

5. SUBGROUPS

A *subgroup* is a subset H of a group G which is closed under the operation (the one that makes G into a group) and which satisfies the definition of a group. Since associativity is automatic, the definition can be stated as follows.

5.1. definition and examples.

Definition 5.1. A **subgroup** of a group G is defined to be a subset H with the following properties.

- (1) H is closed under multiplication in the group.
- (2) H contains the identity e
- (3) H contains the inverse h^{-1} of any element $h \in H$.

We write $H \leq G$. ($H < G$ means H is a proper subgroup of G , in other words, H is not the whole group.)

The first conditions is usually written:

$$HH \subseteq H$$

The notation means:

$$HH := \{h_1h_2 \mid h_1, h_2 \in H\}$$

In general AB means the set of all products ab where $a \in A$ and $b \in B$.

The third condition is written:

$$H^{-1} \subseteq H$$

Other examples of this set notation are:

$$aB = \{ab \mid b \in B\}$$

$$a + B = \{a + b \mid b \in B\}$$

Examples of subgroups are:

- (1) $n\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$.
- (2) U_n is a subgroup of (U, \cdot) .
- (3) $SL(n, \mathbb{Z}) < GL(n, \mathbb{Z})$ where $SL(n, \mathbb{Z})$ is the group of $n \times n$ integer matrices with determinant 1.

Theorem 5.2. A subset H of a group G is a subgroup if and only if it is nonempty and satisfies

$$H^{-1}H \subseteq H.$$

The notation means:

$$H^{-1}H = \{h_1^{-1}h_2 \mid h_1, h_2 \in H\}.$$

Proof. We want to show that H is closed under multiplication, has the identity e and is also closed under inverse. Associativity is automatic since $H \subseteq G$.

- (1) ($e \in H$) Since H is nonempty, it has some element h . Then $h^{-1}h = e \in H^{-1}H \subseteq H$.
- (2) (H is closed under inverse.) Since $e \in H$, $H^{-1} = H^{-1}e \subseteq H^{-1}H \subseteq H$. Also, $H \subseteq H^{-1}$ since each $h \in H$ is equal to $(h^{-1})^{-1} \in H^{-1}$. Thus $H = H^{-1}$.
- (3) (H is closed.) $HH = H^{-1}H \subseteq H$.

Thus, H is a subgroup of G . □

5.2. cyclic subgroup. If a is an element of a group G then the set of all powers of a forms a subgroup denoted $\langle a \rangle$ and called the *cyclic subgroup generated by a* :

$$\langle a \rangle := \{a^n \mid n \in \mathbb{Z}\}$$

Why is this a subgroup?

Take the group U of complex numbers with absolute value 1. What is $\langle i \rangle$? What happened to the negative powers of i ?

If we can find an element of the group $a \in G$ so that $G = \langle a \rangle$ then G is called a **cyclic group** with generator a . For example \mathbb{Z}_n is a cyclic group (under addition) with generator 1. Can you find another generator?

The Klein four group is often denoted V (for **v**ier). I would call it the 2-bit addition group:

$$V = \{00, 01, 10, 11\}$$

with addition given on each coordinate without carrying. The elements form a square.

Find all cyclic subgroups of V . Conclude that V is not a cyclic group.

If we add a parity bit (the sum of the digits) V becomes isomorphic to a subgroup of the 3-bit addition group:

$$H = \{000, 011, 101, 110\} < \{a_1a_2a_3 \mid a_i = 0 \text{ or } 1\}$$

If we draw a picture we would see that H forms a tetrahedron inside a cube. This demonstrates the three fold symmetry of the Klein 4-group V . (In general the n -bit addition group has $n + 1$ fold symmetry.)