MATH 433

Applied Algebra

Lecture 28:
Subgroups.
Cyclic groups.

Subgroups

Definition. A group H is a called a **subgroup** of a group G if H is a subset of G and the group operation on H is obtained by restricting the group operation on G. Notation: $H \leq G$.

Proposition If H is a subgroup of G then **(i)** the identity element in H is the same as the identity element in G;
(ii) for any $g \in H$ the inverse g^{-1} taken in H is the same as the inverse taken in G.

Proof. Let e_G be the identity element of G and e_H be the identity element of H. Then $e_G e_H = e_H$ in G. Further, $e_H e_H = e_H$ in H (but also in G). Hence $e_G e_H = e_H e_H$ in G. By right cancellation in G, $e_G = e_H$.

Now take any $g \in H$. Let g' be the inverse of g in G and g'' be the inverse of g in H. Then $g'g = e_G$ in G and $g''g = e_H = e_G$ in H (but also in G). Hence $g'g = g''g$ in G. By right cancellation in G, $g' = g''$.

Examples of subgroups: • $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{R}, +)$.

• $(\mathbb{Q} \setminus \{0\}, \times)$ is a subgroup of $(\mathbb{R} \setminus \{0\}, \times)$.

• The alternating group $A(n)$ is a subgroup of the symmetric group $S(n)$.

• If V_0 is a subspace of a vector space V, then it is also a subgroup of the additive group V.

• Any group G is a subgroup of itself.

• If e is the identity element of a group G, then $\{e\}$ is the **trivial** subgroup of G.

Counterexamples: • $(\mathbb{R} \setminus \{0\}, \times)$ is not a subgroup of $(\mathbb{R}, +)$ since the operations do not agree.

• $(\mathbb{Z}_n, +)$ is not a subgroup of $(\mathbb{Z}, +)$ since $\mathbb{Z}_n$ is not a subset of $\mathbb{Z}$ (although every element of $\mathbb{Z}_n$ is a subset of $\mathbb{Z}$).

• $(\mathbb{Z} \setminus \{0\}, \times)$ is not a subgroup of $(\mathbb{R} \setminus \{0\}, \times)$ since $(\mathbb{Z} \setminus \{0\}, \times)$ is not a group (it is a **subsemigroup**).

Theorem Let H be a subset of a group G and define an operation on H by restricting the group operation of G. Then the following statements are equivalent:

(i) H is a subgroup of G;

(ii) H contains e and is closed under the operation and under taking the inverse, that is, $g, h \in H \implies gh \in H$ and $g \in H \implies g^{-1} \in H$;

(iii) H is nonempty and $g, h \in H \implies gh^{-1} \in H$.

Proof. **(i)** $\Longrightarrow$ **(ii)** If H is a subgroup of G, then $g, h \in H \implies gh \in H$ since the operations agree and H satisfies the closure axiom. Further, $e \in H$ since e is also the identity element in H and $g \in H \implies g^{-1} \in H$ since g^{-1} is also the inverse of g in H.

(ii) $\Longrightarrow$ **(i)** By construction, H is a subgroup of G as soon as it is a group. (ii) implies the closure axiom, existence of the identity and the inverse. Associativity is inherited from G.

Theorem Let H be a subset of a group G and define an operation on H by restricting the group operation of G. Then the following statements are equivalent:

(i) H is a subgroup of G;

(ii) H contains e and is closed under the operation and under taking the inverse, that is, $g, h \in H \implies gh \in H$ and $g \in H \implies g^{-1} \in H$;

(iii) H is nonempty and $g, h \in H \implies gh^{-1} \in H$.

Proof. **(ii)** $\Longrightarrow$ **(iii)** is obvious.

(iii) $\Longrightarrow$ **(ii)** Take any $h \in H$. Then $e = hh^{-1} \in H$ and $h^{-1} = eh^{-1} \in H$. Further, for any $g \in H$ we have $gh = g(h^{-1})^{-1} \in H$.

Intersection of subgroups

Theorem 1 Let H_1 and H_2 be subgroups of a group G. Then the intersection $H_1 \cap H_2$ is also a subgroup of G.

Proof: The identity element e of G belongs to every subgroup. Hence $e \in H_1 \cap H_2$. In particular, the intersection is nonempty. Now for any elements g and h of the group G,
$g, h \in H_1 \cap H_2 \implies g, h \in H_1$ and $g, h \in H_2$
$\implies gh^{-1} \in H_1$ and $gh^{-1} \in H_2 \implies gh^{-1} \in H_1 \cap H_2$.

