On homework and tests in this class you will be asked to prove 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 $a \ast a = e$.

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

**Example**

$\mathbb{Z}_3 = \{0, 1, 2\} \quad (e = 0)$

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

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

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

Let $a = 2$

then $a \ast a = 2 \ast 2 = 0 = e$

$1 \ast 1 = 2 \neq e$

$2 \ast 2 = 1 \neq e$

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

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

**Proposition** Suppose $G$ is a finite group.

If $|G|$ is even then there is an $a \in G$, $a \neq e$ for which $a \ast a = e$.

**Proof**

Suppose it's not true that there is an $a \in G$, $a \neq e$ with $a \ast a = e$. Then $a \ast a \neq e$ for every $a \in G$.

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

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

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

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

Now list the elements of $G$ as $e, a_1, a_2, a_3, \ldots, a_n$.

Then $|G| = 1 + 2n$ is odd, so $|G|$ is not even.
Section 5 Subgroups

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

In algebra, the * operator is rarely used. Instead we write \( a \ast b \) 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 calculations apply:

1. \( 3a - 5a = a + a + a - a - a - a - a = -a - a = -2a \)
2. \( a^3 a^{-5} = aaaa a^{-1} a^{-1} a^{-1} a^{-1} = a^{-1} a^{-1} a^{-1} = a^{-2} \)

With this in mind, let's 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**

\(<\mathbb{Z},+>\) subgroup of \(<\mathbb{R},+>\)

\(<\mathbb{R},+>\) subgroup of \(<\mathbb{C},+>\)

\(<2\mathbb{Z},+>\) subgroup of \(<\mathbb{Z},+>\)

\(<\mathbb{U},>\) subgroup of \(<\mathbb{C}^*,>\)

**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: \( H \leq G \) 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 \( < \mathbb{Z}, + > \)

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

\( K = \{\ldots, -3, -1, 0, 3, 6, 9, 12, \ldots \} = \{3n \mid n \in \mathbb{Z}\} = 3\mathbb{Z} \)

\( L = \{\ldots, -12, -6, -3, 0, 3, 6, 9, 12, 15, \ldots \} = \{4n \mid n \in \mathbb{Z}\} = 4\mathbb{Z} \)

Example: Subgroup of \( < \mathbb{R}^*, \cdot > \)

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

\( K = \{\ldots, \frac{1}{8}, \frac{1}{2}, 1, 3, 9, 27, 81, \ldots \} = \{3^n \mid n \in \mathbb{Z}\} \)