# about groups

# 4 Groups

## 4.1 basic definitions

**group**

- $G = (S, \circ)$

$$S \text{ set },\ \circ : S \times S \to S$$

- identity

$$\exists e \in S.\ \forall a \in S. \quad e \circ a = a \circ e = e$$

- associativity

$$(a \circ b) \circ c = a \circ (b \circ c)$$

- inverse elements

$$\forall a \in S.\ \exists \text{ unique } b \in S. \quad a \circ b = b \circ a = e$$

  The inverse of $a$ is often denoted by $a^{-1}$.

- group is *abelian* if commutative law holds

$$a \circ b = b \circ a$$

# 4 Groups

## 4.1 basic definitions

**group**

- $G = (S, \circ)$

$$S \text{ set} \ , \ \circ : S \times S \to S$$

- identity

$$\exists e \in S. \, \forall a \in S. \quad e \circ a = a \circ e = e$$

- associativity

$$(a \circ b) \circ c = a \circ (b \circ c)$$

- inverse elements

$$\forall a \in S. \, \exists \text{ unique } b \in S. \quad a \circ b = b \circ a = e$$

  The inverse of $a$ is often denoted by $a^{-1}$.

- group is *abelian* if commutative law holds

$$a \circ b = b \circ a$$

## 4.2 group for modular addition

$$(\mathbb{Z}_n, +_n) \ , \ \mathbb{Z}_n = [0 : n-1] \ , \ a +_n b = (a+b) \bmod n$$

- neutral element:

$$e = 0$$

- inverse of $a$

$$-a = n - a$$

$$(a + (n-a)) \bmod n = n \bmod n = 0$$

- abelian

### 4.3 group for modular multiplication

$$(Z_n^*, \cdot_n)\ ,\ a \cdot_n b = a \cdot b \bmod n$$

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \ :\ gcd(a,n) = 1\}$$

## 4.3 group for modular multiplication

$$(Z_n^*, \cdot_n)\ ,\ a \cdot_n b = a \cdot b \bmod n$$

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \ : \ gcd(a,n) = 1\}$$

- abelian (if it is a group)
- neutral element

$$e = 1$$

- $\cdot_n : \mathbb{Z}_n^* \times \mathbb{Z}_n^* \to \mathbb{Z}_n^*$

$$a,b \in \mathbb{Z}_n^* \ \to gcd(a,n) = gcd(b.n) = 1$$

$$\begin{aligned}
gcd(ab,n) &= 1 \quad \text{(lemma 3)} \\
\exists x,y \in Z : 1\ abx + ny &= 1 \quad \text{(lemma 1)} \\
q &= \lfloor ab/n \rfloor \\
1 &= abx - qnx + qnx + ny \\
&= (ab - qn)x + n(qx + y) \\
&= (ab \bmod n) + n(qx + y) \\
gcd(ab \bmod n, n) &= 1 \quad \text{(lemma 1)}
\end{aligned}$$

### 4.3 group for modular multiplication

$$(Z_n^*, \cdot_n)\ ,\ a \cdot_n b = a \cdot b \bmod n$$

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n\ :\ gcd(a,n) = 1\}$$

- abelian (if it is a group)
- neutral element

$$e = 1$$

- $\cdot_n : \mathbb{Z}_n^* \times \mathbb{Z}_n^* \to \mathbb{Z}_n^*$

$$a, b \in \mathbb{Z}_n^* \ \to gcd(a,n) = gcd(b.n) = 1$$

$$\begin{aligned}
gcd(ab,n) &= 1 \quad \text{(lemma 3)} \\
\exists x, y \in Z : 1\ abx + ny &= 1 \quad \text{(lemma 1)} \\
q &= \lfloor ab/n \rfloor \\
1 &= abx - qnx + qnx + ny \\
&= (ab - qn)x + n(qx + y) \\
&= (ab \bmod n) + n(qx + y) \\
gcd(ab \bmod n, n) &= 1 \quad \text{(lemma 1)}
\end{aligned}$$

- inverse of $a$

$$\begin{aligned}
gcd(a,n) &= 1 \\
\exists x, y \in Z :\ ax + ny &= 1 \quad \text{(lemma 1)} \\
ax &\equiv 1 \bmod n \\
a \cdot_n x &= 1
\end{aligned}$$

## 4.3 group for modular multiplication

$$(Z_n^*, \cdot_n) \ , \ a \cdot_n b = a \cdot b \bmod n$$

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \ : \ gcd(a,n) = 1\}$$

- abelian (if it is a group)
- neutral element

$$e = 1$$

- $\cdot_n : \mathbb{Z}_n^* \times \mathbb{Z}_n^* \to \mathbb{Z}_n^*$

$$a, b \in \mathbb{Z}_n^* \ \to gcd(a,n) = gcd(b.n) = 1$$

$$\begin{aligned}
gcd(ab,n) &= 1 \quad \text{(lemma 3)} \\
\exists x, y \in Z : 1\ abx + ny &= 1 \quad \text{(lemma 1)} \\
q &= \lfloor ab/n \rfloor \\
1 &= abx - qnx + qnx + ny \\
&= (ab - qn)x + n(qx + y) \\
&= (ab \bmod n) + n(qx + y) \\
gcd(ab \bmod n, n) &= 1 \quad \text{(lemma 1)}
\end{aligned}$$

- inverse of $a$

$$\begin{aligned}
gcd(a,n) &= 1 \\
\exists x, y \in Z : \ ax + ny &= 1 \quad \text{(lemma 1)} \\
ax &\equiv 1 \bmod n \\
a \cdot_n x &= 1
\end{aligned}$$

- uniqueness of inverse: later (lemma 23)

