Math 4550

Topic 1 - Groups

In this class we will be interested in studying a mathematical object called a group.

<u>Def:</u> A <u>group</u> $\langle G, * \rangle$ is a set G with a binary operation $*$ such that four properties hold:

① (closure) If $a, b \in G$, then $a * b \in G$.

② (associativity) If $a, b, c \in G$, then
$$a * (b * c) = (a * b) * c$$

③ (identity element) There exists an identity element $e \in G$ such that
$$a * e = e * a = a \quad \text{for all } a \in G.$$

④ (inverses) If $a \in G$, then there exists $b \in G$ with $a * b = e$ and $b * a = e$

Ex: $\langle \mathbb{Z}, + \rangle$ is a group where

$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

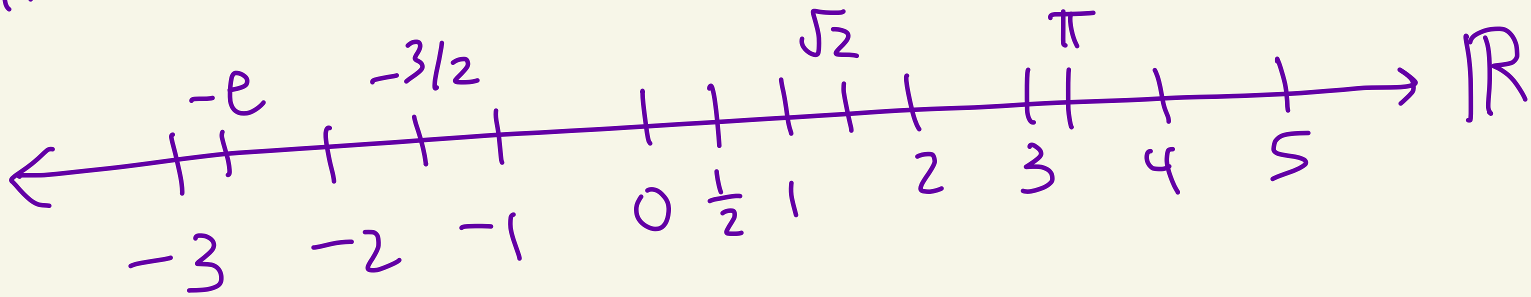
is the set of integers.

1. If a, b are integers, then $a+b$ is an integer.
2. If a, b, c are integers, then $a+(b+c) = (a+b)+c$

assumptions on $\mathbb{Z}$ that we won't prove

3. $e = 0$ is an identity element since $0 + a = a + 0 = a$ for any integer a.
4. Given $a \in \mathbb{Z}$ we know $b = -a$ is an integer and $a + (-a) = 0$ and $(-a) + a = 0$.

Ex: $\langle \mathbb{R}, + \rangle$ is a group where $\mathbb{R}$ is the set of real numbers.



① If $a, b \in \mathbb{R}$, then $a+b \in \mathbb{R}$

② If $a, b, c \in \mathbb{R}$, then $a+(b+c) = (a+b)+c$

assumptions on $\mathbb{R}$ that we won't prove

③ $e = 0$ is in $\mathbb{R}$ and $0 + a = a + 0 = a$ for any $a \in \mathbb{R}$

④ If $a \in \mathbb{R}$, then $b = -a$ is in $\mathbb{R}$ and $a + (-a) = (-a) + a = 0$

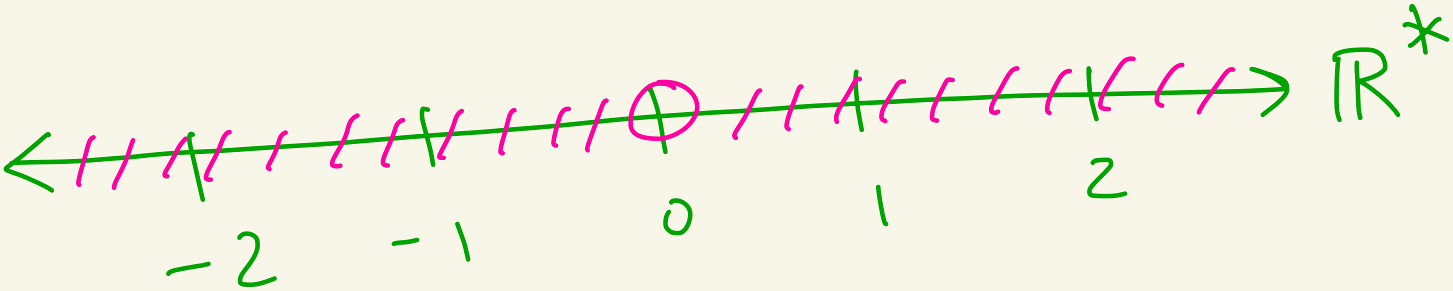
Ex: $\mathbb{R}$ under multiplication $\cdot$ is not a group.

Properties 1, 2, 3 will hold with $e=1$ in 3. However 4 will not hold. Why?

Pick $a=0$. Then there is no b where $\underbrace{0b}_{a\cdot b}=\underbrace{1}_{e}$

$a\cdot b=e$

Ex: Let $\mathbb{R}^* = \underbrace{\mathbb{R} - \{0\}}_{\text{remove } 0 \text{ from } \mathbb{R}}$



Then $\mathbb{R}^*$ is a group under multiplication

① Let $a, b \in \mathbb{R}^*$. Then $a, b \in \mathbb{R}$ and $a \neq 0, b \neq 0$.

Since $a \in \mathbb{R}$ and $b \in \mathbb{R}$ we know $ab \in \mathbb{R}$.
Since $a \neq 0$ and $b \neq 0$ we know $ab \neq 0$.

assumptions on $\mathbb{R}$

By the way there are groups where $a \neq 0$ and $b \neq 0$ but $ab = 0$.

Thus, $ab \in \mathbb{R}^*$.

② Let $a, b, c \in \mathbb{R}^*$. Then

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

property of $\mathbb{R}$ we won't prove

③ $e=1$ is in $\mathbb{R}^*$ and $a \cdot 1 = 1 \cdot a = a$ for all $a \in \mathbb{R}^*$.

④ Let $a \in \mathbb{R}^*$. Then $a \in \mathbb{R}$, $a \neq 0$.
Thus, $b = \frac{1}{a} \in \mathbb{R}$ and $b \neq 0$.

And $\frac{1}{a} \cdot a = a \cdot \frac{1}{a} = 1$

$\boxed{}$

Def: A group $\langle G, * \rangle$ is **abelian** if $a * b = b * a$ for every $a, b \in G$.

Ex: $\langle \mathbb{Z}, + \rangle$ is abelian

$\langle \mathbb{R}, + \rangle$ is abelian.

$\langle \mathbb{R}^*, \cdot \rangle$ is abelian

Ex: The set of rational numbers

$$\mathbb{Q} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z}, b \neq 0 \right\}$$

is an abelian group under addition

Ex: (Integers modulo n)

Recall that if $a, b \in \mathbb{Z}$ then a divides b if there exists $k \in \mathbb{Z}$ with $b = ak$. If so then we write $\underbrace{a \mid b}_{\text{read: "a divides b"}}$.

Ex: $5 \mid 15$ because $15 = (5)\underbrace{(3)}_{k}$

$6 \mid -42$ because $-42 = (6)\underbrace{(-7)}_{k}$

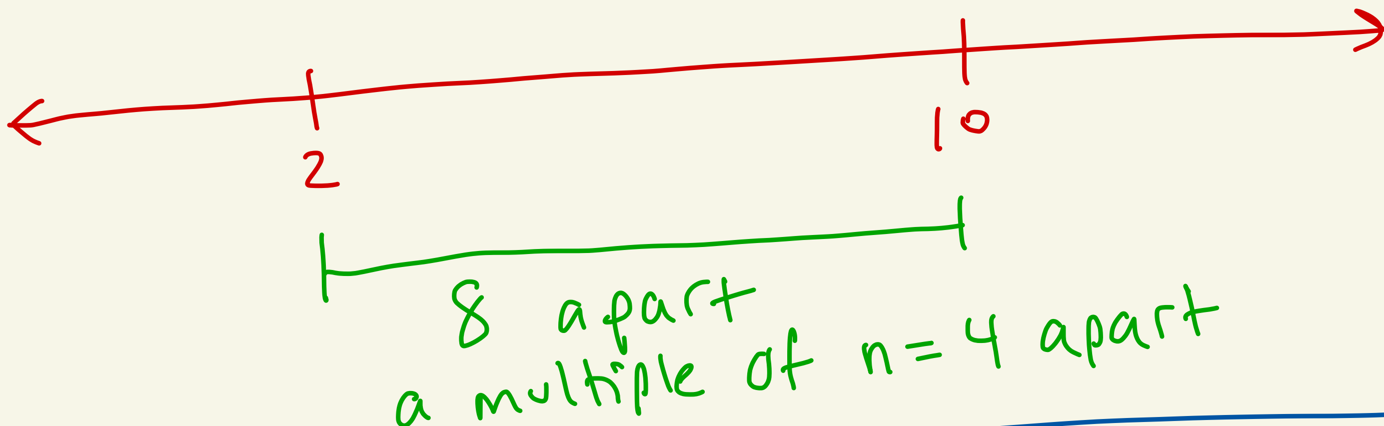
Recall from 3450:

Let $n \in \mathbb{Z}$, $n \geq 2$.