Theorem 2 Let H_α, $\alpha \in A$ be a nonempty collection of subgroups of the same group G (where the index set A may be infinite). Then the intersection $\bigcap_\alpha H_\alpha$ is also a subgroup of G.

Generators of a group

Let S be a set (or a list) of some elements of a group G. The **group generated by** S, denoted $\langle S \rangle$, is the smallest subgroup of G that contains the set S. The elements of the set S are called **generators** of the group $\langle S \rangle$.

Theorem 1 The group $\langle S \rangle$ is well defined. Indeed, it is the intersection of all subgroups of G that contain S.

Note that we have at least one subgroup of G containing S, namely, G itself. If it is the only one, i.e., $\langle S \rangle = G$, then S is called a **generating set** for the group G.

Theorem 2 If S is nonempty, then the group $\langle S \rangle$ consists of all elements of the form $g_1 g_2 \dots g_k$, where each g_i is either a generator $s \in S$ or the inverse s^{-1} of a generator.

Example. Suppose $S = \{a, b, c\}$. Let $g = abc^{-1}a$ and $h = bcba^{-1}$. Then $gh = abc^{-1}abcba^{-1}$, $hg = bcb^2c^{-1}a$, $g^2 = abc^{-1}a^2bc^{-1}a$, $g^{-1} = a^{-1}cb^{-1}a^{-1}$.

Cyclic groups

A **cyclic group** is a group generated by a single element.

Cyclic group: $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$ (in multiplicative notation) or $\langle g \rangle = \{ng : n \in \mathbb{Z}\}$ (in additive notation).

Any cyclic group is Abelian since $g^k g^m = g^{k+m} = g^m g^k$ for all $k, m \in \mathbb{Z}$.

If g has finite order n, then the cyclic group $\langle g \rangle$ consists of n elements $g, g^2, \dots, g^{n-1}, g^n = e$.

If g is of infinite order, then $\langle g \rangle$ is infinite.

Examples of cyclic groups: $\mathbb{Z}$, $3\mathbb{Z}$, $\mathbb{Z}_5$, G_7, $S(2)$, $A(3)$.

Examples of noncyclic groups: any uncountable group, any non-Abelian group, G_8 with multiplication, $\mathbb{Q}$ with addition, $\mathbb{Q} \setminus \{0\}$ with multiplication.

Subgroups of a cyclic group

Theorem Every subgroup of a cyclic group is cyclic as well.

Proof: Suppose that G is a cyclic group and H is a subgroup of G. Let g be the generator of G, $G = \{g^n : n \in \mathbb{Z}\}$. Denote by k the smallest positive integer such that $g^k \in H$ (if there is no such integer then $H = \{e\}$, which is a cyclic group). We are going to show that $H = \langle g^k \rangle$.

Since $g^k \in H$, it follows that $\langle g^k \rangle \subset H$. Let us show that $H \subset \langle g^k \rangle$. Take any $h \in H$. Then $h = g^n$ for some $n \in \mathbb{Z}$. We have $n = kq + r$, where q is the quotient and r is the remainder after division of n by k $(0 \leq r < k)$. It follows that $g^r = g^{n-kq} = g^n g^{-kq} = h(g^k)^{-q} \in H$. By the choice of k, we obtain that $r = 0$. Thus $h = g^n = g^{kq} = (g^k)^q \in \langle g^k \rangle$.

Examples

- Integers $\mathbb{Z}$ with addition.

The group is cyclic, $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$. The proper cyclic subgroups of $\mathbb{Z}$ are: the trivial subgroup $\{0\} = \langle 0 \rangle$ and, for any integer $m \geq 2$, the group $m\mathbb{Z} = \langle m \rangle = \langle -m \rangle$. These are all subgroups of $\mathbb{Z}$.

- $\mathbb{Z}_5$ with addition.

The group is cyclic, $\mathbb{Z}_5 = \langle [1] \rangle = \langle [-1] \rangle = \langle [2] \rangle = \langle [-2] \rangle$. The only proper subgroup is the trivial subgroup $\{[0]\} = \langle [0] \rangle$.

- G_7 with multiplication.

The group is cyclic, $G_7 = \langle [3]_7 \rangle$. Indeed, $[3]^2 = [9] = [2]$, $[3]^3 = [6]$, $[3]^4 = [4]$, $[3]^5 = [5]$, and $[3]^6 = [1]$. Also, $G_7 = \langle [3]^{-1} \rangle = \langle [5] \rangle$. Proper subgroups are $\{[1], [2], [4]\}$, $\{[1], [6]\}$, and $\{[1]\}$.