2, x^3, \ldots$ upprepa sig. Det minsta tal $m > 0$ så att $x^m = 1$ kallas elementets ordning.

Sats: Låt x ha ordning m i G och anta att $x^s = 1$, då gäller $m \mid s$.

bevis: Om $x^s = 1$ och $s > 0$ så är $s \geq m$ (för m var det minsta sådana talet) säg $s = mq + r$, $0 \leq r < m$.

$1 = e$

Vi får $1 = x^s = x^{mq+r} = x^{mq} x^r =$

$= (x^m)^q x^r = 1 \cdot x^r = x^r$. Alltså $x^r = 1$.

Men m var det minsta talet > 0 så att

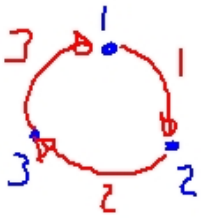
$x^m = 1 \Rightarrow r = 0. \Rightarrow m \mid s.$

Ex: $(U_8, \cdot)$ $3^2 = 9 = 1$

$5^2 = 25 = 1$ 3, 5, 7 har ordning 2

$7^2 = 49 = 1$

Ex: S_3 $(12)(12) = id$ (12) har ordning 2



$(123)^3 = id$ (123) har ordning 3