Given $a, b \in \mathbb{Z}$ we write $a \equiv b \pmod{n}$ if n divides $a-b$.

For example, $10 \equiv 2 \pmod{4}$ $\leftarrow$ $n=4$

because $10-2=8$ and 4 divides 8.



In Math 3450, you show that mod n is an equivalence relation.

Hence the set of equivalence classes

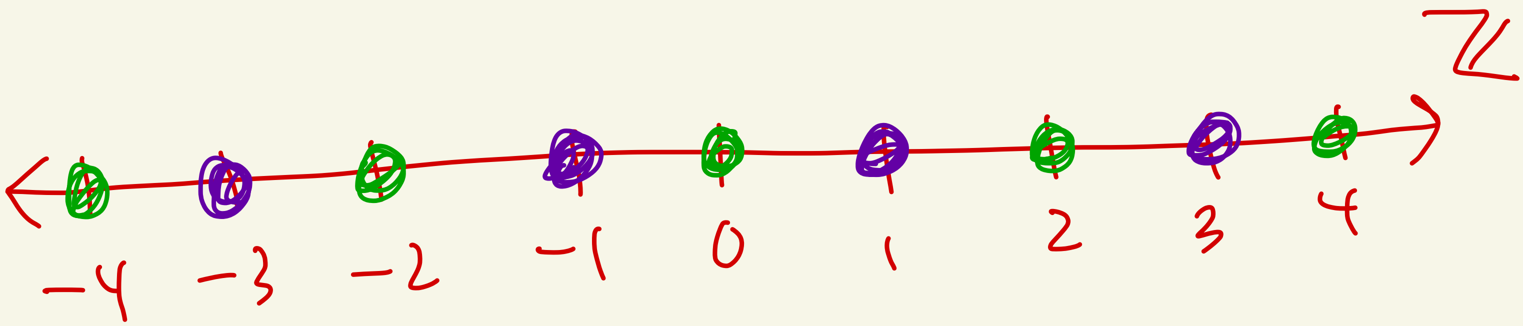
$$\overline{x} = \{ y \mid y \in \mathbb{Z} \text{ and } y \equiv x \pmod{n} \}$$

partition $\mathbb{Z}$.

For example, if $n=2$, then

$$\overline{0} = \{ y \mid y \in \mathbb{Z} \text{ and } y \equiv 0 \pmod{2} \}$$
$$= \{ \ldots, -6, -4, -2, 0, 2, 4, 6, 8, \ldots \}$$

$$\overline{1} = \{ y \mid y \in \mathbb{Z} \text{ and } y \equiv 1 \pmod{2} \}$$
$$= \{ \ldots, -5, -3, -1, 1, 3, 5, 7, \ldots \}$$



Note,

$$\overline{5} = \{ y \mid y \equiv 5 \pmod{2} \}$$
$$= \{ \ldots, -3, -1, 1, 3, 5, 7, 9, 11, \ldots \}$$
$$= \overline{1}$$

and

$$\overline{-2} = \{ y \mid y \equiv -2 \pmod 2 \}$$

$$= \{ \ldots, -8, -6, -4, -2, 0, 2, 4, 6, \ldots \}$$

$$= \overline{0}$$

The unique equivalence classes modulo $n = 2$ are $\overline{0}, \overline{1}$.

For general n, the unique equivalence classes are $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$.

We define the <u>set of integers modulo n</u> to be

$$\mathbb{Z}_n = \{ \overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1} \}$$

In $\mathbb{Z}_n$ one has:

- $\overline{a} = \overline{b}$ iff $a \equiv b \pmod{n}$
- If you divide n into x and get remainder r, then $\overline{x} = \overline{r}$.
- Define

$$\overline{a} + \overline{b} = \overline{a+b}$$
$$\overline{a} \cdot \overline{b} = \overline{ab}$$

In Math 3450/4460 you show these operations are well-defined.

Ex: $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

$\bar{3} + \bar{5} = \bar{8} = \bar{2}$

way 1:

$8 \equiv 2 \pmod 6$

since 6 divides

$8 - 2 = 6$

Way 2:

$$\begin{array}{r} 1 \\ 6\overline{)\,8} \\ -6 \\ \hline 2 \end{array}$$

← remainder

$\bar{5} + \bar{4} \cdot \bar{3} = \bar{5} + \overline{12} = \overline{17} = \bar{5}$

way 1:

$17 \equiv 5 \pmod 6$

since

$17 - 5 = 12$

and $6 \mid 12$

way 2:

$$\begin{array}{r} 2 \\ 6\overline{)\,17} \\ -12 \\ \hline 5 \end{array}$$

remainder

In $\mathbb{Z}_6$ we have: identity is $\overline{0}$

$\overline{x}$	inverse of $\overline{x}$
$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{5}$
$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{3}$
$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{1}$

$\leftarrow \overline{0}+\overline{0}=\overline{0}$

$\leftarrow \overline{1}+\overline{5}=\overline{6}=\overline{0}$

$\leftarrow \overline{2}+\overline{4}=\overline{6}=\overline{0}$

$\leftarrow \overline{3}+\overline{3}=\overline{6}=\overline{0}$

$\leftarrow \overline{4}+\overline{2}=\overline{6}=\overline{0}$

$\leftarrow \overline{5}+\overline{1}=\overline{6}=\overline{0}$

<u>Theorem:</u> The set $\mathbb{Z}_n$ is a group under addition. The identity element is $\overline{0}$. The inverse of $\overline{a}$ is $-\overline{a}=\overline{n-a}$. Further, $\mathbb{Z}_n$ is an abelian group.

Proof: (Skip in class)

(1) Given $\bar{a}, \bar{b} \in \mathbb{Z}_n$ with $a, b \in \mathbb{Z}$ we have $\bar{a} + \bar{b} = \overline{a+b} \in \mathbb{Z}_n$ since $a+b \in \mathbb{Z}$.

(2) Given $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$ we have

$$\bar{a} + (\bar{b} + \bar{c}) = \bar{a} + \overline{b+c} = \overline{a+(b+c)}$$
$$= \overline{(a+b)+c} = \overline{a+b} + \bar{c}$$
$$= (\bar{a} + \bar{b}) + \bar{c}$$

since $\mathbb{Z}$ is associative under $+$

(3) $\bar{0} \in \mathbb{Z}_n$ and given $\bar{x} \in \mathbb{Z}_n$ we have

$$\bar{0} + \bar{x} = \overline{0+x} = \bar{x}$$
$$\bar{x} + \bar{0} = \overline{x+0} = \bar{x}$$

So, $\bar{0}$ is an identity element.

(4) Let $\bar{x} \in \mathbb{Z}_n$ with $x \in \mathbb{Z}$

Then $\overline{-x} \in \mathbb{Z}_n$ and

$$\bar{x} + (\overline{-x}) = \overline{x-x} = \bar{0}$$
$$(\overline{-x}) + \bar{x} = \overline{-x+x} = \bar{0}$$

So, $\overline{-x}$ is an inverse for $\bar{x}$

(5) Given $\bar{x}, \bar{y} \in \mathbb{Z}_n$ with $x, y \in \mathbb{Z}$ we have

$$\bar{x} + \bar{y} = \overline{x+y} = \overline{y+x} = \bar{y} + \bar{x}$$

since $\mathbb{Z}$ is abelian under $+$

So, $\mathbb{Z}_n$ is abelian.

