

## Subgroups and Cyclic Groups

(Section 2.2)

Recall: (subspaces) If  $V$  is a vector space, a **Subspace** of  $V$  is a potentially smaller subset of  $V$  that is a vector space under the operations of  $V$ . We want the analogous construction for groups.

Definition : ( subgroup and notation)

Let  $G$  be a group under  
" $\cdot$ ". A nonempty subset  
 $H$  of  $G$  is said to be  
a **Subgroup** if  $H$  is  
a group under " $\cdot$ ".  
Notation: " $H \subseteq G$ "

Theorem: (subgroup test) Let  $G$  be a group under " $\cdot$ " and let  $H$  be a nonempty subset of  $G$ . Then  $H$  is a subgroup of  $G$  if and only if both

$\rightarrow 1)$  if  $x, y \in H$ , then  $x \cdot y \in H$

$\rightarrow 2)$  if  $x \in H$ , then  $x^{-1} \in H$ .

proof:  $\Rightarrow$  trivial, since 1) and 2) correspond to " $\cdot$ " is a binary operation on  $H$  and we know that  $x^{-1} \in H$  from the group axioms

$\leftarrow$  from 1), we know that " $\cdot$ " is a binary operation on  $H$ . From 2), we know that  $x^{-1} \in H$  ( $x^{-1}$  exists since  $x \in H \subseteq G$ , and we know  $G$  is a group).

We need to check that " $\cdot$ " is associative and that  $\exists$  identity  $e_H$  for  $H$ . However, since  $G$  is a group under " $\cdot$ ", we know " $\cdot$ " is associative on elements of  $G$ .

So in particular, “.” is associative on elements of  $H$ .

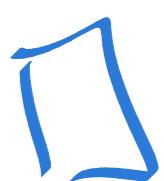
Now combining 1) and 2),

if  $x \in H$ ,  $x^{-1} \in H$ , and

$$x \cdot x^{-1} = e_6 \in H.$$

Therefore,  $e_6 \in H$  and

is the identity of  $H$ .



**Terminology:** if  $G$  is a group under " $\cdot$ " and  $\emptyset \neq S \subseteq G$ ,  
then if  $x \cdot y \in S \wedge x^{-1} \cdot y \in S$ ,  
we say  $S$  is **closed**  
under " $\cdot$ ".

Example 1:  $\{a + b\sqrt{17} \mid a, b \in \mathbb{Q}\}$

$\subseteq \mathbb{R}^*$  is a subgroup

of  $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ .

Why? Use the subgroup test!

Let  $a+b\sqrt{17}, c+d\sqrt{17} \in \mathbb{R}^*$ ,

$a, b, c, d \in \mathbb{Q}$ . Then

$$(a+b\sqrt{17}) \cdot (c+d\sqrt{17})$$

$$= (a \cdot c + b \cdot d \cdot \cancel{17}) + (ad + bc)\sqrt{17}$$

$\in \mathbb{Q}$

Since  $\mathbb{Q}$  is a field,

$$a \cdot c + 17 b \cdot d, ad+bc \in \mathbb{Q}.$$

Therefore, we have closure  
under multiplication.

Inverses: Take  $a+b\sqrt{17}$ ,  $a,b \in \mathbb{Q}$ .

We know in  $\mathbb{R}^*$ ,

$$(a+b\sqrt{17})^{-1} = \frac{1}{a+b\sqrt{17}}.$$

Multiply by  $1 = \frac{a-b\sqrt{17}}{a-b\sqrt{17}}$

We get

$$(a+b\sqrt{17})^{-1} = \frac{a-b\sqrt{17}}{a^2 - b^2 \cdot 17}$$

and

$$(a + b\sqrt{17})^{-1} = \frac{a}{a^2 - b^2 \cdot 17} + \left( \frac{-b}{a^2 - b^2 \cdot 17} \right) \sqrt{17}$$

Since  $\mathbb{Q}$  is a field,

$$\frac{a}{a^2 - b^2 \cdot 17}, \frac{-b}{a^2 - b^2 \cdot 17} \in \mathbb{Q}$$

unless  $a^2 - b^2 \cdot 17 = 0$ !

But if this were so,

then  $a^2 = b^2 \cdot 17$

$$\frac{a^2}{b^2} = 17$$

and  $\sqrt{17}$  would be rational, which is not true! So therefore,

$(a+b\sqrt{17})^{-1}$  has the desired form. By

the subgroup test,

$\{a+b\sqrt{17} \mid a, b \in \mathbb{Q}\}$   
is a subgroup of  $\mathbb{R}^+$ !

Example 2 : ( subgroups of any group  
and simple groups)

Let  $G$  be a group under  
" . ".  $G$  always has  
at least two subgroups;  
 $G$  itself and  $H = \{e_G\}$ .

By the subgroup test,

$$e_G^{-1} = e_G \in H$$

$$e_G \cdot e_G = e_G \in H, \text{ so}$$

$\{e_G\}$  is a subgroup.