Cayley-Tables

$G = \{a_1, \ldots, a_n\}$ (distinct elements) binary operation $* \mid a*b = ab$

	a_1	a_2	$\cdots$	a_j	$\cdots$	a_k	$\cdots$	a_n
a_1	a_1a_1	a_1a_2		a_1a_j		a_1a_k		a_1a_n
$\vdots$								
a_i	a_ia_1	a_ia_2		a_ia_j		a_ia_k		
$\vdots$								
a_n	a_na_1			a_na_j				a_na_n

Cancellation law (1.13a) $\Rightarrow$ elements in each row and column are distinct

$\left[\begin{array}{l} a_ia_j = a_ia_k \Rightarrow a_j = a_k \\ a_ja_i = a_ka_i \Rightarrow a_j = a_k \end{array}\right] \Rightarrow$ in each row (respective columns) there are n distinct elements.

$\Rightarrow$ each element turns up exactly once in each row and each column.

Convention: $a_1 = e$. Can build 'small' groups from Cayley-table.

Examples: a) $|G| = 1$ $G = \{e\}$

e	e

i group of order 1 – call it TRIVIAL GROUP.

b) $|G| = 2$ $G = \{e, a\}$

	e	a
e	e	a
a	a	e

$\Rightarrow a^2 = e$

again no choice $\Rightarrow$ essentially 1 group of order 2.

c) $|G| = 3$ $G = \{e, a, b\}$

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

$aa = \begin{cases} e \\ b \end{cases}$ Suppose $aa = e$

$\Rightarrow ab = b \Leftrightarrow ab = eb \Rightarrow a = e$ ↯

(each element turns up once in each row) Hence $aa \neq b$ and then 'fill up' table. Again no choice $\Rightarrow$ essentially one group of order 3

$G = \{e, a, b\}$ as above $G = \left(\left\{\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}, \begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}, \begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}\right\}, \circ\right)$ A_3.

d) $|G| = 4$ $G = \{e, a, b, c\}$

2 cases: i) each element is its own inverse i.e. $a^2 = b^2 = c^2 = e$

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

ii) $\exists$ element, say a s.t. $a^{-1} \neq a$

	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

in case i) $ab = \begin{cases} b \Rightarrow a = e$ ↯ (see above) \\ c$ ✓ \end{cases}$ $ba = \begin{cases} b \Rightarrow a = e$ ↯ \\ c$ ✓ \end{cases}$ 'fill up'

this is Klein's 4-group e.g. this is the group of symmetries of rectangle.

ii) wlog $a^{-1} = b \Rightarrow ab = ba = e$ as above $ac \neq c$ $(a \neq e)$

$ac \neq a$ $(c \neq e) \Rightarrow ac = b$

Similarly $ca = b \Rightarrow aa = c \Rightarrow cc = e$

$(cb \neq e$ as we already have a in 3rd column)

$(\{1, -1, i, -i\}, \cdot)$, $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ essentially 2 different groups of order 4.

$\mathbb{C}$

§2 - CONGRUENCES.

for this chapter $* = +$ 'All about integers'.

Proposition 2.1 $(\mathbb{Z}, +)$ is an abelian group $(\mathbb{Z}, +)$ infinite.

Definition 2.2 let $m > 0$ be a positive integer. Then $a, b \in \mathbb{Z}$ are congruent modulo m. $a \equiv b \pmod{m}$ if m divides $(a-b)$ $[m \mid (a-b)]$

Remark $a \equiv b \pmod{m}$ is an equivalence relation

i) $a \equiv a \pmod{m}$ as $m \mid 0 = (a-a)$

ii) $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$ as $m \mid (a-b) \Rightarrow m \mid (b-a)$.

iii) $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$

$\Downarrow$ $\Downarrow$

$\exists x \in \mathbb{Z}$ s.t. $mx = a-b$ $\exists y \in \mathbb{Z}$ s.t. $my = b-c$ $a-c = a-b+b-c$

$= mx+my = m(x+y)$.

$\Rightarrow \mathbb{Z}$ splits up into equivalence classes - congruence classes modulo m

$\forall a \in \mathbb{Z}$ $[a] = [a]_m = \{a+qn \mid q \in \mathbb{Z}\}$.

$$\mathbb{Z} = \bigcup_{a \in \mathbb{Z}} [a]_m \sim \text{disjoint union}$$

$[a]_m$ uniquely determined.