By (1)–(5), $\mathbb{Z}_n$ is an abelian group. $\blacksquare$

<u>Def:</u> A <u>group table</u> is a table of all the group calculations done like this

G	. . . .	b	
⋮			
a		$a*b$	

Ex: Let's calculate the group table for $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$

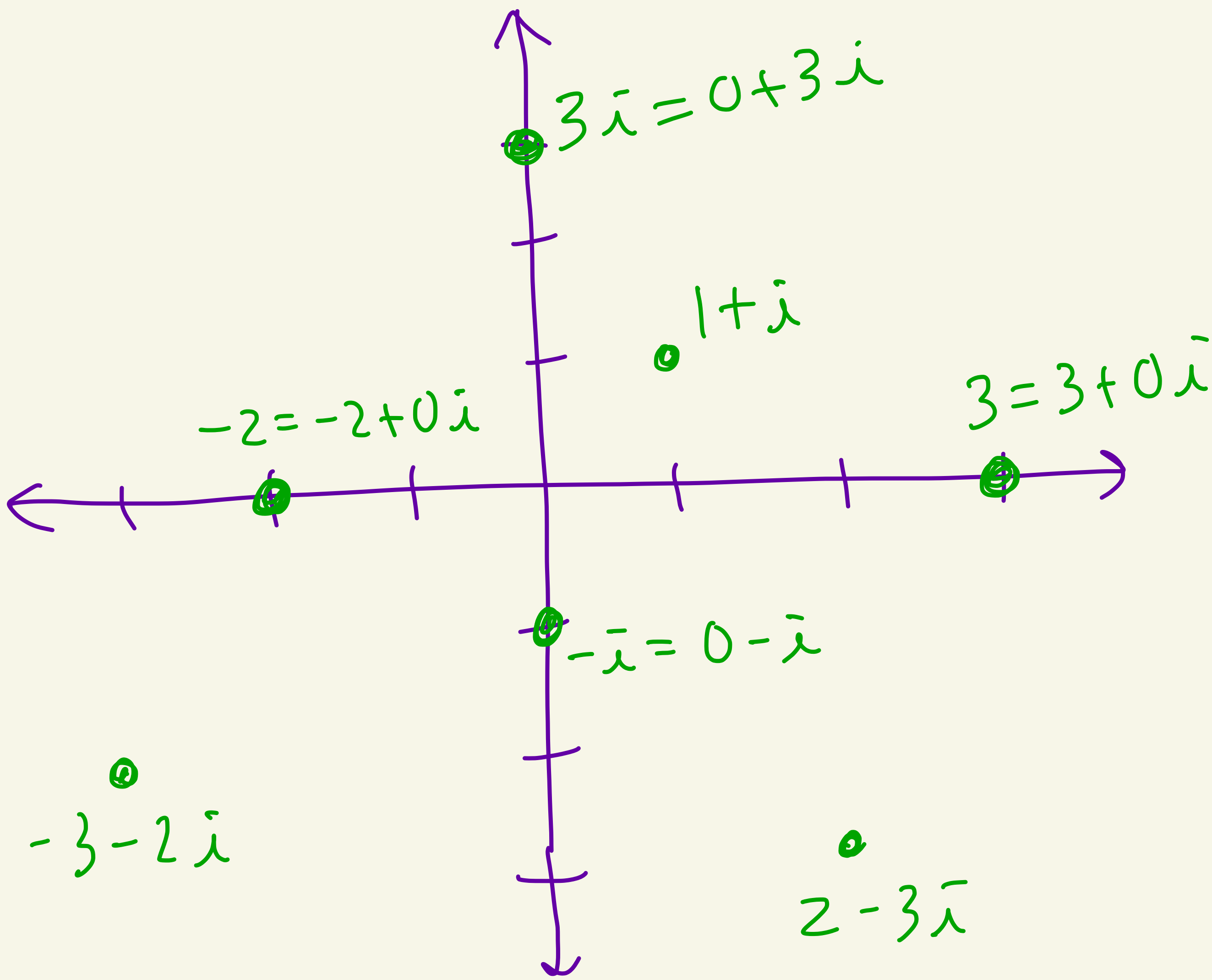
$\mathbb{Z}_3$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

Ex: (The n-th roots of unity)

Recall that the set of complex numbers is

$$\mathbb{C} = \{ a+bi \mid a,b \in \mathbb{R} \}$$

where $i^2 = -1$.

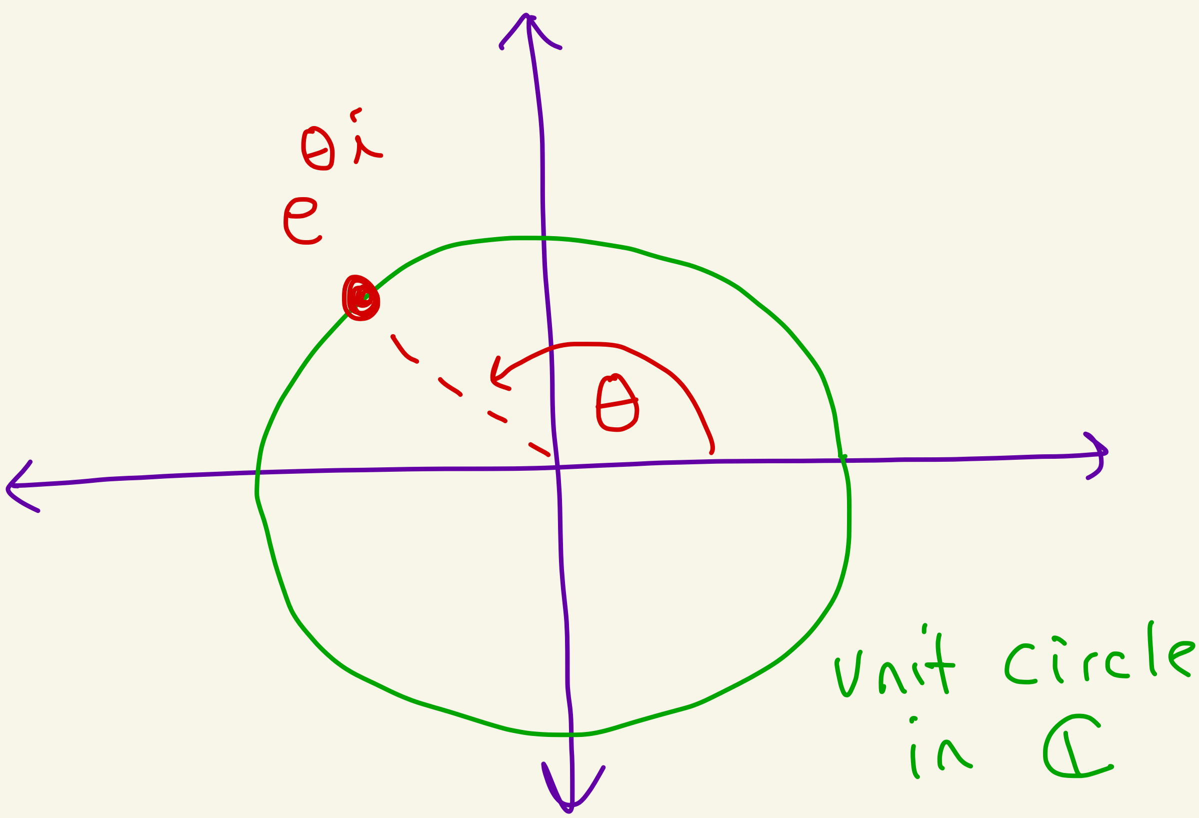


In Math 4680, you will study the complex exponential function. Part of that will involve Euler's formula. Define

$$e^{\theta i} = \cos(\theta) + i\sin(\theta)$$

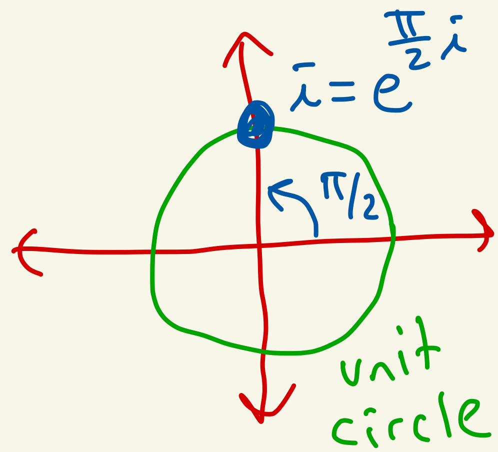
Euler's formula

when θ is a real number.



