

Math 250, Fall 2019
Groups, Rings and Fields, Fall 2019
Richard E. Borcherds, 219 Dwinelle, 9:30-11AM

Contents

| | | |
|----------|------------------|----------|
| 1 | Groups | 1 |
| 1.1 | Groups | 1 |

1 Groups

1.1 Groups

There are two definitions to define a group.

Definition 1.1 (Concrete definition)

A group is a symmetries of something 1:1 map preserving “structure”.

Example 1.2

Consider the rotation of a rectangle, we have a group of order 4.

Example 1.3

Consider the rotation of a icosahedron, we are able to obtain a group of order 60.

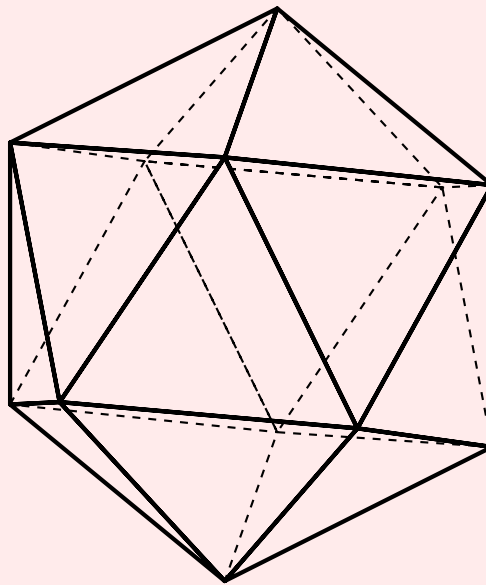


Image of a Icosahedron

Example 1.4

Let V be a n -dimensional over \mathbb{R} . The general linear group $GL_n(\mathbb{R})$, all matrices with $\det \neq 0$ from a group.

Definition 1.5 (Abstract Definition, Cayley)

A group is a set G with a binary operation $a + b$ or $a \times b$ or $a \circ b$ or ab (notation sucks) such that

1. Identity element 0, 1, or e , i.e $a1 = 1a = a$.
2. Each element has inverse a^{-1} , i.e $aa^{-1} = a^{-1}a = 1$.
3. Associative $(ab)c = a(bc)$ for all $a, b, c \in G$

Definition 1.6

A group G acts on S means given operation

$$G \times S \rightarrow S$$

such that $1s = s$ and $a(bs) = ab(s)$.

Example 1.7

Let G be the icosahedron group and let S be the icosahedron.

Question 1.8

How does G acts on G ?

Definition 1.9

There are 8 different types of actions

1. $g(s) = s$, left action (trivial)
2. $g(s) = gs$
3. $g(s) = sg^{-1}$
4. $g(s) = gsg^{-1}$, adjoint action

Note that all of these are left actions of the group, then similarly there are also 4 right group actions. $S \times G \rightarrow S$

1. $sg = s$
2. $sg = sg$
3. $sg = g^{-1}s$
4. $sg = g^{-1}sg$

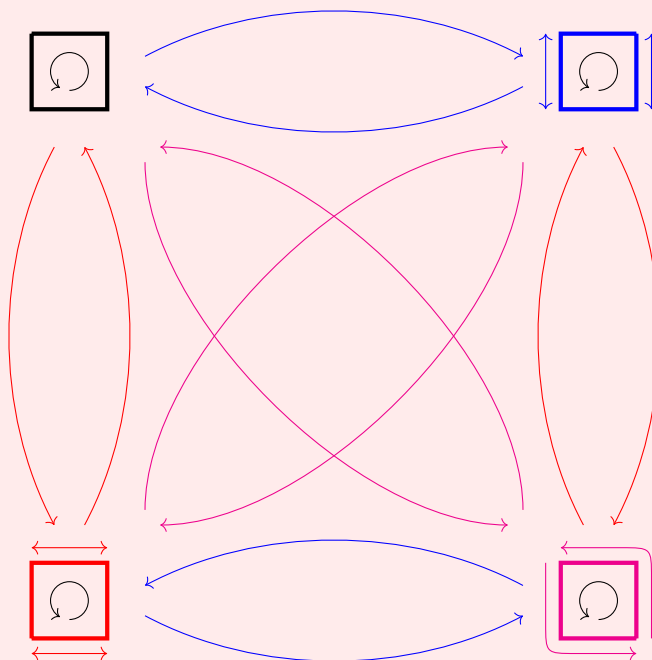
Remark 1.10

$g(s) = gs, g(s) = sg^{-1}, sg = sg, sg = g^{-1}s$ does not preserve group operation of S .

We let G act on $S(= G)$ by $g(s) = gs$. This means G into subset of all permutations of $S(= G)$. Now we want to add extra “structure” to S so G is exactly symmetries of S with this structure.

Extra structure is **right** action of G on S . We now have 3 copies of G

1. Set $S(= G)$.
2. G acting on **right** on $S \leftarrow$ part of structure
3. G acting on **left** on $S \leftarrow$ symmetry group

Example 1.11 (Cayley Graph of 4 elements)

We get colored (directed) graph arrow gives **right** action of G , which is not the same as the **left** action.