# 5 Euler's $\varphi$-function

$$\varphi(n) = |\mathbb{Z}_n^*| \quad \text{cardinality, number of elements)}$$

**Lemma 6.**

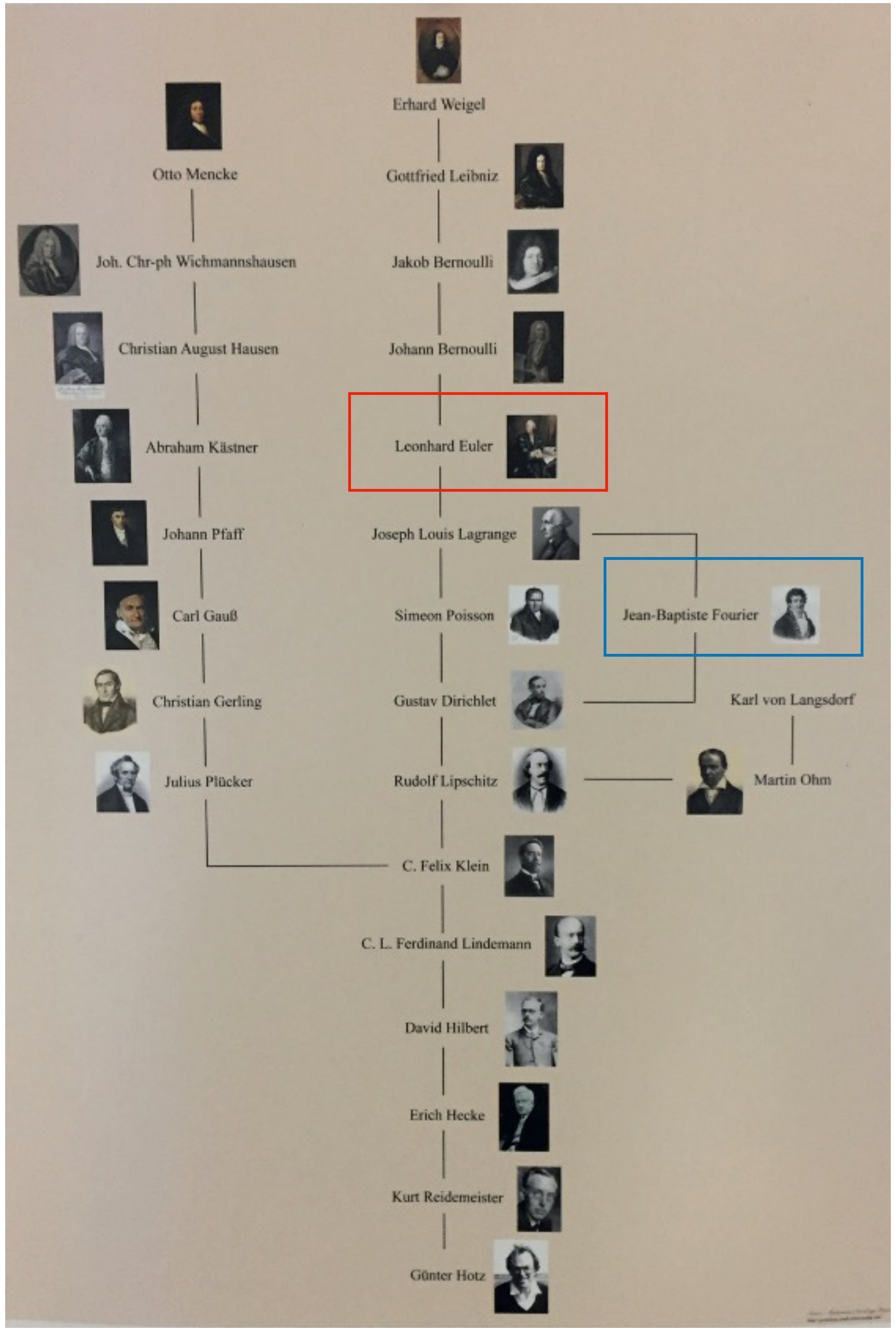
$$gcd(n,m) = 1 \rightarrow \varphi(nm) = \varphi(n) \cdot \varphi(m)$$

## 5 Euler's $\varphi$-function

$\varphi(n) = |\mathbb{Z}_n^*|$ cardinality, number of elements)

**Lemma 6.**

$$gcd(n,m) = 1 \to \varphi(nm) = \varphi(n) \cdot \varphi(m)$$




# 5 Euler's $\varphi$-function

$$\varphi(n) = |\mathbb{Z}_n^*| \quad \text{cardinality, number of elements)}$$

**Lemma 6.**

$$gcd(n,m) = 1 \to \varphi(nm) = \varphi(n) \cdot \varphi(m)$$

*Proof.* transscribed from a *great (!!)* YouTube video of Michael Penn. However a few details were added, because in the video only $\varphi(nm) \geq \varphi(n) \cdot \varphi(m)$ is shown, and one has also to show, that the elements outside the identified set are not in $\mathbb{Z}_{mn}^*$. Arrange elements of

$$\mathbb{Z}_{mn} = \{\ell m + k \;:\; k \in \mathbb{Z}_m \;,\; \ell \in \mathbb{Z}_n\}$$

in an $n \times m$-table as shown in table 2.

| | | ... | C(k) | ... | |
|---|---|---|---|---|---|
| 0 | 1 | ... | k | ... | m-1 |
| m | m+1 | ... | m+k | ... | 2m-1 |
| $\vdots$ | | | | | $\vdots$ |
| $m\ell$ | $m\ell+1$ | ... | $m\ell+k$ | ... | $m(\ell+1)-1$ |
| $\vdots$ | | | | | $\vdots$ |
| $m(n-1)$ | | | $m(n-1)+k$ | | mn-1 |

Table 2: Arranging $\mathbb{Z}_{mn}$ in a table of $n$ rows and $m$ columns

For $k \in \mathbb{Z}_m$ collect elements in column $k$ into the set

$$C(k) = \{m\ell + k \;:\; \ell \in \mathbb{Z}_n\}$$

# 5 Euler's $\varphi$-function

$$\varphi(n) = |\mathbb{Z}_n^*| \quad \text{cardinality, number of elements)}$$

**Lemma 6.**

$$gcd(n,m) = 1 \to \varphi(nm) = \varphi(n) \cdot \varphi(m)$$

*Proof.* transscribed from a *great (!!)* YouTube video of Michael Penn. However a few details were added, because in the video only $\varphi(nm) \geq \varphi(n) \cdot \varphi(m)$ is shown, and one has also to show, that the elements outside the identified set are not in $\mathbb{Z}_{mn}^*$. Arrange elements of

$$\mathbb{Z}_{mn} = \{\ell m + k \;:\; k \in \mathbb{Z}_m \;,\; \ell \in \mathbb{Z}_n\}$$

in an $n \times m$-table as shown in table 2.

| | | ... | C(k) | ... | |
|---|---|---|---|---|---|
| 0 | 1 | ... | k | ... | m-1 |
| m | m+1 | ... | m+k | ... | 2m-1 |
| $\vdots$ | | | | | $\vdots$ |
| $m\ell$ | $m\ell+1$ | ... | $m\ell+k$ | ... | $m(\ell+1)-1$ |
| $\vdots$ | | | | | $\vdots$ |
| $m(n-1)$ | | | $m(n-1)+k$ | | mn-1 |

Table 2: Arranging $\mathbb{Z}_{mn}$ in a table of $n$ rows and $m$ columns

For $k \in \mathbb{Z}_m$ collect elements in column $k$ into the set

$$C(k) = \{m\ell + k \;:\; \ell \in \mathbb{Z}_n\}$$

- For elements $a = m\ell + k \in C(k)$

$$\begin{aligned} gcd(a,m) &= gcd(m\ell+k,m) \\ &= gcd(m, m\ell+k \text{ mod } m) \quad \text{(lemma 4 )} \\ &= gcd(m,k) \end{aligned}$$