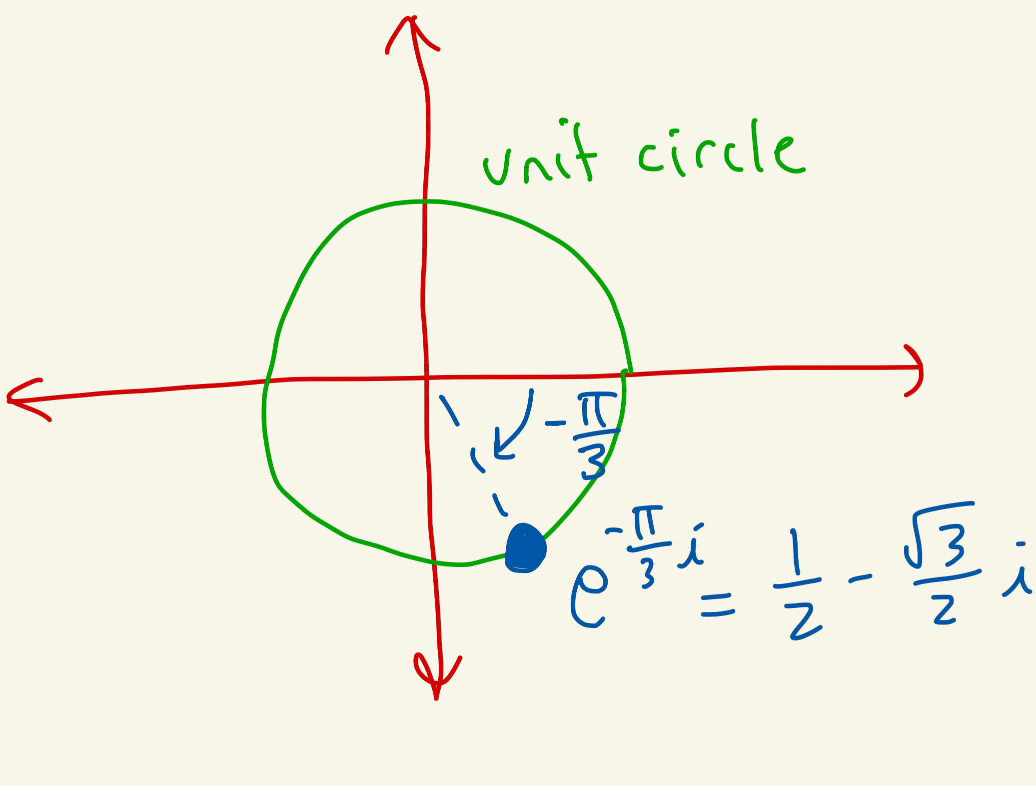
For example,

$$e^{\frac{\pi}{2}i} = \cos\left(\frac{\pi}{2}\right) + i\sin\left(\frac{\pi}{2}\right)$$
$$= 0 + i \cdot 1$$
$$= i$$



and

$$e^{-\frac{\pi}{3}i} = \cos\left(-\frac{\pi}{3}\right) + i\sin\left(-\frac{\pi}{3}\right)$$
$$= \frac{1}{2} - \frac{\sqrt{3}}{2}i$$



Key facts:

$$e^{2\pi i} = 1$$

$$e^{2\pi k i} = 1 \quad \text{if} \quad k \in \mathbb{Z}$$

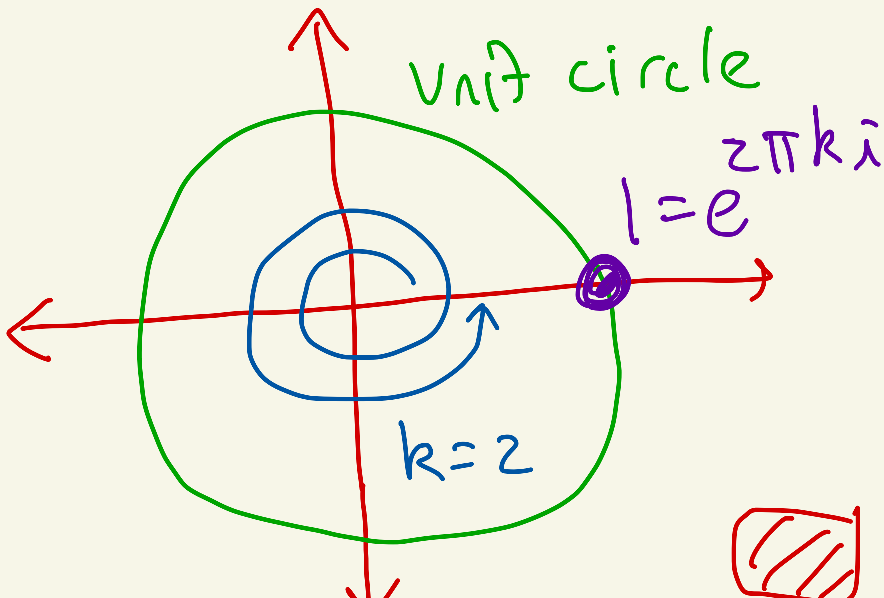
---

proof:

$$e^{2\pi k i} = \cos(2\pi k) + i\sin(2\pi k)$$

$$= 1 + i0$$

$$= 1$$



<u>Theorem:</u> If $\theta_1, \theta_2 \in \mathbb{R}$, then $e^{\theta_1 i} \cdot e^{\theta_2 i} = e^{(\theta_1+\theta_2) i}$

<u>proof:</u>

$$e^{\theta_1 i} e^{\theta_2 i} = \left[\cos(\theta_1) + i\sin(\theta_1)\right]\left[\cos(\theta_2) + i\sin(\theta_2)\right]$$

$$= \left[\cos(\theta_1)\cos(\theta_2) - \sin(\theta_1)\sin(\theta_2)\right]$$

$i^2 = -1$

$$+ i\left[\cos(\theta_1)\sin(\theta_2) + \sin(\theta_1)\cos(\theta_2)\right]$$

$$= \cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2)$$

trig identities

$$= e^{(\theta_1+\theta_2) i}$$

$\blacksquare$

<u>Ex:</u> $e^{\frac{\pi}{2} i} e^{\frac{3\pi}{2} i} = e^{\frac{4\pi}{2} i} = e^{2\pi i} = 1$

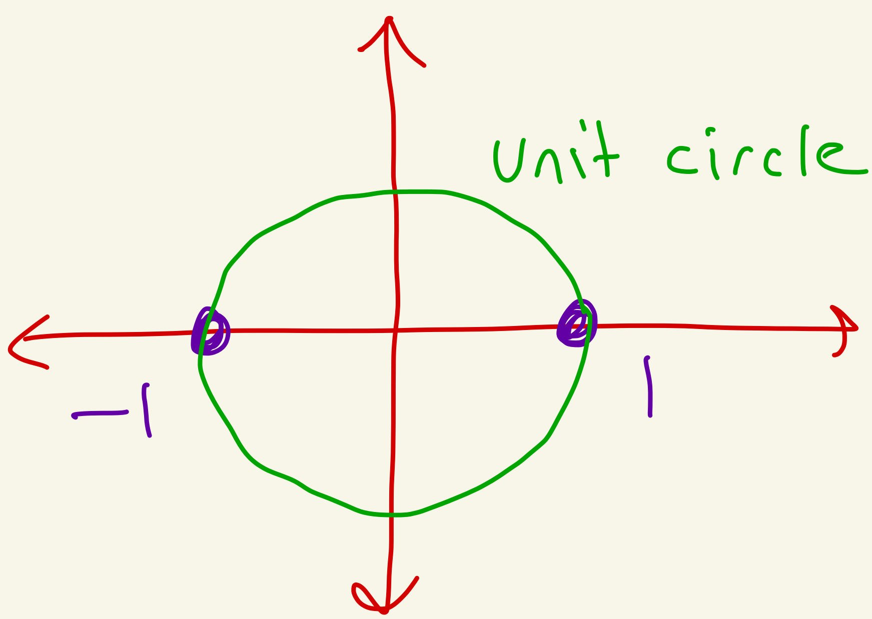
Define the <u>n-th roots of unity</u> to be

