2. Groups

2.1 Groups

Let G be a set with the $\cdot$ operation. Then $(G, \cdot)$ is a group $\iff$

1. $a, b \in G \Rightarrow ab \in G$ - **closure**
2. $a, b, c \in G \Rightarrow (ab)c = a(bc)$ - **Assiociativity**
3. $\exists\ e \in G\ s.t\ ae = ea = e,\ \forall\ a \in G$ - **Identity**
4. $\forall\ a \in G\ \exists a' \in G\ s.t.\ aa' = a'a = e$ - **Inverses**

Examples:

Group	Operation	Identity	Form of Element	Inverse	Abelian
Z	Addition	0	k	$-k$	Yes
Q^+	Multiplication	1	m/n, $m, n > 0$	n/m	Yes
Z_n	Addition mod n	0	k	$n - k$	Yes
$\mathbf{R}^*$	Multiplication	1	x	$1/x$	Yes
$\mathbf{C}^*$	Multiplication	1	$a + bi$	$\frac{1}{a^2 + b^2}a - \frac{1}{a^2 - b^2}bi$	Yes
$GL(2, F)$	Matrix multiplication	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $ad - bc \neq 0$	$\begin{bmatrix} \frac{d}{ad - bc} & \frac{-b}{ad - bc} \\ \frac{-c}{ad - bc} & \frac{a}{ad - bc} \end{bmatrix}$	No
$U(n)$	Multiplication mod n	1	k, $\gcd(k, n) = 1$	Solution to $kx \bmod n = 1$	Yes
$\mathbf{R}^n$	Componentwise addition	$(0, 0, \ldots, 0)$	$(a_1, a_2, \ldots, a_n)$	$(-a_1, -a_2, \ldots, -a_n)$	Yes
$SL(2, F)$	Matrix multiplication	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $ad - bc = 1$	$\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$	No
D_n	Composition	R_0	R_α, L	$R_{360 - \alpha}, L$	No

Propreties

> The identity e is unique
>
> The inverse of an element a is unique
>
> $(ab)^{-1} = b^{-1}a^{-1}$

2.2 Mappings

$$F : S \to S'$$

Example

- $f : \mathbb{R} \to \mathbb{R};\ f(x) = x^2 \iff x \mapsto x^2$

injectivity, bijectivity, surjectivity - known
identity mapping, Inverse, composites - known

Permutations

> $P(S)$ is a **group** with the composiotion as law

2.3 Homomorphisms

Let

- G, G' be groups

> A Homomorphism is a map $f : G \to G'$ with the following property:
>
> $$f(xy) = f(x)f(y)\ \forall x, y, \in G$$

- Homomorphisms preserve structure

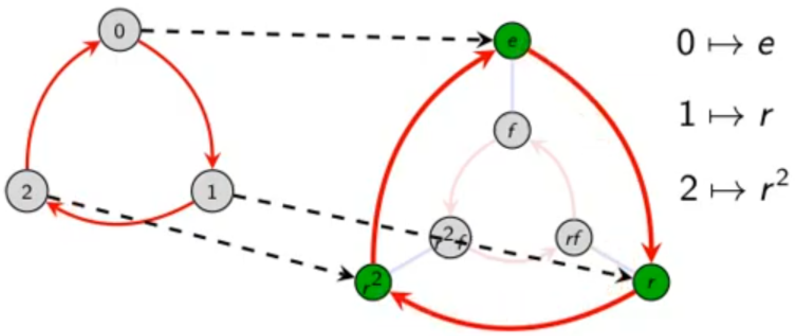
Example
$x \mapsto e^x$ is a homomorphism from the multiplicative to the additive group

Proprieties of a homomorphism $f : G \to G'$

1. Let e, e' be the unit elements $\Rightarrow f(e) = e'$
   - *Proof*:
   - $f(e) = f(ee) = f(e)f(e)|_{\cdot f(e)^{-1}} \iff e' = f(e)$
2. Let $x \in G \Rightarrow f(x^{-1}) = f(x)^{-1}$
   - *Proof*:
   - $e' = f(e) = f(xx^{-1}) = f(x)f(x^{-1})_{\cdot f(x)^{-1}} \iff f(x)^{-1} = f(x^{-1})$
3. Let $g : G' \to G''$ be a group homomorphism $\Rightarrow g \circ f$ is a group homomorphism from G to G''

Intuition - Homomorphism

Consider the statement: $\mathbb{Z}_3 < D_3$. Here is a visual:



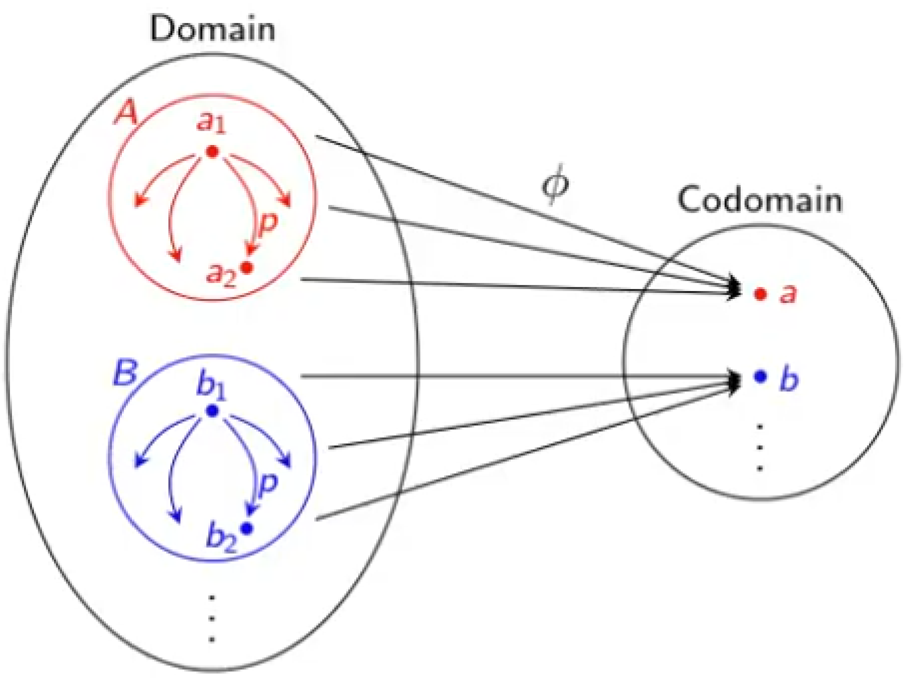
The group D_3 contains a size-3 cyclic subgroup $\langle r \rangle$, which is identical to $\mathbb{Z}_3$ in structure only. None of the elements of $\mathbb{Z}_3$ (namely 0, 1, 2) are actually in D_3.

When we say $\mathbb{Z}_3 < D_3$, we really mean that the structure of $\mathbb{Z}_3$ shows up in D_3.

In particular, there is a bijective correspondence between the elements in $\mathbb{Z}_3$ and those in the subgroup $\langle r \rangle$ in D_3. Furthermore, the *relationship* between the corresponding nodes is the same.

Preimage

> If $f: G \to H$ is a homomorphism and $h \in Im(f) < H$ the **preiamge** of h is the set $f^{-1}(h) = \{g \in G : f(g) = h\}$



Property

- All preimages have the same structure

Kernel of a homomorphism

> All $g \in G$ with $f(g) = e'$ form the **kernel**
> = Preimage of e'

Proprieties

- if $Ker(f) = e$ then f is injective
  - *Proof*: $x, y \in G$ and $f(x) = f(y)$
  - $e' = f(x)f(y)^{-1} = f(xy^{-1}) \Rightarrow xy^{-1} = e \Rightarrow x = y$

> An injective homomorphism is called an **embedding**

Isomorphism

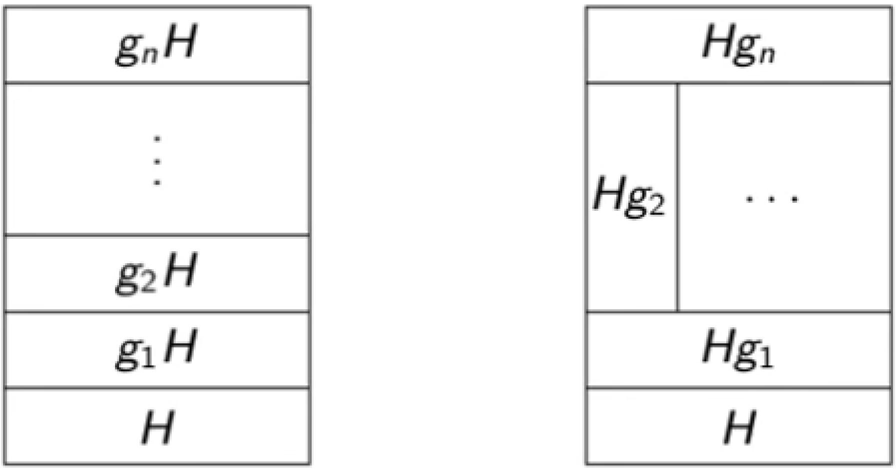
> Let $f : G \to G'$ be a group homomorphism
> f is an **Isomorphism** $\iff$ $\exists g : G' \to G$ s.t $f \circ g$ and $g \circ f$ are the identity mappings