# 5 Euler's $\varphi$-function

$$\varphi(n) = |\mathbb{Z}_n^*| \quad \text{cardinality, number of elements)}$$

**Lemma 6.**

$$gcd(n,m) = 1 \to \varphi(nm) = \varphi(n) \cdot \varphi(m)$$

*Proof.* transscribed from a *great (!!)* YouTube video of Michael Penn. However a few details were added, because in the video only $\varphi(nm) \geq \varphi(n) \cdot \varphi(m)$ is shown, and one has also to show, that the elements outside the identified set are not in $\mathbb{Z}_{mn}^*$. Arrange elements of

$$\mathbb{Z}_{mn} = \{\ell m + k \ : \ k \in \mathbb{Z}_m \ , \ \ell \in \mathbb{Z}_n\}$$

in an $n \times m$-table as shown in table 2.

| | | ... | C(k) | ... | |
|---|---|---|---|---|---|
| 0 | 1 | ... | k | ... | m-1 |
| m | m+1 | ... | m+k | ... | 2m-1 |
| $\vdots$ | | | | | $\vdots$ |
| $m\ell$ | $m\ell+1$ | ... | $m\ell+k$ | ... | $m(\ell+1)-1$ |
| $\vdots$ | | | | | $\vdots$ |
| $m(n-1)$ | | | $m(n-1)+k$ | | mn-1 |

Table 2: Arranging $\mathbb{Z}_{mn}$ in a table of $n$ rows and $m$ columns

For $k \in \mathbb{Z}_m$ collect elements in column $k$ into the set

$$C(k) = \{m\ell + k \ : \ \ell \in \mathbb{Z}_n\}$$

- For elements $a = m\ell + k \in C(k)$

$$\begin{aligned} gcd(a,m) &= gcd(m\ell+k,m) \\ &= gcd(m, m\ell+k \bmod m) \quad \text{(lemma 4 )} \\ &= gcd(m,k) \end{aligned}$$

- For $k \notin \mathbb{Z}_m^*$ and element $a = m\ell + k \in C(k)$

$$1 < gcd(k,m) = gcd(a,m) \leq gcd(a,mn) \ , \ a \notin \mathbb{Z}_{mn}^*$$

$$\mathbb{Z}_{mn}^* \subseteq \bigcup_{k \in \mathbb{Z}_m^*} C(k)$$

This excludes elements outside of $\varphi(m)$ columns.

# 5 Euler's $\varphi$-function

$$\varphi(n) = |\mathbb{Z}_n^*| \quad \text{cardinality, number of elements)}$$

**Lemma 6.**

$$gcd(n,m) = 1 \to \varphi(nm) = \varphi(n) \cdot \varphi(m)$$

*Proof.* transscribed from a *great (!!)* YouTube video of Michael Penn. However a few details were added, because in the video only $\varphi(nm) \geq \varphi(n) \cdot \varphi(m)$ is shown, and one has also to show, that the elements outside the identified set are not in $\mathbb{Z}_{mn}^*$. Arrange elements of

$$\mathbb{Z}_{mn} = \{\ell m + k \ : \ k \in \mathbb{Z}_m \ , \ \ell \in \mathbb{Z}_n\}$$

in an $n \times m$-table as shown in table 2.

| | | ... | C(k) | ... | |
|---|---|---|---|---|---|
| 0 | 1 | ... | k | ... | m-1 |
| m | m+1 | ... | m+k | ... | 2m-1 |
| $\vdots$ | | | | | $\vdots$ |
| $m\ell$ | $m\ell+1$ | ... | $m\ell+k$ | ... | $m(\ell+1)-1$ |
| $\vdots$ | | | | | $\vdots$ |
| $m(n-1)$ | | | $m(n-1)+k$ | | mn-1 |

Table 2: Arranging $\mathbb{Z}_{mn}$ in a table of $n$ rows and $m$ columns

For $k \in \mathbb{Z}_m$ collect elements in column $k$ into the set

$$C(k) = \{m\ell + k \ : \ \ell \in \mathbb{Z}_n\}$$

- For elements $a = m\ell + k \in C(k)$

$$\begin{aligned} gcd(a,m) &= gcd(m\ell+k, m) \\ &= gcd(m, m\ell+k \bmod m) \quad \text{(lemma 4 )} \\ &= gcd(m,k) \end{aligned}$$

- For $k \notin \mathbb{Z}_m^*$ and element $a = m\ell + k \in C(k)$

$$1 < gcd(k,m) = gcd(a,m) \leq gcd(a,mn) \ , \ a \notin \mathbb{Z}_{mn}^*$$

$$\mathbb{Z}_{mn}^* \subseteq \bigcup_{k \in \mathbb{Z}_m^*} C(k)$$

This excludes elements outside of $\varphi(m)$ columns.

- For $k \in \mathbb{Z}_m^*$ , $a \in C(k)$

$$gcd(a,m) = gcd(a,k) = 1$$

# 5 Euler's $\varphi$-function

$$\varphi(n) = |\mathbb{Z}_n^*| \quad \text{cardinality, number of elements)}$$

**Lemma 6.**

$$gcd(n,m) = 1 \rightarrow \varphi(nm) = \varphi(n) \cdot \varphi(m)$$

*Proof.* transscribed from a *great (!!)* YouTube video of Michael Penn. However a few details were added, because in the video only $\varphi(nm) \geq \varphi(n) \cdot \varphi(m)$ is shown, and one has also to show, that the elements outside the identified set are not in $\mathbb{Z}_{mn}^*$. Arrange elements of

$$\mathbb{Z}_{mn} = \{\ell m + k \;:\; k \in \mathbb{Z}_m \;,\; \ell \in \mathbb{Z}_n\}$$

in an $n \times m$-table as shown in table 2.

| | | ... | C(k) | ... | |
|---|---|---|---|---|---|
| 0 | 1 | ... | k | ... | m-1 |
| m | m+1 | ... | m+k | ... | 2m-1 |
| $\vdots$ | | | | | $\vdots$ |
| $m\ell$ | $m\ell+1$ | ... | $m\ell+k$ | ... | $m(\ell+1)-1$ |
| $\vdots$ | | | | | $\vdots$ |
| $m(n-1)$ | | | $m(n-1)+k$ | | mn-1 |

Table 2: Arranging $\mathbb{Z}_{mn}$ in a table of $n$ rows and $m$ columns

For $k \in \mathbb{Z}_m$ collect elements in column $k$ into the set

$$C(k) = \{m\ell + k \;:\; \ell \in \mathbb{Z}_n\}$$

- For elements $a = m\ell + k \in C(k)$

$$\begin{aligned} gcd(a,m) &= gcd(m\ell+k,m) \\ &= gcd(m, m\ell+k \bmod m) \quad \text{(lemma 4 )} \\ &= gcd(m,k) \end{aligned}$$

- For $k \notin \mathbb{Z}_m^*$ and element $a = m\ell + k \in C(k)$

$$1 < gcd(k,m) = gcd(a,m) \leq gcd(a,mn) \;,\; a \notin \mathbb{Z}_{mn}^*$$

$$\mathbb{Z}_{mn}^* \subseteq \bigcup_{k \in \mathbb{Z}_m^*} C(k)$$

This excludes elements outside of $\varphi(m)$ columns.