$$U_n = \{ z \mid z \in \mathbb{C} \text{ where } z^n = 1 \}$$

For example,

$$U_2 = \{ z \mid z \in \mathbb{C} \text{ where } z^2 = 1 \}$$

$$= \{ 1, -1 \}$$



In Math 4680 you show that

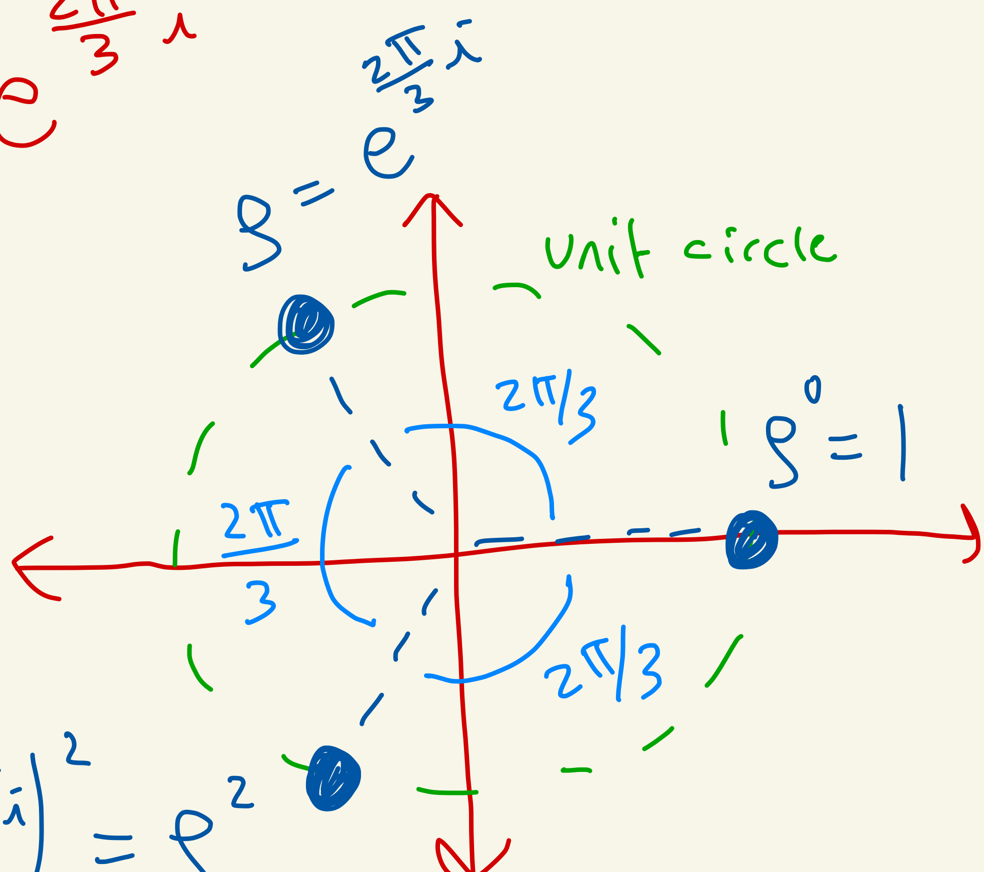
$$U_n = \left\{ \left(e^{\frac{2\pi}{n} i}\right)^k \,\middle|\, k = 0, 1, 2, \ldots, n-1 \right\}$$

$$= \{ \rho^0, \rho^1, \rho^2, \ldots, \rho^{n-1} \}$$

where $\rho = e^{\frac{2\pi}{n} i}$

<u>Ex:</u> $U_3 = \{ \rho^0, \rho^1, \rho^2 \} = \{ 1, \rho, \rho^2 \}$

where $\rho = e^{\frac{2\pi}{3} i}$



$$e^{\frac{4\pi}{3} i} = \left(e^{\frac{2\pi}{3} i}\right)^2 = \rho^2$$

Theorem: U_n is a group under multiplication. The identity element is 1. Furthermore, U_n is abelian.

proof: (Skip in class)

① Let $z_1, z_2 \in U_n$. Then, $z_1^n = 1$ and $z_2^n = 1$.

So, $(z_1 z_2)^n = z_1^n z_2^n = 1 \cdot 1 = 1$.

because multiplication is commutative in $\mathbb{C}$

So, $z_1 z_n \in U_n$.

② Given $a, b, c \in U_n$ we have

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

because $\mathbb{C}$ is commutative under multiplication.

③ $1^n = 1$.

Thus, $1 \in U_n$.

④ If $z^n = 1$, then $1 = \frac{1}{z^n} = \left(\frac{1}{z}\right)^n$ giving $\frac{1}{z} \in U_n$.

⑤ $\mathbb{C}$ is commutative under multiplication

Thus, $a \cdot b = b \cdot a$ if $a, b \in U_n$.

By ① – ⑤ we have that U_n is an abelian group. $\blacksquare$

<u>Key computational fact:</u>

In U_n, if $\zeta = e^{\frac{2\pi}{n} i}$ then $\zeta^n = 1$

Some multiplications in $U_3 = \{1, \rho, \rho^2\}$

$$1 \cdot \rho^2 = \rho^2$$

$$\rho \cdot \rho^2 = \rho^3 = \left(e^{\frac{2\pi}{3} i}\right)^3 = e^{2\pi i} = 1$$