Theorem

> - If $Ker(f) = e$ then f is an isomorphism with the image $f(G)$
>   - *Proof*: f is always surjective into its image and we proved above it's injective

2.4 Cosets

> Let G be a group and H be a subgroup. The **set** of all elements ax with $x \in H$ is called a **coset** of H in G
>
> - Denoted by aH

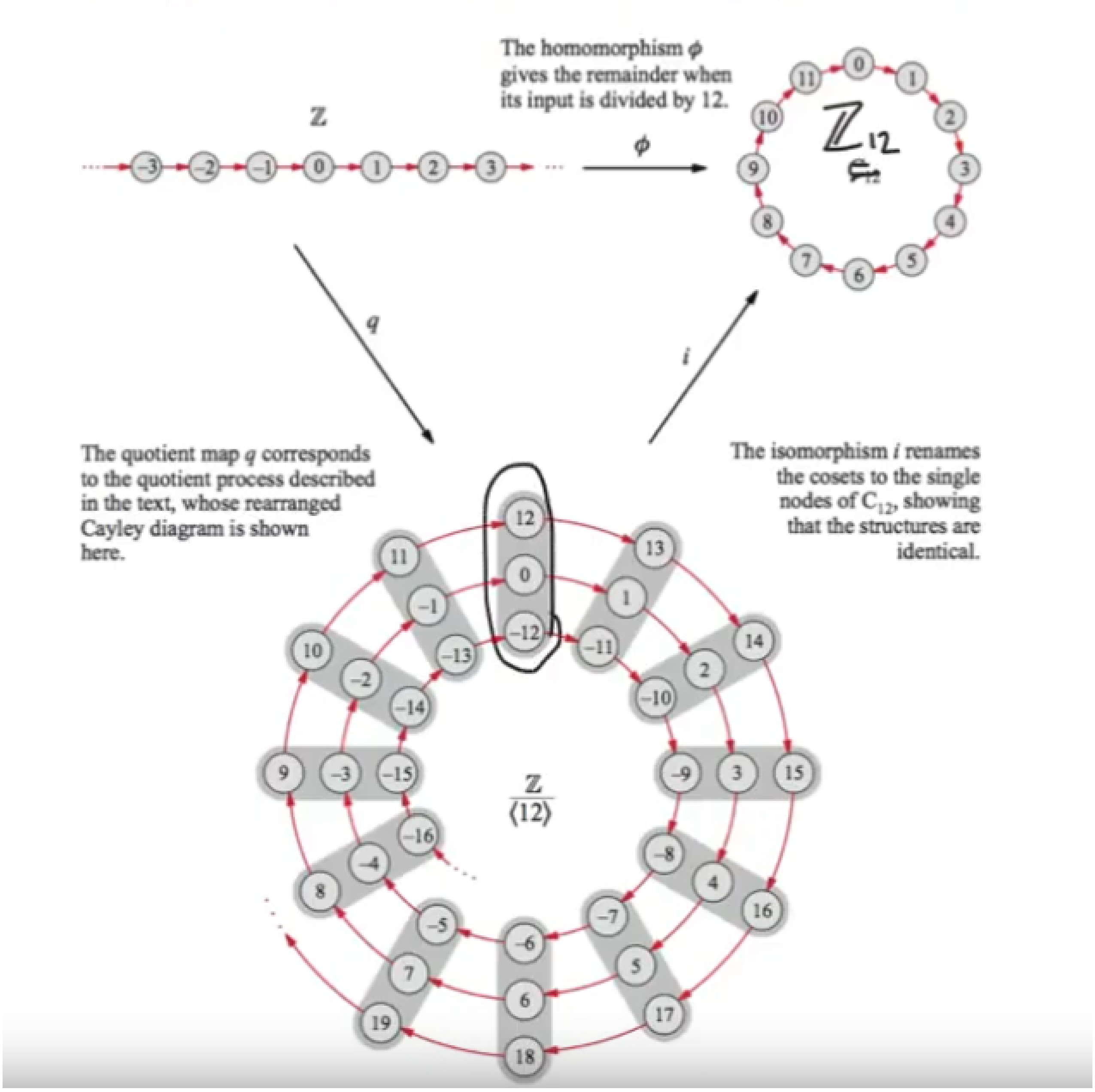


- https://www.youtube.com/watch?v=TCcSZEL_3CQ&list=PLi01XoE8jYoi3SgnnGorR_XOW3IcK-TP6&index=7
- https://www.youtube.com/watch?v=Ia_CSTWVkuc&list=PLwV-9DG53NDxU337smpTwm6sef4x-SCLv&index=12

Proprieties

Let $H < G$ and $a, b \in G$

- Two cosets of the same subgroup either are equal or have no element in common
- $|H| = |aH| = |bH|$ - same number of elements
- $a \in aH$
- $aH = H \iff a \in H$
- $aH = bH \iff a \in bH$
- $aH = Ha \iff H = aHa^{-1}$
- $aH < G \iff a \in H$



Note

- The coset is **not** necesarily a group

Normal subgroup

- https://en.wikipedia.org/wiki/Normal_subgroup

- https://math.stackexchange.com/questions/1014535/is-there-any-intuitive-understanding-of-normal-subgroup/1014791

Definition - normal subgroup

> A subgroup H of a group G is called a **normal subgroup** of G if $aH = Ha \, \forall a \in G$
> Notation: $H \lhd G$.