- For $k \in \mathbb{Z}_m^* \;,\; a \in C(k)$

$$gcd(a,m) = gcd(a,k) = 1$$

- For $k \in \mathbb{Z}_m^*$ and elements $m\ell + k, m\ell' + k \in C(k)$ solve

$$\begin{aligned} m\ell + k &\equiv m\ell' + k \bmod n \\ m(\ell - \ell') &\equiv 0 \bmod n \quad \text{(subtracting right hand side)} \\ n &\mid (\ell - \ell') \quad \text{(because } n \nmid m) \\ \ell &= \ell' \quad (\ell - \ell' \in [-n+1 : n-1]) \end{aligned}$$

| | | ... | C(k) | ... | |
|---|---|---|---|---|---|
| 0 | 1 | ... | k | ... | m-1 |
| m | m+1 | ... | m+k | ... | 2m-1 |
| $\vdots$ | | | | | $\vdots$ |
| $m\ell$ | $m\ell+1$ | ... | $m\ell+k$ | ... | $m(\ell+1)-1$ |
| $\vdots$ | | | | | $\vdots$ |
| $m(n-1)$ | | | $m(n-1)+k$ | | mn-1 |

Table 2: Arranging $\mathbb{Z}_{mn}$ in a table of $n$ rows and $m$ columns

- For elements $a = m\ell + k \in C(k)$

$$\begin{aligned} gcd(a,m) &= gcd(m\ell+k,m) \\ &= gcd(m, m\ell+k \bmod m) \quad \text{(lemma 4 )} \\ &= gcd(m,k) \end{aligned}$$

- For $k \notin \mathbb{Z}_m^*$ and element $a = m\ell + k \in C(k)$

$$1 < gcd(k,m) = gcd(a,m) \le gcd(a,mn) \ , \ a \notin \mathbb{Z}_{mn}^*$$

$$\mathbb{Z}_{mn}^* \subseteq \bigcup_{k \in \mathbb{Z}_m^*} C(k)$$

This excludes elements outside of $\varphi(m)$ columns.

- For $k \in \mathbb{Z}_m^*$ , $a \in C(k)$

$$gcd(a,m) = gcd(a,k) = 1$$

- For $k \in \mathbb{Z}_m^*$ and elements $m\ell + k, m\ell' + k \in C(k)$ solve

$$\begin{aligned} m\ell + k &\equiv m\ell' + k \bmod n \\ m(\ell - \ell') &\equiv 0 \mod n \quad \text{(subtracting right hand side)} \\ n &\mid (\ell - \ell') \quad \text{(because } n \nmid m\text{)} \\ \ell &= \ell' \quad (\ell - \ell' \in [-n+1 : n-1]) \end{aligned}$$

| | | ... | C(k) | ... | |
|---|---|---|---|---|---|
| 0 | 1 | ... | k | ... | m-1 |
| m | m+1 | ... | m+k | ... | 2m-1 |
| $\vdots$ | | | | | $\vdots$ |
| $m\ell$ | $m\ell+1$ | ... | $m\ell+k$ | ... | $m(\ell+1)-1$ |
| $\vdots$ | | | | | $\vdots$ |
| $m(n-1)$ | | | $m(n-1)+k$ | | mn-1 |

Table 2: Arranging $\mathbb{Z}_{mn}$ in a table of $n$ rows and $m$ columns

- For elements $a = m\ell + k \in C(k)$

$$\begin{aligned} gcd(a,m) &= gcd(m\ell+k,m) \\ &= gcd(m, m\ell+k \bmod m) \quad \text{(lemma 4 )} \\ &= gcd(m,k) \end{aligned}$$

- For $k \notin \mathbb{Z}_m^*$ and element $a = m\ell + k \in C(k)$

$$1 < gcd(k,m) = gcd(a,m) \leq gcd(a,mn)\ ,\ a \notin \mathbb{Z}_{mn}^*$$

$$\mathbb{Z}_{mn}^* \subseteq \bigcup_{k \in \mathbb{Z}_m^*} C(k)$$

This excludes elements outside of $\varphi(m)$ columns.

- For $k \in \mathbb{Z}_m^*$ , $a \in C(k)$

$$gcd(a,m) = gcd(a,k) = 1$$

- For $k \in \mathbb{Z}_m^*$ and elements $m\ell + k, m\ell' + k \in C(k)$ solve

$$\begin{aligned} m\ell + k &\equiv m\ell' + k \bmod n \\ m(\ell - \ell') &\equiv 0 \mod n \quad \text{(subtracting right hand side)} \\ n &\mid (\ell - \ell') \quad (\text{because } n \nmid m) \\ \ell &= \ell' \quad (\ell - \ell' \in [-n+1 : n-1]) \end{aligned}$$

- now a counting argument

$$C'(k) = \{m\ell + k \bmod n\ :\ \ell \in \mathbb{Z}_n\} \subseteq \mathbb{Z}_n$$

as elements in $C'(k)$ are mutually distinct

$$|C'(k)| = n\ ,\ C'(k) = \mathbb{Z}_n$$

| | | ... | C(k) | ... | |
|---|---|---|---|---|---|
| 0 | 1 | ... | k | ... | m-1 |
| m | m+1 | ... | m+k | ... | 2m-1 |
| $\vdots$ | | | | | $\vdots$ |
| $m\ell$ | $m\ell+1$ | ... | $m\ell+k$ | ... | $m(\ell+1)-1$ |
| $\vdots$ | | | | | $\vdots$ |
| $m(n-1)$ | | | $m(n-1)+k$ | | mn-1 |

Table 2: Arranging $\mathbb{Z}_{mn}$ in a table of $n$ rows and $m$ columns

- For elements $a = m\ell + k \in C(k)$

$$\begin{aligned} gcd(a,m) &= gcd(m\ell+k,m) \\ &= gcd(m, m\ell+k \text{ mod } m) \quad \text{(lemma 4 )} \\ &= gcd(m,k) \end{aligned}$$

- For $k \notin \mathbb{Z}_m^*$ and element $a = m\ell + k \in C(k)$

$$1 < gcd(k,m) = gcd(a,m) \leq gcd(a,mn) \ , \ a \notin \mathbb{Z}_{mn}^*$$

$$\mathbb{Z}_{mn}^* \subseteq \bigcup_{k \in \mathbb{Z}_m^*} C(k)$$

This excludes elements outside of $\varphi(m)$ columns.

