2. Groups

- Some images are taken from this lecture [visual group theory]

2.1 Groups

Definition

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**

If $a, b \in G \Rightarrow ab = ba$ we call G an **abelian group**

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

- Photo from Contemporary abstract algebra

Propreties

1. The identity e is unique
2. The inverse of an element a is unique and $(a^{-1})^{-1} = a$
3. $(ab)^{-1} = b^{-1}a^{-1}$
4. The **trivial group** is formed only by the identity element – $\{1\}$

Notation - sometimes the identity $e \in G$ will be denoted with 1_G

2.2 Mappings

$$f : S \to S'$$

Example

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

Definitions

- injectivity, bijectivity, surjectivity - wiki these
- identity mapping, Inverse, composites - wiki these

Left multiplication is a bijection
Let G be a group and fix g. Then the map $G \to G$ with $x \mapsto gx$ is a **bijection**

Example: Let $G = (\mathbb{Z}/5\mathbb{Z})^*$ and pick $g = 2$

$$\begin{aligned} 1 &\overset{\times 2}{\mapsto} 2 \bmod 5 \\ 2 &\overset{\times 2}{\mapsto} 4 \bmod 5 \\ 3 &\overset{\times 2}{\mapsto} 1 \bmod 5 \\ 4 &\overset{\times 2}{\mapsto} 3 \bmod 5 \end{aligned}$$

Permutations

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

2.3 Homomorphisms

Definition – homomorphisms

Let G, H be groups. A **homomorphism** is a map $f : G \to H$ with the following property:

$$f(xy) = f(x)f(y)\ \forall x, y \in G$$

- Homomorphisms preserve structure

Examples

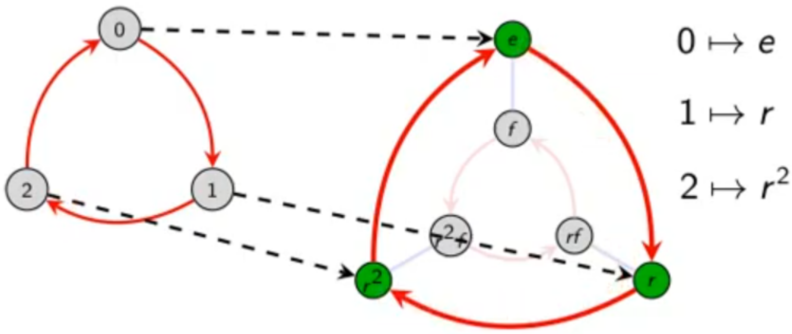
1. $x \mapsto e^x$ is a homomorphism from the multiplicative to the additive group
2. $\phi : \mathbb{Z} \to \mathbb{Z}/100\mathbb{Z},\ \phi(x) = x \bmod 100$

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

1. Let $1_G, 1_H$ be the unit elements $\Rightarrow f(1_G) = 1_H$
   Proof:
$$f(1_G) = f(1_G 1_G) = f(1_G)f(1_G)|_{\cdot f(1_G)^{-1}} \iff 1_H = f(1_G)$$
2. Let $x \in G \Rightarrow f(x^{-1}) = f(x)^{-1}$
   Proof:
$$1_H = f(1_G) = f(xx^{-1}) = f(x)f(x^{-1})_{\cdot f(x)^{-1}} \iff f(x)^{-1} = f(x^{-1})$$
3. Let $f : G \to G'$ be a group homomorphism and 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.

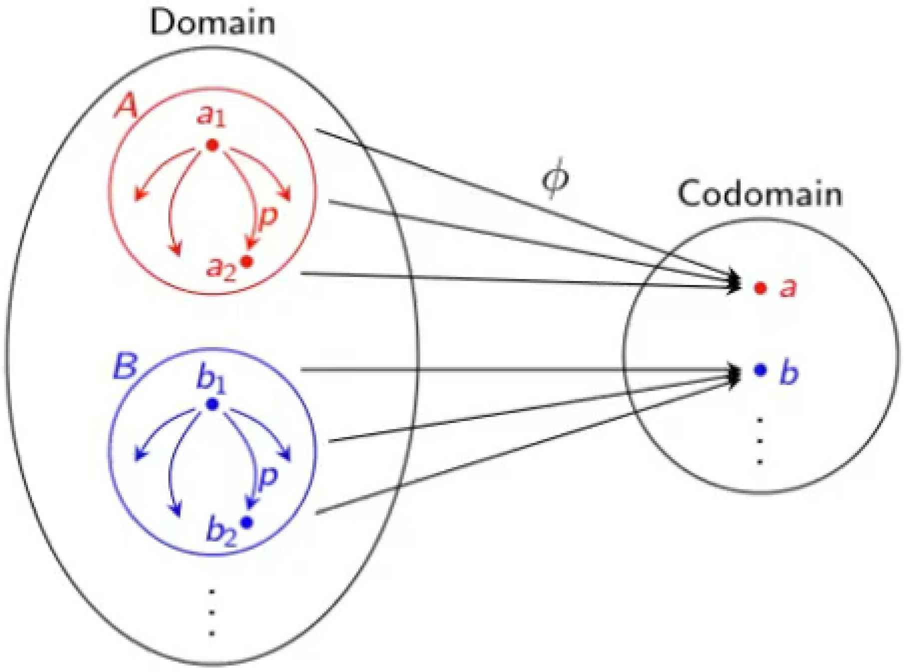
In particular, there is a bijective correspondence between the elements in $\mathbb{Z}_3$ and those in the subgroup $\langle r \rangle$ in D_3. Furthermore, the *relationship* between the corresponding nodes is the same.