Remark 1.12

Goals of group theory

1. Classify all groups
2. Given a group G , find all ways G acts on something.

Example 1.13

Linear representation = actions of G over vector space.

Permutation = actions of G over on a set.

Definition 1.14

A homomorphism $f : G \rightarrow H$ map preserving group structure. i.e. $f(gh) = f(g)f(h)$.

A isomorphism is a homomorphism that is a bijection.

The kernel of f is the set of elements such that it maps to the trivial element of H

Example 1.15

Consider the function

$$\exp : \langle \mathbb{R}, + \rangle \rightarrow \langle \mathbb{R}^*, \cdot \rangle$$

\exp is a isomorphism from \mathbb{R} to $R_{>0}$

Example 1.16

Consider the function

$$\exp : \langle \mathbb{C}, + \rangle \rightarrow \langle \mathbb{C}^*, \cdot \rangle$$

kernel = elements $2\pi in, n \in \mathbb{Z}$.

Example 1.17 (Number Theory)

Consider $\mathbb{Z}/4\mathbb{Z}$ integers mod 4. and $(\mathbb{Z}/5\mathbb{Z})^*$ nonzero integers mod 5 under multiplication.

Example 1.18

Consider the function :

$$\det : GL_n(\mathbb{R}) \rightarrow \mathbb{R}^*$$

is a homomorphism.

kernel = $SL_n(\mathbb{R})$ = special linear group.

Theorem 1.19 (Lagrange's Theorem)

If H is a subgroup of G , order of H divides order of G . (G is finite)

Lemma 1.20

2 cosets either are the same or disjoint.

Proof. If $aH \cap bH = \emptyset$, then the proof is done.

Now we suppose $aH \cap bH \neq \emptyset$, then we know that $ah_1 = bh_2$ for some element in aH and bH . We compute $ah_1 = bh_2 \implies h_1 = a^{-1}bh_2 \implies a^{-1}b = h_1h_2^{-1} \implies a^{-1}b \in H$. By proposition 1 we know that $aH = bH$.

We can use a similar argument to show that this works for the right cosets as well. This is left as an exercises to the reader. ■

Lemma 1.21

Any cosets have the same size.

Proof. We can simply prove that $\phi : h \mapsto bh$ is bijective, therefore $|H| = |bH|$.

This proof is trivial and is left as an exercise to the reader. (Hint: prove that ϕ is injective and say it's surjective by construction) ■

Proof. Suppose G acts on S . Pick $s \in S$, put $H = \text{set of elements fixing } s$ such that $hs = s$, then H is a subgroup of G .

Given a subgroup H of G , we can find set S acted on by G , $s \in S$. $H = \text{things fixed in } S$.

Given $g, h (H \subseteq G)$. $S = \text{left cosets of } H$.

we get action of G on set of cosets by putting $g(aH) = (ga)H$. (well-defined left as an exercise)

Therefore $|G| = |H| \times \text{number of cosets}$. Therefore the order of H divides the order of H . ■

Theorem 1.22

If $g \in G$, then the order of g divides order of G .

Corollary 1.23

If G is prime order, it is cyclic

Proof. Pick any element $g \neq 1$. Order divided p , so p is primes. so $G = \text{powers of } g$ ■

Example 1.24

List of all groups

1. Order 1 : Trivial group
2. Order 2 : 1 group $\mathbb{Z}/2\mathbb{Z}$, 0, 1.
3. Order prime p : Integer mod p .
4. Order 4 : Cyclic group $\mathbb{Z}/4\mathbb{Z}$ and symmetry of a rectangle. These are not isomorphic as the symmetry group of rectangle does not have a element of order 4.
5. Classify all groups with $g^2 = 1$ for all g . We want to show that group is abelian, or $gh = hg$ for all $g, h \in G$. This follows because $ghgh = (gh)^2 = 1 = h^2g^2 = hhgg \implies hg = gh$. Since G is abelian, we can write group operation as $+$. Notice that G is a vector space over field of order 2, namely $\mathbb{Z}/2\mathbb{Z}$. so h has a basis, and is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^n$ (n -dimensional vector space) to some n . So there is only 1 other group of order 4.

Definition 1.25

Suppose G, H are groups, then the product(sum) of the group is defined as follows

$$G \times H = \text{set of pairs}(g, h)$$

and the operation is defined as

$$(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2)$$

Example 1.26

symmetry of rectangle is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Example 1.27

$\mathbb{C}^* = S \times \mathbb{R}_{>0}$, where S is the circle group. Notice that this is the polar decomposition of complex numbers.

Definition 1.28

The product(sum) of groups are elements (g_1, g_2, \dots) such that all but finite number of g_i are trivial.

Example 1.29

\mathbb{Q}^* = infinite sum of groups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \dots$. This follows by fundamental theorem of arithmetic.