- For $k \in \mathbb{Z}_m^*$ , $a \in C(k)$

$$gcd(a,m) = gcd(a,k) = 1$$

- For $k \in \mathbb{Z}_m^*$ and elements $m\ell+k, m\ell'+k \in C(k)$ solve

$$\begin{aligned} m\ell+k &\equiv m\ell'+k \text{ mod } n \\ m(\ell-\ell') &\equiv 0 \text{ mod } n \quad \text{(subtracting right hand side)} \\ n &\mid (\ell-\ell') \quad \text{(because } n \not| m) \\ \ell &= \ell' \quad (\ell-\ell' \in [-n+1 : n-1]) \end{aligned}$$

- now a counting argument

$$C'(k) = \{m\ell + k \text{ mod } n \ : \ \ell \in \mathbb{Z}_n\} \subseteq \mathbb{Z}_n$$

as elements in $C'(k)$ are mutually distinct

$$|C'(k)| = n \ , \ C'(k) = \mathbb{Z}_n$$

- for $\ell m + k \text{ mod } n \notin \mathbb{Z}_n^*$

$$\begin{aligned} 1 &< gcd(m\ell+k \text{ mod } n, n) \\ &= gcd(m\ell+k, n) \quad \text{(lemma 4 )} \\ &\leq gcd(m\ell+k, nm) \\ m\ell+k &\notin \mathbb{Z}_{mn}^* \end{aligned}$$

This excludes $n-\varphi(n)$ elements in each of the remaining $\varphi(m)$ columns.

| | | ... | C(k) | ... | |
|---|---|---|---|---|---|
| 0 | 1 | ... | k | ... | m-1 |
| m | m+1 | ... | m+k | ... | 2m-1 |
| $\vdots$ | | | | | $\vdots$ |
| $m\ell$ | $m\ell+1$ | ... | $m\ell+k$ | ... | $m(\ell+1)-1$ |
| $\vdots$ | | | | | $\vdots$ |
| $m(n-1)$ | | | $m(n-1)+k$ | | mn-1 |

Table 2: Arranging $\mathbb{Z}_{mn}$ in a table of $n$ rows and $m$ columns

- For elements $a = m\ell + k \in C(k)$

$$\begin{aligned} gcd(a,m) &= gcd(m\ell+k,m) \\ &= gcd(m, m\ell+k \bmod m) \quad \text{(lemma 4 )} \\ &= gcd(m,k) \end{aligned}$$

- For $k \notin \mathbb{Z}_m^*$ and element $a = m\ell + k \in C(k)$

$$1 < gcd(k,m) = gcd(a,m) \leq gcd(a,mn) \ , \ a \notin \mathbb{Z}_{mn}^*$$

$$\mathbb{Z}_{mn}^* \subseteq \bigcup_{k \in \mathbb{Z}_m^*} C(k)$$

This excludes elements outside of $\varphi(m)$ columns.

- For $k \in \mathbb{Z}_m^*$ , $a \in C(k)$

$$gcd(a,m) = gcd(a,k) = 1$$

- For $k \in \mathbb{Z}_m^*$ and elements $m\ell + k, m\ell' + k \in C(k)$ solve

$$\begin{aligned} m\ell + k &\equiv m\ell' + k \bmod n \\ m(\ell - \ell') &\equiv 0 \mod n \quad \text{(subtracting right hand side)} \\ n &\mid (\ell - \ell') \quad \text{(because } n \not| m) \\ \ell &= \ell' \quad (\ell - \ell' \in [-n+1 : n-1]) \end{aligned}$$

- now a counting argument

$$C'(k) = \{m\ell + k \bmod n \ : \ \ell \in \mathbb{Z}_n\} \subseteq \mathbb{Z}_n$$

as elements in $C'(k)$ are mutually distinct

$$|C'(k)| = n \ , \ C'(k) = \mathbb{Z}_n$$

- for $\ell m + k \bmod n \in \mathbb{Z}_n^*$

$$\begin{aligned} 1 &= gcd(m\ell + k \bmod n, n) \\ &= gcd(m\ell + k, n) \quad \text{(lemma 4 )} \\ 1 &= gcd(m\ell + k, m) \quad \text{(shown above for } k \in \mathbb{Z}_m^*) \\ 1 &= gcd(m\ell + k, mn) \quad \text{(lemma 3)} \\ m\ell + k &\in \mathbb{Z}_{mn}^* \end{aligned}$$

This identifies $\varphi(n)$ elements in each of the remaining $\varphi(m)$ columns as elements of $\mathbb{Z}_{mn}^*$.

# 5 Euler's $\varphi$-function

**powers of primes:**

**Lemma 7.**
$$n = p^k \ , \ p \ prime \quad \rightarrow \quad \varphi(n) = n(1 - \frac{1}{p})$$

*Proof.*
$$\begin{aligned} F &= \{a \in \mathbb{Z}_n \ : \ gcd(a,n) > 1\} \\ &= \{1p, 2p, 3p, \ldots, p^{k-1}p\} \end{aligned}$$

$$\begin{aligned} \varphi(n) &= n - |F| \\ &= p^k - p^{k-1} \\ &= p^k(1 - \frac{1}{p}) \end{aligned}$$

# 5 Euler's $\varphi$-function

**powers of primes:**

**Lemma 7.**

$$n = p^k \text{ , } p \text{ prime} \quad \rightarrow \quad \varphi(n) = n(1 - \frac{1}{p})$$

*Proof.*

$$\begin{aligned} F &= \{a \in \mathbb{Z}_n \ : \ gcd(a,n) > 1\} \\ &= \{1p, 2p, 3p, \ldots, p^{k-1}p\} \end{aligned}$$

$$\begin{aligned} \varphi(n) &= n - |F| \\ &= p^k - p^{k-1} \\ &= p^k(1 - \frac{1}{p}) \end{aligned}$$

special case for $k = 1$

**Lemma 8.**

$$p \text{ prime} \ \rightarrow \ \varphi(p) = p - 1$$

*Proof.*

$$\varphi(p) = p \cdot (1 - \frac{1}{p}) = p - 1$$

# 5 Euler's $\varphi$-function

**powers of primes:**

**Lemma 7.**

$$n = p^k \ , \ p \ prime \quad \rightarrow \quad \varphi(n) = n(1 - \frac{1}{p})$$