Preimages

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

Definition – kernel

The kernel of $f : G \to H$ is represented by all $g \in G$ with $f(g) = 1_H$
Preimage of 1_H

$$\ker f = \{g \in G \ : \ f(g) = 1_H\}$$

Examples of kernels

1. Let $f : \mathbb{Z} \to \mathbb{Z}/100\mathbb{Z}, \ f(x) = x \bmod 100$
   $\ker f = 100\mathbb{Z} = \{..., -200, -100, 0, 100, 200, ...\}$
2. Let $f : \mathbb{Z} \to \mathbb{Z}, \ f(x) = 10x$
   $\ker f = \{0\}$ – trivial
3. Let $f : G \to H, \ f(g) = 1_H$
   $\ker f = G$ – all of G represents the kernel

Proprieties

- if $\ker(f) = 1_G$ then f is injective

Proof:

Let $x, y \in G$ and $f(x) = f(y)$
$1_H = f(x)f(y)^{-1} = f(xy^{-1}) \Rightarrow xy^{-1} = 1_G \Rightarrow x = y$

Definition – Embedding

An injective homomorphism is called an **embedding**

Isomorphism

Definition – Isomorphism

Let $f : G \to H$ be a group homomorphism

f is an **isomorphism** $\iff$ $\exists g : H \to G$ s.t $f \circ g$ and $g \circ f$ are the identity mappings

f is an **isomorphism** if f is a bijection and a homomorphism

Example: Consider $\mathbb{Z}$ and $10\mathbb{Z}$ with the map $f : \mathbb{Z} \to 10\mathbb{Z}$ with $\phi(x) = 10x$

- f is a bijection
- $f(x+y) = 10(x+y) = 10x + 10y = f(x) + f(y)$

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

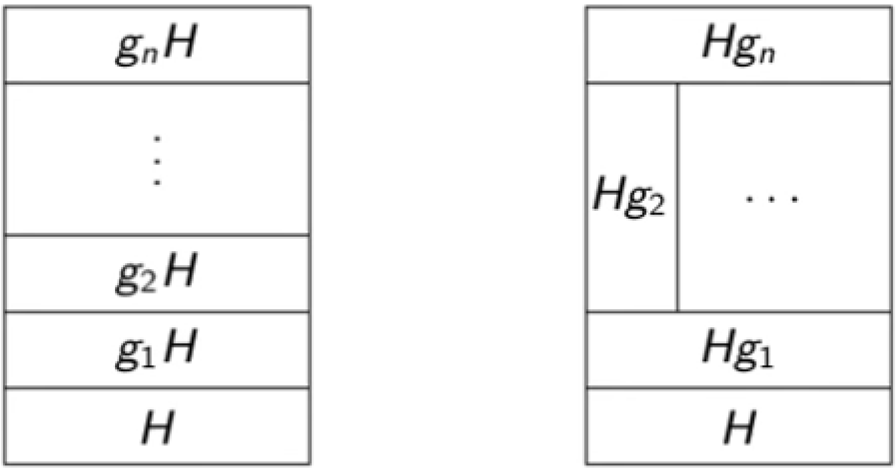
2.4 Cosets

- written – page 71 – good example – follow along with this, it's explained better