$$\rho^2 \cdot \rho^2 = \rho^4 = \rho^3 \cdot \rho = 1 \cdot \rho = \rho$$

$\rho^3 = 1$ from above

U_3	1	ρ	ρ^2
1	1	ρ	ρ^2
ρ	ρ	ρ^2	1
ρ^2	ρ^2	1	ρ

<u>Note:</u>

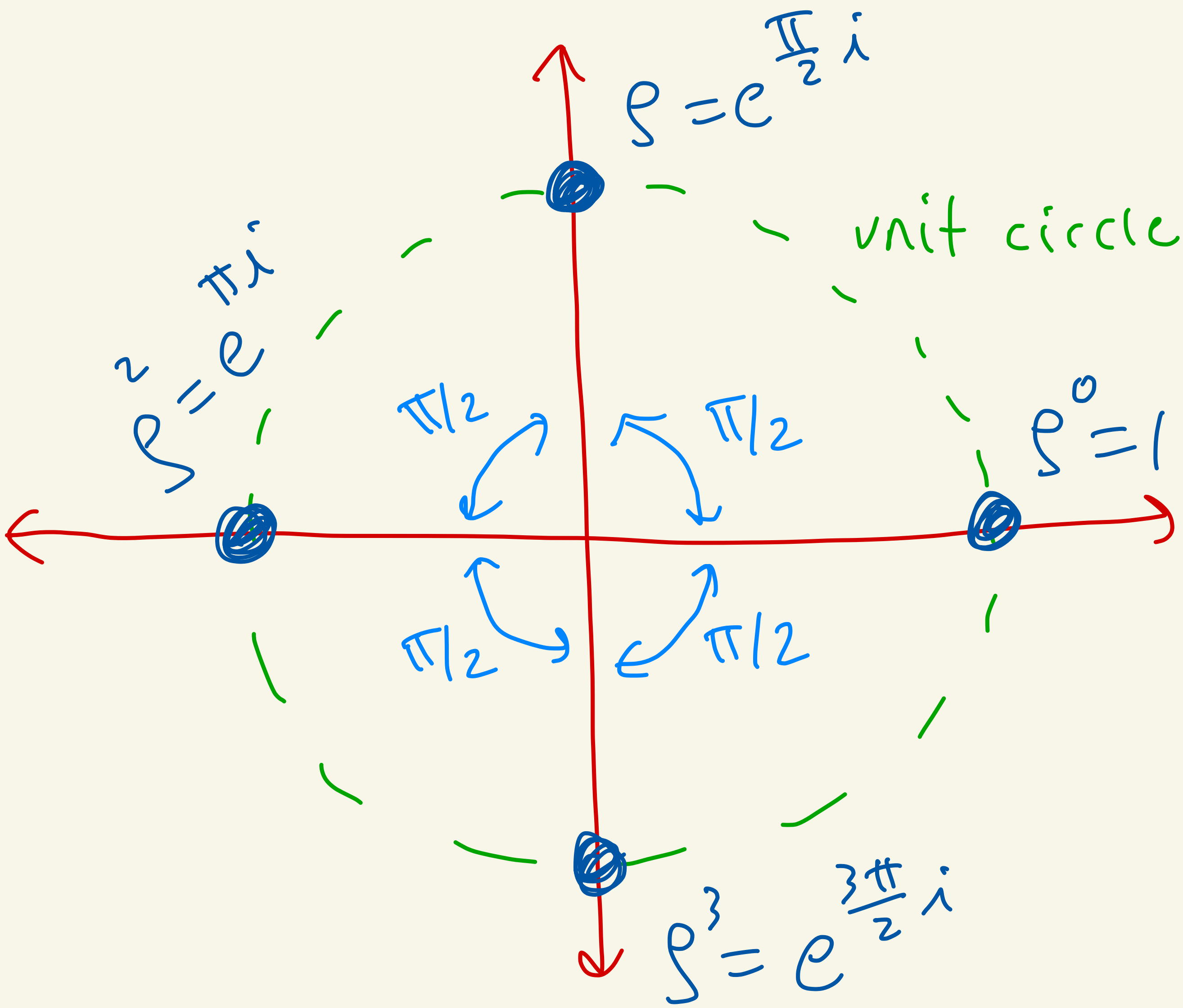
$\rho^{-1} = \rho^2$

$(\rho^2)^{-1} = \rho$

$1^{-1} = 1$

Ex: $U_4 = \{\rho^0, \rho^1, \rho^2, \rho^3\} = \{1, \rho, \rho^2, \rho^3\}$

where $\rho = e^{\frac{2\pi}{4}i} = e^{\frac{\pi}{2}i}$



Here $\rho^4 = 1$.

So for example, $\rho^3 \rho^2 = \rho^5 = \rho^4 \rho = \rho$

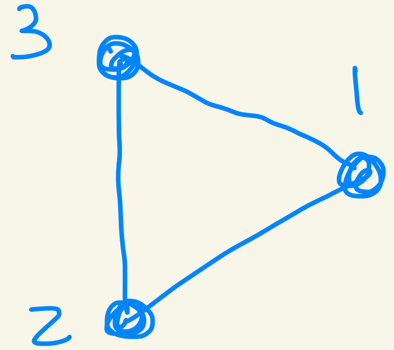
And $(\rho^3)^{-1} = \rho$ because $\rho^3 \rho = \rho^4 = 1$

Example: Dihedral groups

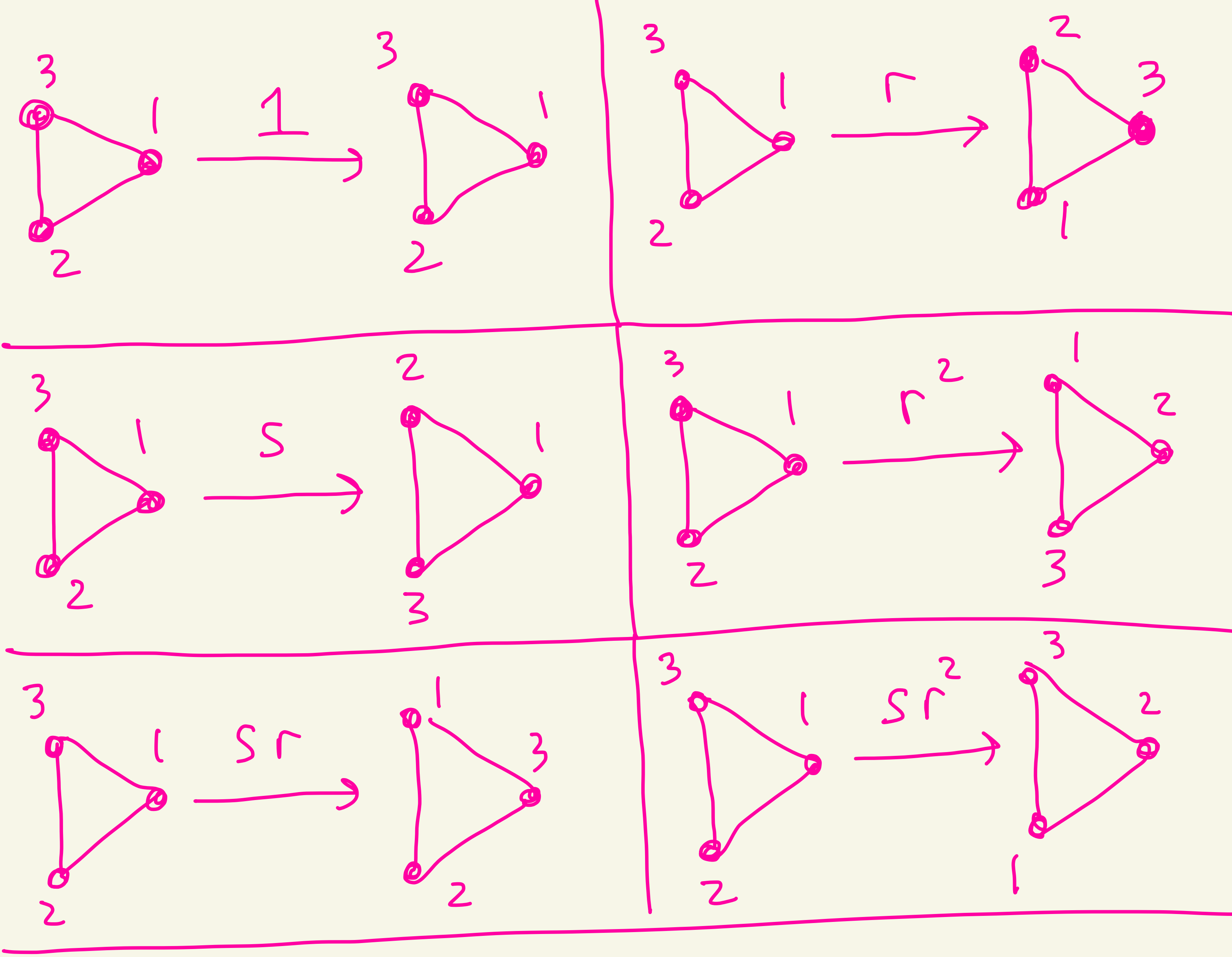
Let $n \geq 3$. The dihedral group D_{2n} is the set of symmetries of the regular n-gon (an n-sided polygon with each side of equal length, ex: equilateral triangle, square, pentagon, hexagon, etc).

The operation on two symmetries is function composition.

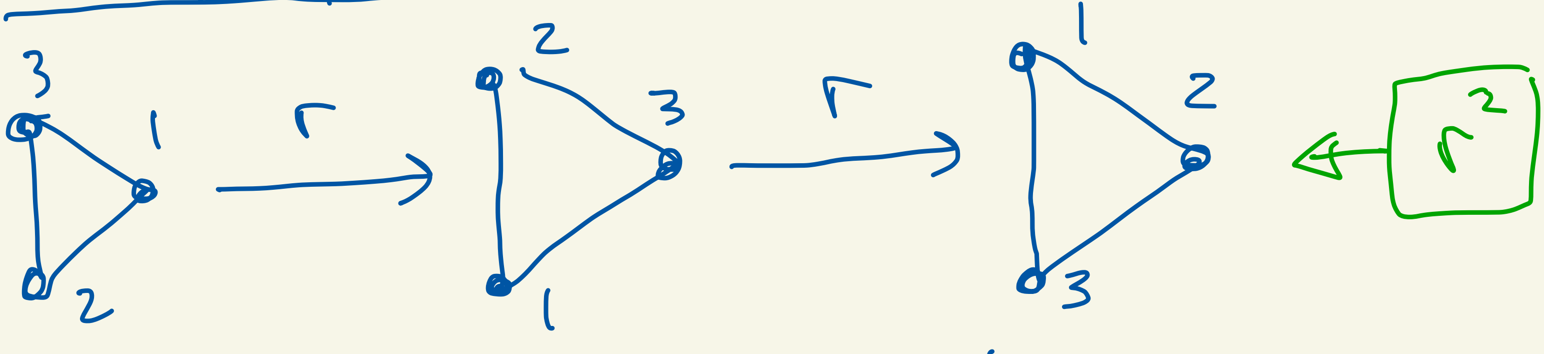
Let's look at D_6 $(n=3)$, the symmetries of an equilateral triangle