*Proof.*

$$\begin{aligned} F &= \{a \in \mathbb{Z}_n \ : \ gcd(a,n) > 1\} \\ &= \{1p, 2p, 3p, \ldots, p^{k-1}p\} \end{aligned}$$

$$\begin{aligned} \varphi(n) &= n - |F| \\ &= p^k - p^{k-1} \\ &= p^k(1 - \frac{1}{p}) \end{aligned}$$

special case for $k = 1$

**Lemma 8.**

$$p \ prime \ \rightarrow \ \varphi(p) = p - 1$$

*Proof.*

$$\varphi(p) = p \cdot (1 - \frac{1}{p}) = p - 1$$

**general case:**

**Lemma 9.**

$$\varphi(n) = n \cdot \prod_{p|n, p \ prime} (1 - \frac{1}{p})$$

*Proof.* Let the prime factorization of $n$ be

$$n = p_1^{k_1} \ldots p_s^{k_s}$$

Then

$$\begin{aligned} \varphi(n) &= \prod_i \varphi(p^{k_i}) \quad \text{(lemma 6} \\ &= \prod_i n \cdot (1 - \frac{1}{p_i}) \quad \text{(lemma 7)} \\ &= n \cdot \prod_{p|n, p \text{ prime}} (1 - \frac{1}{p}) \end{aligned}$$

# 6 Subgroups and Lagrange's Theorem

**subgroups:**

Let $G = (S, \circ)$ be a group, $S' \subseteq S$

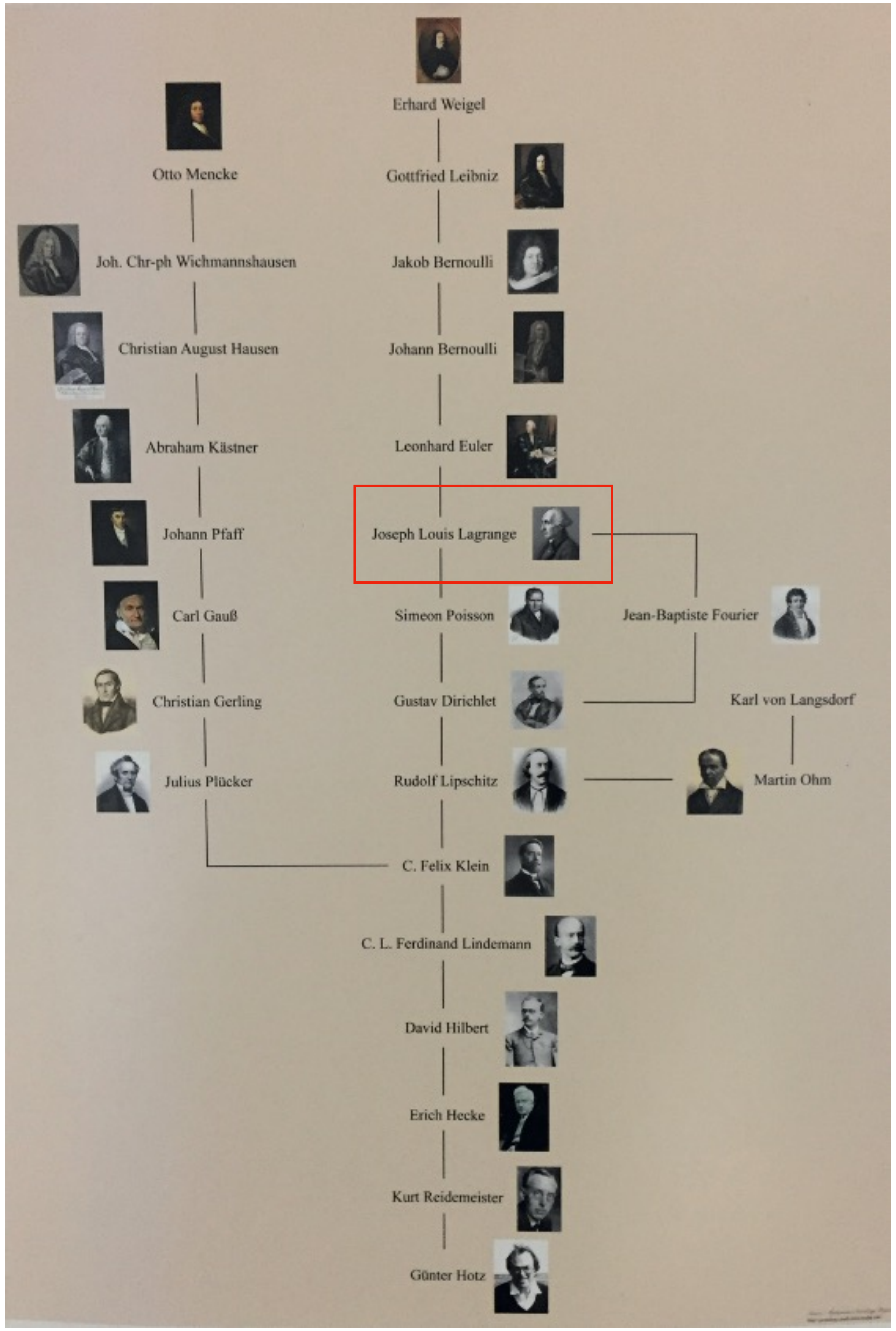
$$a \circ' b = a \circ b \text{ for all } a, b \in S'$$

Then $G'$ is a *subgroup* of $G$ iff

$$a \circ b \in S' \text{ for all } a, b \in S'$$

**examples:**

- let $\mathbb{Z}_{even} = \{2z \ : \ z \in \mathbb{Z}\}$ be the set of even integers. Then $(\mathbb{Z}_{even}, +)$ is subgroup of $(\mathbb{Z}, +)$.
- let $S' = \{0, 2, 4\}$. Then $(S', +_6)$ is subgroup of $(\mathbb{Z}_6, +_6)$.