Definition - conjugate

> Let $a \in G$
> The set $aHa^{-1} = \{aha^{-1} | h \in H\}$ is called the conjugate of H by a

Test to see if H is normal

- H is a normal subgroup of $G \iff aHa^-1 \subseteq H \forall a \in G$

Note

- for an element $h \in H$, ah is not necessarily equal to ha.
- The idea is that the cosets are equal.

Intuition

- Looks the same over all perspectives

2.5 Cyclic groups

> A group G is cyclic if $\exists a \in G \; s.t. \; G = \{a^n | n \in \mathbb{Z}\}$
> Notation: $G = \langle a \rangle$

Theorem

> Let a be an element of order n and k a positive int
> $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ and $|a^k| = n/gcd(n,k)$

Proof

- Let $d = \gcd(n,k), \; k = dr$
- Since $a^k = (a^d)^r \Rightarrow \langle a^k \rangle \subseteq \langle a^d \rangle$ (1)
- By $\gcd \Rightarrow \exists s,t \in \mathbb{Z} \; s.t. \; d = ns + kt \Rightarrow a^d = a^{ns+kt} = a^{ns}a^{kt} = e(a^{kt}) = (a^k)^t \in \langle a^k \rangle \Rightarrow \langle a^d \rangle \subseteq \langle a^k \rangle$ (2)
- By (1) and (2) we proved the theorem

Theorem - Lagrange

> Let $G = \langle a \rangle$
> The order of any subgroup H of G divides the order of G

Theorem - Isomorphisms between cyclic groups

> Any 2 cyclic groups of order d are isomorphic.
> If a is a generator of G then there is a unique isomorphism $f : \mathbb{Z}/d\mathbb{Z} \to G$ s.t. $f(1) = a$

Note

- All groups of prime order are cyclic

2.6 Direct product

External

> Let $G_1, ..., G_n$ a finite collection of groups
> The **external direct product** is the set of all n-tuples for which the i'th component is an element of G_i with the operation componentwise
> Notation $G_1 \oplus G_2 \oplus ... \oplus G_n = \{(g_1, ...g_n) \mid g_i \in G_i\}$

Example

- $\mathbb{Z}_2 \oplus \mathbb{Z}_3 = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}$
- Note that $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \sim \mathbb{Z}_6$

Theorem - order of an element in the external direct product

> $|(g_1, g_2, ..., g_n) = lcm(|g_1|, |g_2|, ..., |g_n|)$

Theorem - isomorphism

> Let $m = n_1 n_2 ... n_k$
> Then $\mathbb{Z}_m$ is isomorphic to $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus ... \oplus \mathbb{Z}_{n_k} \iff \gcd(n_i, n_j) = 1$ for $i \neq j$

Theorem - direct product is cyclic?

> $G \oplus H$ is cyclic $\iff \gcd(|G|, |H|) = 1$

Application - Binary strings

- An n-bit string can be an element of $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus ... \oplus \mathbb{Z}_2$ - n times

Internal

> Let $H, K < G$
> $G = H \times K$ if H, K are normal subgroups and $G = HK$ and $H \cap K = \{e\}$

2.7 Finite ableian groups

Torsion element

> An element $a \in A$ is said to be a **torsion element** if it has finite period
> The subset of all torsion elements of A is a **subgroup** of A and is called the **torsion**

> **subgroup**

Proprerty

- a has period m
- b has period n
- $\Rightarrow a \pm b$ has period dividing mn

Theorem

> The group A is the direct sum of its subgroups $A(p)$ for all primes p dividing n

Fundamental Theorem of Finite Abelian Groups

> Every finite Abelian group is a direct product of cyclic groups of prime power order
> Moreover the number of terms and the orders of the cyclic groups are **uniquely** determiend by the group
> Every abelian cyclic group $G \approx \mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_{\mathbb{k}}^{n_{\mathbb{k}}}}$

Note

- p_i aren't necessarily distinct primes

Existenc eof subgroups of abelian groups

> If m divides $|G|$ then G has a subgroups of order m