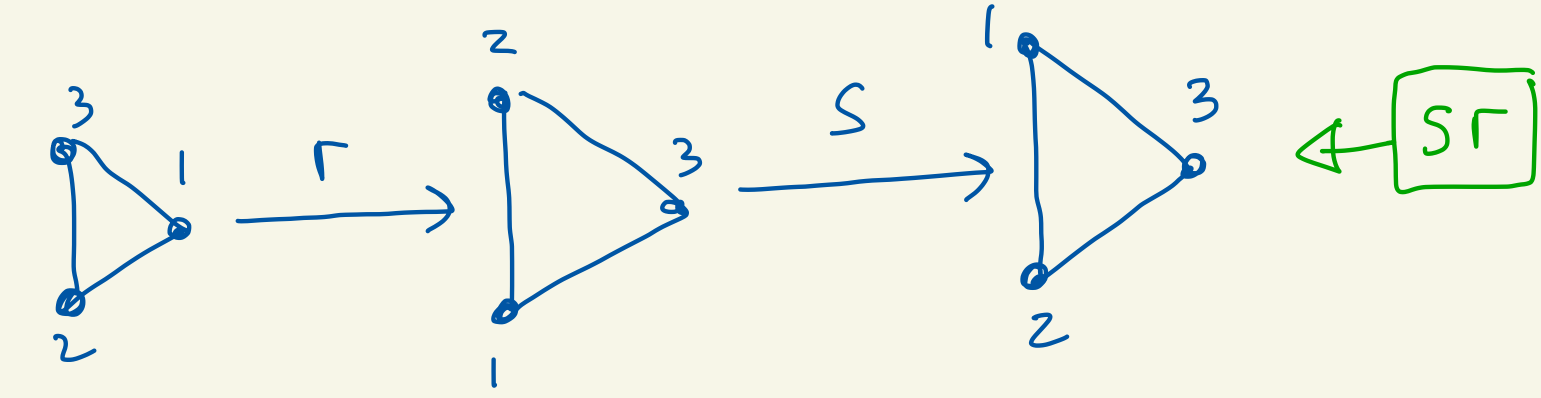


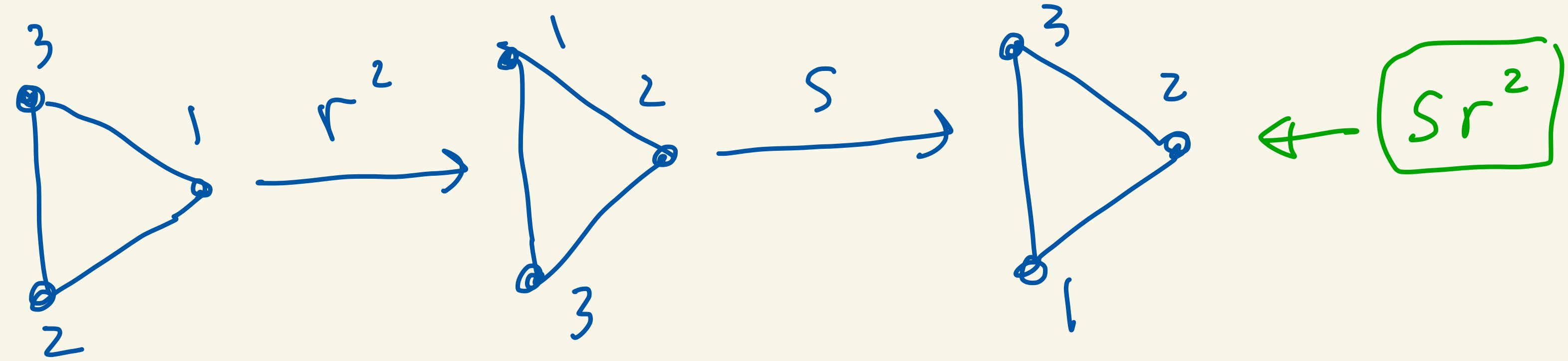
3-gon



Example products:







Here $D_6 = \{1, r, r^2, s, sr, sr^2\}$

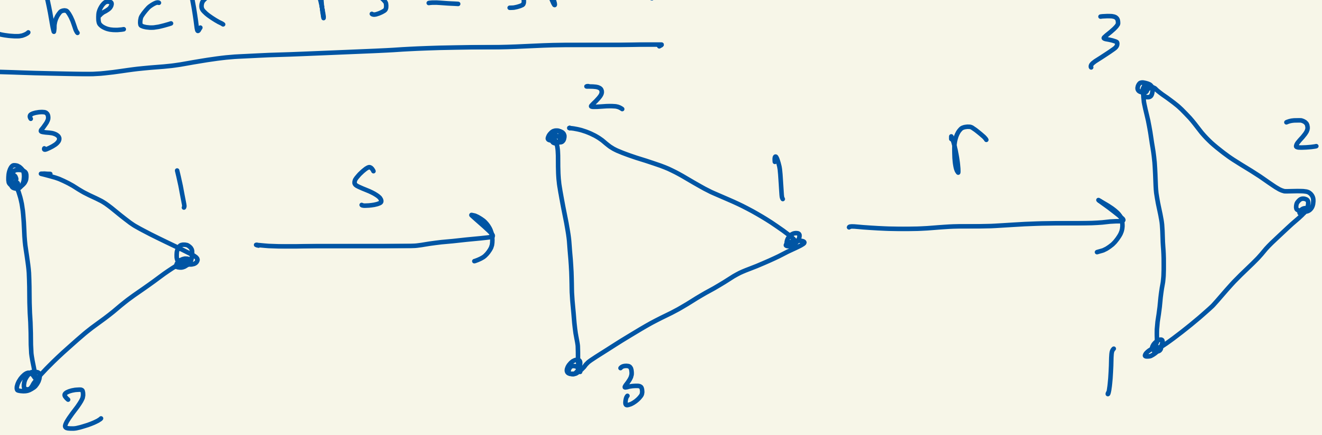
where 1 is the identity function,

$r^3 = 1$, $s^2 = 1$. So, $\underbrace{r^{-1} = r^2}_{\text{since } rr^2 = 1}$

and $\underbrace{s^{-1} = s}_{\text{since } ss = 1}$.

Also, $rs = sr^{-1} = sr^2$ and $r^2 s = sr^{-2} = sr$

Check $rs = sr^2$:



Let's do some calculations in

$D_6 = \{1, r, r^2, s, sr, sr^2\}$

Main things to use are:

$s^2 = 1$, $r^3 = 1$, $rs = sr^{-1}$, $r^2 s = sr^{-2}$

$r^{-1} = r^2$, $r^{-2} = r$

Here we go:

$$r^2 s r^3 = s r^{-2} r^3 = sr$$

$$(sr)(sr) = s\underline{rs}r = s\underline{sr^{-1}}r = s^2 = 1$$

$$(sr)(r^2) = sr^3 = s$$

$$(r^2)(sr) = \underline{r^2 s}r = sr^{-2}r = sr^{-1} \overset{r^3=1}{=} sr^{3-1} = sr^2$$

Note $(sr)(r^2) \neq (r^2)(sr)$ so D_6 is not abelian.

In HW you will calculate the group table for D_6.

For general D_{2n}, $n \geq 3$ we have:

$$D_{2n} = \{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}$$

where

$$r^n = 1$$

$$s^2 = 1$$

$$r^{-k} = r^{n-k}$$

$$r^k s = s r^{-k} = s r^{n-k}$$

For a derivation of these facts see the free Judson textbook. It's in section 5.2.

