On homework and tests in this class you will be asked to <u>prove</u> things about groups. Let's do an example.

§4 (29) Suppose G is a finite group. Prove the following: If $|G|$ is even, then there is an element $a \in G$ with $a \neq e$ and $a * a = e$.

Let's first look at some examples to get a feel for the question.

<u>Ex</u> $\mathbb{Z}_3 = \{0, 1, 2\}$ $(e = 0)$

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$1 * 1 = 2 \neq e$

$2 * 2 = 1 \neq e$

(But $|\mathbb{Z}_3| = 3$ is odd)

$\mathbb{Z}_4 = \{0, 1, 2, 3\}$

Let $a = 2$

Then $a * a =$

$2 * 2 = 0$

$= e$

$V = \{e, a, b, c\}$

e	e	a	b	c
e	e	a	b	c
a	a	e	c	
b	b	c	e	a
c	c	b	a	e

$a * a = e$

$b * b = e$

$c * c = e$

In the examples above where $|G|$ is even we were always able to find an $a \in G$, $a \neq e$ with $a * a = e$.

<u>Proposition</u> Suppose G is a finite group. If $|G|$ is even then there is an $a \in G$, $a \neq e$ for which $a * a = e$.

Contrapositive Proof

<u>Proof</u> Suppose it's not true that there is an $a \in G$, $a \neq e$ with $a * a = e$. Then $a * a \neq e$ for every $a \in G$

So $a' * (a * a) \neq a' * e$ for every $a \in G$

i.e. $(a' * a) * a \neq a'$ for every $a \in G$

i.e. $e * a \neq a'$ for every $a \in G$

i.e. $a \neq a'$ for every $a \in G$.

Now list the elements of G as $e \quad \begin{matrix} a_1 & a_2 & a_3 & \cdots & a_n \\ a_1' & a_2' & a_3' & \cdots & a_n' \end{matrix}$

Then $|G| = 1 + 2n$ is odd, so $|G|$ is not even. $\blacksquare$

Section 5 Subgroups.

Before getting to today's main topic, its a good time to introduce some notation and conventions

In algebra, the $*$ operator is rarely used. Instead we write $a*b$ as either ab or $a+b$ depending on whether we are thinking more of addition or multiplication.

Convention + is used only for abelian groups.

Notation : $a+a+a+a = 4a$, etc. $a' = -a$ $-5a = 5(-a)$

$aaaa = a^4$, etc. $a' = a^{-1}$ $a^{-5} = (a^{-1})^5$

Thus the usual cacelations apply:

- $3a - 5a = a+a+a-a-a-a-a-a = -a-a = -2a$
- $a^3a^{-5} = aaaa^{-1}a^{-1}a^{-1}a^{-1}a^{-1} = a^{-1}a^{-1}a^{-1} = a^{-2}$

With this in mind, lets get started.

Sub groups

Sometimes a group sits inside a larger group, and both groups use the same operation. When this happens we say the smaller group is a subgroup of the larger one.

Examples $\langle \mathbb{Z}, + \rangle$ subgroup of $\langle \mathbb{R} + \rangle$

$\langle \mathbb{R} + \rangle$ subgroup of $\langle \mathbb{C}, + \rangle$

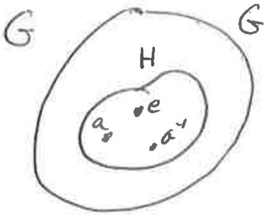
$\langle 2\mathbb{Z}, + \rangle$ subgroup of $\langle \mathbb{Z} + \rangle$

$\langle U \cdot \rangle$ subgroup of $\langle \mathbb{C}^* \cdot \rangle$

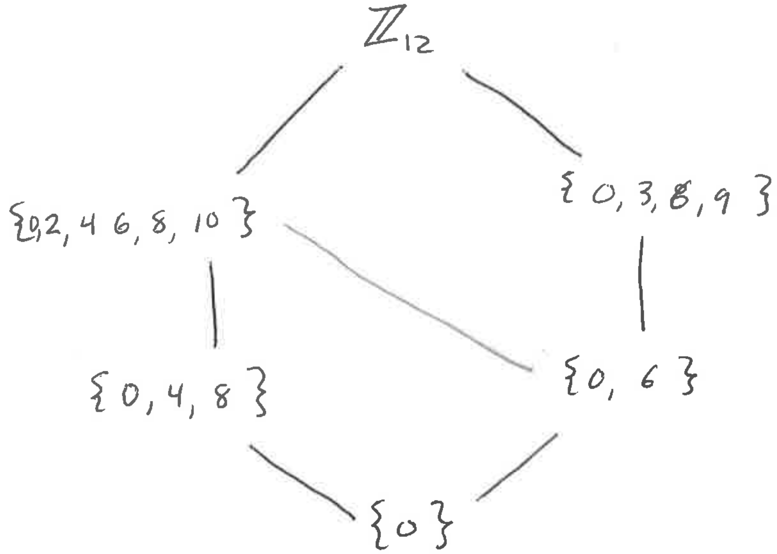
Definition A subset $H \subseteq G$ is a subgroup of G if H is a group under the operation of G. We write this as $H \leq G$

Theorem $H \subseteq G$ is a subgroup of G if and only if

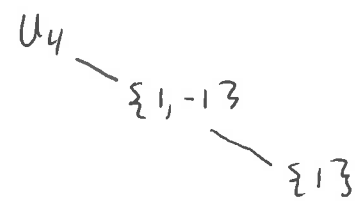
1. H is closed under the binary operation of G
2. Identity element of G is in H
3. If $a \in H$ then $a^{-1} \in H$



Example Find all subgroups of $\mathbb{Z}_{12}$



Example Subgroups of $U_4 = \{1, i, -1, -i\}$



Example Find some subgroups of $\langle \mathbb{Z}, + \rangle$

$H = \{\ldots, -6, -4, -2, 0, 2, 4, 6, 8, \ldots\} = \{2n \mid n \in \mathbb{Z}\} = 2\mathbb{Z}$

$K = \{\ldots, -9, -6, -3, 0, 3, 6, 9, 12, \ldots\} = \{3n \mid n \in \mathbb{Z}\} = 3\mathbb{Z}$

$L = \{\ldots, -12, -8, -4, 0, 4, 8, 12, 16, \ldots\} = \{4n \mid n \in \mathbb{Z}\} = 4\mathbb{Z}$

Ex Subgroup of $\langle \mathbb{R}^*, \cdot \rangle$

$H = \{\ldots, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, 16, \ldots\} = \{2^n \mid n \in \mathbb{Z}\}$

$K = \{\ldots, \frac{1}{9}, \frac{1}{3}, 1, 3, 9, 27, 81, \ldots\} = \{3^n \mid n \in \mathbb{Z}\}$