# 6 Subgroups and Lagrange's Theorem

**subgroups:**

Let $G = (S, \circ)$ be a group, $S' \subseteq S$

$$a \circ' b = a \circ b \text{ for all } a, b \in S'$$

Then $G'$ is a *subgroup* of $G$ iff

$$a \circ b \in S' \text{ for all } a, b \in S'$$

**examples:**

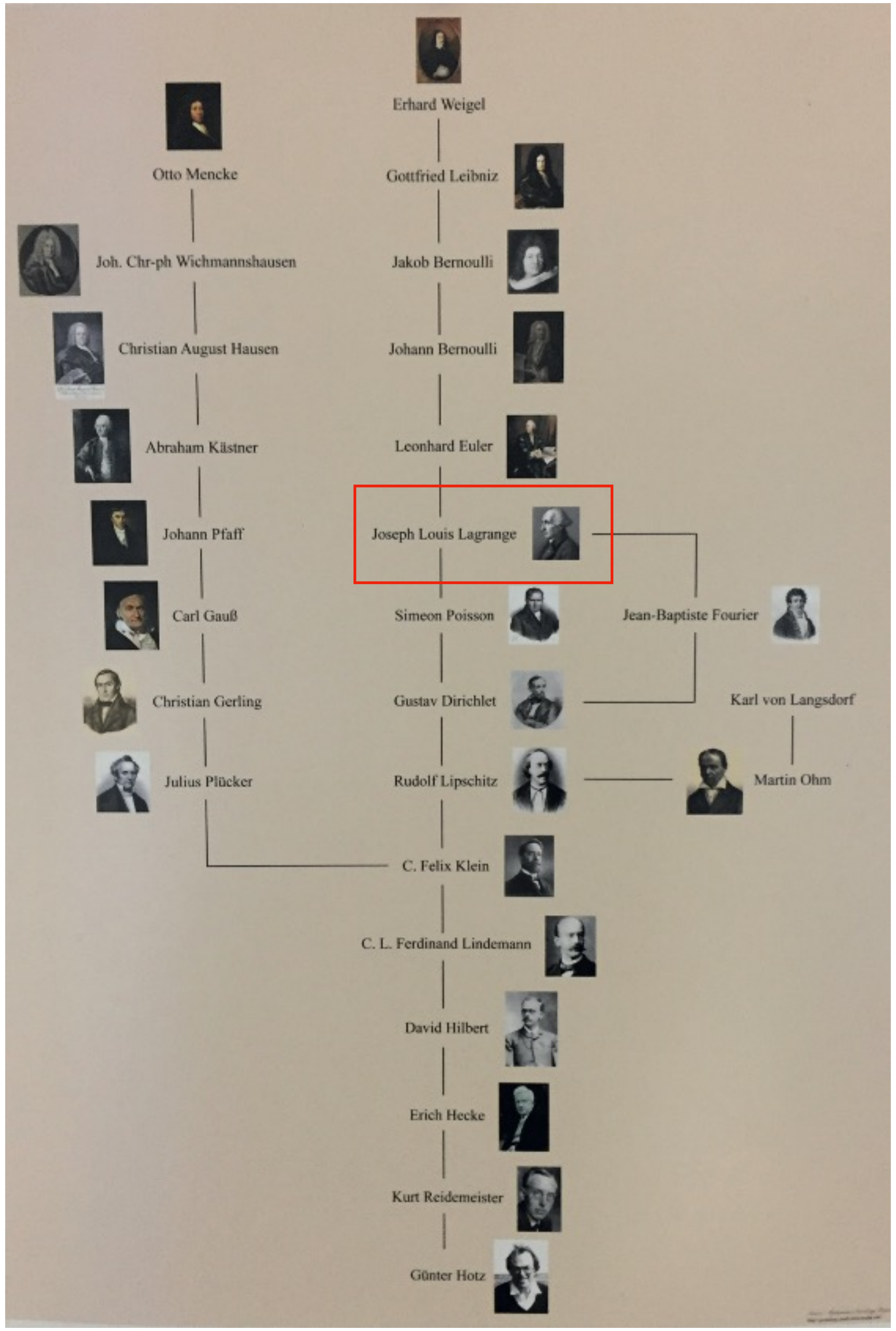
- let $\mathbb{Z}_{even} = \{2z \ : \ z \in \mathbb{Z}\}$ be the set of even integers. Then $(\mathbb{Z}_{even}, +)$ is subgroup of $(\mathbb{Z}, +)$.
- let $S' = \{0, 2, 4\}$. Then $(S', +_6)$ is subgroup of $(\mathbb{Z}_6, +_6)$.

**convention:**

If $\circ$ is clear we speak of

- group $S$ instead of $(S, \circ)$
- subgroup $S'$ instead of $(S', \circ')$

now along the lines of https://crypto.stanford.edu/pbc/notes/group/



# 6 Subgroups and Lagrange's Theorem

**subgroups:**

Let $G = (S, \circ)$ be a group, $S' \subseteq S$

$$a \circ' b = a \circ b \text{ for all } a, b \in S'$$

Then $G'$ is a *subgroup* of $G$ iff

$$a \circ b \in S' \text{ for all } a, b \in S'$$

**examples:**

- let $\mathbb{Z}_{even} = \{2z \ : \ z \in \mathbb{Z}\}$ be the set of even integers. Then $(\mathbb{Z}_{even}, +)$ is subgroup of $(\mathbb{Z}, +)$.
- let $S' = \{0, 2, 4\}$. Then $(S', +_6)$ is subgroup of $(\mathbb{Z}_6, +_6)$.

**convention:**

If $\circ$ is clear we speak of

- group $S$ instead of $(S, \circ)$
- subgroup $S'$ instead of $(S', \circ')$

now along the lines of https://crypto.stanford.edu/pbc/notes/group/

**definition:**

For subgroups $H$ of $G$ and $r \in G$ one defines *right hand cosets*

$$Hr = \{h \circ r \ : \ h \in H\}$$

# 6 Subgroups and Lagrange's Theorem

**subgroups:**

Let $G = (S, \circ)$ be a group, $S' \subseteq S$

$$a \circ' b = a \circ b \text{ for all } a, b \in S'$$

Then $G'$ is a *subgroup* of $G$ iff

$$a \circ b \in S' \text{ for all } a, b \in S'$$

**examples:**

- let $\mathbb{Z}_{even} = \{2z \ : \ z \in \mathbb{Z}\}$ be the set of even integers. Then $(\mathbb{Z}_{even}, +)$ is subgroup of $(\mathbb{Z}, +)$.
- let $S' = \{0, 2, 4\}$. Then $(S', +_6)$ is subgroup of $(\mathbb{Z}_6, +_6)$.

**convention:**

If $\circ$ is clear we speak of

- group $S$ instead of $(S, \circ)$
- subgroup $S'$ instead of $(S', \circ')$

now along the lines of https://crypto.stanford.edu/pbc/notes/group/

**definition:**

For subgroups $H$ of $G$ and $r \in G$ one defines *right hand cosets*

$$Hr = \{h \circ r \ : \ h \in H\}$$

**Lemma 10.**

$$|Hr| = |H|$$

The mapping

$$b : H \to G \ , \ b(h) = h \circ r$$

is injective:

$$\begin{aligned} h \circ r &= h' \circ r \quad || \circ r^{-1} \\ \to h &= h' \end{aligned}$$

# 6 Subgroups and Lagrange's Theorem

**subgroups:**

Let $G = (S, \circ)$ be a group, $S' \subseteq S$

$$a \circ' b = a \circ b \text{ for all } a, b \in S'$$

Then $G'$ is a *subgroup* of $G$ iff

$$a \circ b \in S' \text{ for all } a, b \in S'$$

**examples:**

- let $\mathbb{Z}_{even} = \{2z \ : \ z \in \mathbb{Z}\}$ be the set of even integers. Then $(\mathbb{Z}_{even}, +)$ is subgroup of $(\mathbb{Z}, +)$.
- let $S' = \{0, 2, 4\}$. Then $(S', +_6)$ is subgroup of $(\mathbb{Z}_6, +_6)$.