<u>Ex:</u> $D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$

$r^4 = 1$, $s^2 = 1$

some computations:

$$r^2 s r^3 = s r^{-2} r^3 = sr$$

$$s(sr^2)(sr) = s^2 r^2 sr = r^2 sr = s r^{-2} r = s r^{-1}$$

$$= s r^{4-1} = s r^3$$

$\boxed{r^4 = 1}$

Let's review some Math 2550 so we can look at matrix groups

Given two matrices $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$, then

$$AB = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} e & f \\ g & h \end{pmatrix}$$

$$= \begin{pmatrix} (a\ b)\cdot\begin{pmatrix} e \\ g \end{pmatrix} & (a\ b)\cdot\begin{pmatrix} f \\ h \end{pmatrix} \\ (c\ d)\cdot\begin{pmatrix} e \\ g \end{pmatrix} & (c\ d)\cdot\begin{pmatrix} f \\ h \end{pmatrix} \end{pmatrix}$$

For example,

$$\begin{pmatrix} 1 & 1 \\ -1 & 3 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 4 & -3 \end{pmatrix} = \begin{pmatrix} (1\ 1)\begin{pmatrix} 2 \\ 4 \end{pmatrix} & (1\ 1)\begin{pmatrix} 0 \\ -3 \end{pmatrix} \\ (-1\ 3)\begin{pmatrix} 2 \\ 4 \end{pmatrix} & (-1\ 3)\begin{pmatrix} 0 \\ -3 \end{pmatrix} \end{pmatrix}$$

$$= \begin{pmatrix} 1\cdot 2 + 1\cdot 4 & 1\cdot 0 + 1\cdot(-3) \\ -1\cdot 2 + 3\cdot 4 & -1\cdot 0 + 3(-3) \end{pmatrix} = \begin{pmatrix} 6 & -3 \\ 10 & -6 \end{pmatrix}$$

Recall that $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity matrix.

A matrix A is invertible if there exists a matrix B where

$$AB = I = BA.$$

Furthermore, $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is invertible iff $\det(A) = ad - bc \neq 0$

And if this is the case then

$$A^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

For example, if $A = \begin{pmatrix} 1 & -1 \\ 2 & 3 \end{pmatrix}$

then $\det(A) = 3 - (-2) = 5 \neq 0$.

So, A is invertible and

$$A^{-1} = \frac{1}{5} \begin{pmatrix} 3 & 1 \\ -2 & 1 \end{pmatrix} = \begin{pmatrix} 3/5 & 1/5 \\ -2/5 & 1/5 \end{pmatrix}$$

Another fact is

$$\det(AB) = \det(A)\det(B)$$

when A, B are matrices.

$\boxed{\text{END OF 2550 FACTS}}$

<u>Theorem:</u> Let

$$GL(2,\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \,\middle|\, \begin{array}{l} a,b,c,d \in \mathbb{R} \\ ad-bc \neq 0 \end{array} \right\}$$

be the set of 2×2 matrices will real number coefficients that have non-zero determinant.

Then, $GL(2,\mathbb{R})$ is a group under matrix multiplication. The identity element is $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and if $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2,\mathbb{R})$ then $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

Proof: (Skip in class)

① Let $A,B \in GL(2,\mathbb{R})$ with $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $B=\begin{pmatrix} e & f \\ g & h \end{pmatrix}$

Then $AB=\begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+gh \end{pmatrix}$ has real number entries

Also since $A,B \in GL(2,\mathbb{R})$ we know

$\det(A) \neq 0$ and $\det(B) \neq 0$.

Thus, $\det(AB) = \det(A)\det(B) \neq 0$.

So, $AB \in GL(2,\mathbb{R})$.

② Let $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}, B=\begin{pmatrix} e & f \\ g & h \end{pmatrix}, C=\begin{pmatrix} i & j \\ k & l \end{pmatrix} \in GL(2,\mathbb{R})$.

Then,

$$A(BC) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} ei+fk & ej+fl \\ gi+hk & gj+hl \end{pmatrix}$$

$$= \begin{pmatrix} aei+afk+bgi+bhk & aej+afl+bgj+bhl \\ cei+cfk+dgi+dhk & cej+cfl+cgj+chl \end{pmatrix}$$

$$= \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}\begin{pmatrix} i & j \\ k & l \end{pmatrix}$$

$$= (AB)C$$

③ $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in GL(2,\mathbb{R})$

④ Let $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2,\mathbb{R})$. Then, $ad-bc \neq 0$.

Set $B = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Then, $\det(B) = \frac{da}{(ad-bc)^2} - \frac{bc}{(ad-bc)^2} = \frac{1}{ad-bc} \neq 0$.

So, $B \in GL(2,\mathbb{R})$. And

$$AB = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} d/(ad-bc) & -b/(ad-bc) \\ -c/(ad-bc) & a/(ad-bc) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$BA = \begin{pmatrix} d/(ad-bc) & -b/(ad-bc) \\ -c/(ad-bc) & a/(ad-bc) \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Thus, B is an inverse for A.

By ①-④, $GL(2,\mathbb{R})$ is a group under matrix mult. $\blacksquare$

Some calculations in $GL(2,\mathbb{R})$.

$$A = \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}, \quad B = \begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix}$$

$\det(A) = -1 \neq 0$ so $A \in GL(2,\mathbb{R})$

$\det(B) = 4-2 = 2 \neq 0$ so $B \in GL(2,\mathbb{R})$

$$AB = \begin{pmatrix} 2+2 & 2+4 \\ -1 & -2 \end{pmatrix} = \begin{pmatrix} 4 & 6 \\ -1 & -2 \end{pmatrix}$$

$$BA = \begin{pmatrix} 2+0 & 4-2 \\ 1+0 & 2-2 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 1 & 0 \end{pmatrix}$$

$AB \neq BA$

$GL(2,\mathbb{R})$ is not abelian!

$$A^{-1} = \frac{1}{-1}\begin{pmatrix} -1 & -2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}$$

$$B^{-1} = \frac{1}{2}\begin{pmatrix} 2 & -2 \\ -1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ -1/2 & 1 \end{pmatrix}$$

Theorem: Let $\langle G, * \rangle$ be a group.

Then:

① The identity element e is unique.

② Each element $a \in G$ has a unique inverse which we will denote by a^{-1}.

③ If $a \in G$, then $(a^{-1})^{-1} = a$

④ If $a, b \in G$, then $(a * b)^{-1} = b^{-1} * a^{-1}$

---

proof:

① Suppose $e_1, e_2 \in G$ are both identities.

That is,

$$e_1 * a = a * e_1 = a$$
$$e_2 * a = a * e_2 = a$$

for every $a \in G$.

Then, $e_1 \underbrace{=}_{\boxed{a = a * e_2}} e_1 * e_2 \underbrace{=}_{\boxed{e_1 * a = a}} e_2$

(2) Let $a \in G$. Suppose b_1, b_2 are both inverses for a.

Then,

$$a * b_1 = b_1 * a = e$$
$$a * b_2 = b_2 * a = e$$

Thus,

$$a * b_1 = e = a * b_2$$

multiply by b_1 on the left to get

$$b_1 * (a * b_1) = b_1 * (a * b_2)$$

Then by associativity

$$\underbrace{(b_1 * a)}_{e} * b_1 = \underbrace{(b_1 * a)}_{e} * b_2$$

So, $e * b_1 = e * b_2$

Thus, $b_1 = b_2$.

③ Since

$a * a^{-1} = e$ and $a^{-1} * a = e$

by def of inverse we have $(a^{-1})^{-1} = a$.

④ $(a*b) * (b^{-1} * a^{-1})$

$= ((a*b) * b^{-1}) * a^{-1}$

$= (a * (b * b^{-1})) * a^{-1}$

$= (a * e) * a^{-1}$

$= a * a^{-1}$

$= e$

Thus, $(a*b)^{-1} = b^{-1} * a^{-1}$.

$\blacksquare$

Notation: When dealing with an abstract group $\langle G, * \rangle$ we make the following conventions.

- We will just write ab instead of $a*b$ for simplicity. For example, $aabcbdd$ means $a*a*b*c*b*d*d$.
- By associativity we never need to use parentheses anymore.
- If n is positive integer, then

$$a^n = \underbrace{aaa \cdots a}_{n \text{ times}}$$

$$a^{-n} = \underbrace{(a^{-1})(a^{-1})(a^{-1}) \cdots (a^{-1})}_{n \text{ times}}$$

$$a^0 = e$$

For example,

$$a^3 = aaa$$

$$a^{-4} = a^{-1}a^{-1}a^{-1}a^{-1}$$

$$a^{-1}a^3b^{-3}c^2 = a^{-1}aaab^{-1}b^{-1}b^{-1}cc$$

In HW 1 we will still see the $*$ notation in proofs for abstract groups but after that we will drop the notation.