Definition – 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



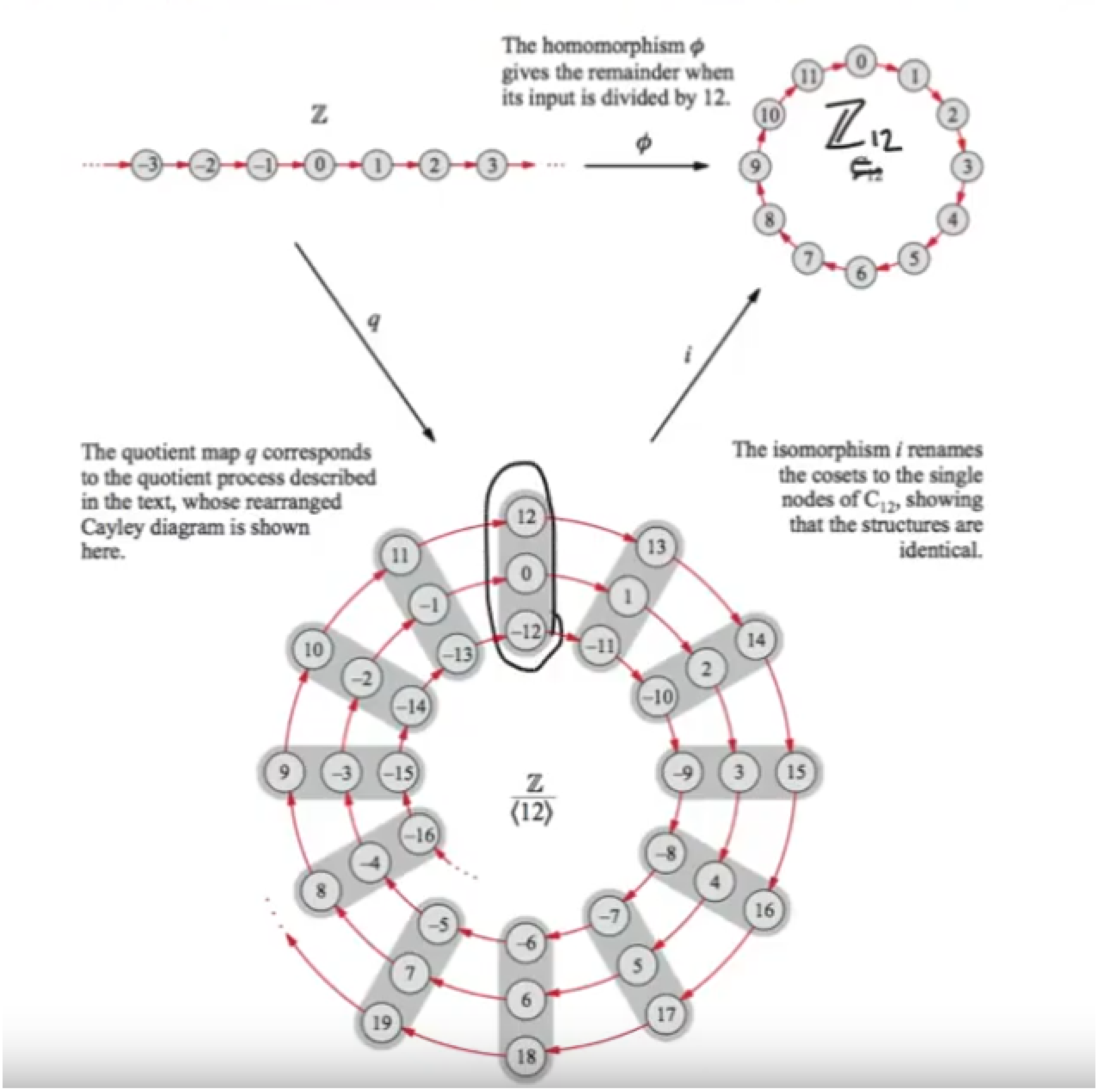
- video – short explanation
- video – socratica explanation
- video – visual group theory explanation

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

Definition – cyclic subgroup

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 $G = \langle a \rangle$ – a cyclic subgroup
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

Definition – External product

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

- $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} = \{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2)\}$
- Note that $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \sim \mathbb{Z}/6\mathbb{Z}$

Theorem – order of an element in the external direct product

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

where lcm = least common multiple

Theorem – isomorphism

Let $m = n_1 n_2 ... n_k$. Then $\mathbb{Z}_m$ is isomorphic to $\mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus ... \oplus \mathbb{Z}/n_k\mathbb{Z} \iff \gcd(n_i, n_j) = 1$ 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 $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus ... \oplus \mathbb{Z}/2\mathbb{Z}$ - n times

Internal

Definition – Internal subgroup

Let $H, K < G$
Then $G = H \times K$ 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 $G \approx \mathbb{Z}/p_1^{n_1}\mathbb{Z} \oplus \mathbb{Z}/p_2^{n_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_k^{n_k}\mathbb{Z}$

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