**convention:**

If $\circ$ is clear we speak of

- group $S$ instead of $(S, \circ)$
- subgroup $S'$ instead of $(S', \circ')$

now along the lines of https://crypto.stanford.edu/pbc/notes/group/

**definition:**

For subgroups $H$ of $G$ and $r \in G$ one defines *right hand cosets*

$$Hr = \{h \circ r \ : \ h \in H\}$$

**Lemma 10.**

$$|Hr| = |H|$$

The mapping

$$b : H \to G \ , \ b(h) = h \circ r$$

is injective:

$$\begin{aligned} h \circ r &= h' \circ r \quad || \circ r^{-1} \\ \to h &= h' \end{aligned}$$

**Lemma 11.**

$$Hr = Hs \leftrightarrow rs^{-1} \in H \ , \ \textit{otherwise } Hr \cap Hs = \emptyset$$

**definition:**

For subgroups $H$ of $G$ and $r \in G$ one defines *right hand cosets*

$$Hr = \{h \circ r \ : \ h \in H\}$$

**Lemma 10.**

$$|Hr| = |H|$$

The mapping

$$b : H \to G \ , \ b(h) = h \circ r$$

is injective:

$$\begin{aligned} h \circ r &= h' \circ r \quad || \circ r^{-1} \\ \to h &= h' \end{aligned}$$

**Lemma 11.**

$$Hr = Hs \ \leftrightarrow \ rs^{-1} \in H \ , \ \textit{otherwise} \ Hr \cap Hs = \emptyset$$

- if $rs^{-1} = h \in H$

$$\begin{aligned} H = Hh &= (Hr)s^{-1} \quad || \circ s \\ Hs &= Hr \end{aligned}$$

**definition:**

For subgroups $H$ of $G$ and $r \in G$ one defines *right hand cosets*

$$Hr = \{h \circ r \;:\; h \in H\}$$

**Lemma 10.**

$$|Hr| = |H|$$

The mapping

$$b : H \to G \;,\; b(h) = h \circ r$$

is injective:

$$\begin{aligned} h \circ r &= h' \circ r \quad || \circ r^{-1} \\ \to h &= h' \end{aligned}$$

**Lemma 11.**

$$Hr = Hs \;\leftrightarrow\; rs^{-1} \in H \;,\; \textit{otherwise } Hr \cap Hs = \emptyset$$

- if $rs^{-1} = h \in H$

$$\begin{aligned} H = Hh &= (Hr)s^{-1} \quad || \circ s \\ Hs &= Hr \end{aligned}$$

- if $Hr = Hs$

$$e \in H \;, r = er \in Hr$$

$$\begin{aligned} r &= h's \quad \text{with } h' \in H \quad || \circ s^{-1} \\ rs^{-1} &= h' \in H \end{aligned}$$

- assume $h_1 r = h_2 s$ with $h_1, h_2 \in H$

$$\begin{aligned} h_1 r &= h_2 s \quad || h_1^{-1} \circ \\ r &= h_1^{-1} h_2 s \quad || \circ s^{-1} \\ rs^{-1} &= h_1^{-1} h_2 \in H \end{aligned}$$

**definition:**

For subgroups $H$ of $G$ and $r \in G$ one defines *right hand cosets*

$$Hr = \{h \circ r \ : \ h \in H\}$$

**Lemma 10.**

$$|Hr| = |H|$$

The mapping

$$b : H \to G \ , \ b(h) = h \circ r$$

is injective:

$$\begin{aligned} h \circ r &= h' \circ r \quad || \circ r^{-1} \\ \to h &= h' \end{aligned}$$

**Lemma 11.**

$$Hr = Hs \ \leftrightarrow \ rs^{-1} \in H \ , \ otherwise\ Hr \cap Hs = \emptyset$$

**Lagrange's theorem:**

**Lemma 12.** *If $H$ is a subgroup of finite group $G$, then $|H|$ divides $|G|$.*

**definition:**

For subgroups $H$ of $G$ and $r \in G$ one defines *right hand cosets*

$$Hr = \{h \circ r \;:\; h \in H\}$$

**Lemma 10.**

$$|Hr| = |H|$$

The mapping

$$b : H \to G \;,\; b(h) = h \circ r$$

is injective:

$$\begin{aligned} h \circ r &= h' \circ r \quad || \circ r^{-1} \\ \to h &= h' \end{aligned}$$

**Lemma 11.**

$$Hr = Hs \;\leftrightarrow\; rs^{-1} \in H \;,\; \textit{otherwise } Hr \cap Hs = \emptyset$$

**Lagrange's theorem:**

**Lemma 12.** *If $H$ is a subgroup of finite group $G$, then $|H|$ divides $|G|$.*

Exhaust $G$ by
$i = 1;\; P(1) = H;$

while $\exists s_i \in G \setminus H(i)$

$P = P \cup Hs_i; i = i + 1$

As $G$ is finite this terminates with some finite $i = n \leq |G|$.

$$G = \bigcup_{i=1}^{n} Hs_i$$

By lemma 11 the union is disjoint.

$$\begin{aligned} |G| &= \sum_{i=1}^{n} |Hs_i| \\ &= n \cdot |H| \quad \text{(lemma 10 )} \end{aligned}$$

**definition:**

For subgroups $H$ of $G$ and $r \in G$ one defines *right hand cosets*

$$Hr = \{h \circ r \ : \ h \in H\}$$

**Lemma 10.**

$$|Hr| = |H|$$

The mapping

$$b : H \to G \ , \ b(h) = h \circ r$$

is injective:

$$\begin{aligned} h \circ r &= h' \circ r \quad || \circ r^{-1} \\ \to h &= h' \end{aligned}$$

**Lemma 11.**

$$Hr = Hs \ \leftrightarrow \ rs^{-1} \in H \ , \ \textit{otherwise}\ Hr \cap Hs = \emptyset$$

**Lagrange's theorem:**

**Lemma 12.** *If $H$ is a subgroup of finite group $G$, then $|H|$ divides $|G|$.*

Exhaust $G$ by
$i = 1;\ P(1) = H;$

while $\exists s_i \in G \setminus H(i)$

$P = P \cup Hs_i; i = i + 1$

As $G$ is finite this terminates with some finite $i = n \leq |G|$.

$$G = \bigcup_{i=1}^{n} Hs_i$$

By lemma 11 the union is disjoint.

$$\begin{aligned} |G| &= \sum_{i=1}^{n} |Hs_i| \\ &= n \cdot |H| \quad \text{(lemma 10 )} \end{aligned}$$

**Lemma 13.** *If $H$ is a proper subroup of finite group $g$, then $|H| \leq |G|/2$*