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.

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.

Theorem Let H be a nonempty subset of a group G and define an operation on H by restricting the group operation of G. Then the following are equivalent:
(i) H is a subgroup of G;
(ii) H 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) $g, h \in H \implies gh^{-1} \in H$.

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 $S(n)$.

• The special linear group $SL(n, \mathbb{R})$ is a subgroup of the general linear group $GL(n, \mathbb{R})$.

• 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**).

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,

$$g, h \in H_1 \cap H_2 \implies g, h \in H_1 \text{ and } g, h \in H_2$$
$$\implies gh^{-1} \in H_1 \text{ and } gh^{-1} \in H_2 \implies gh^{-1} \in H_1 \cap H_2.$$

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.

Theorem The symmetric group $S(n)$ is generated by two permutations: $\tau = (1\ 2)$ and $\pi = (1\ 2\ 3\ \ldots\ n)$.

Proof: Let $H = \langle \tau, \pi \rangle$. We have to show that $H = S(n)$.

First we obtain that $\alpha = \tau\pi = (2\ 3\ \ldots\ n)$. Then we observe that $\sigma(1\ 2)\sigma^{-1} = (\sigma(1)\ \sigma(2))$ for any permutation σ.
In particular, $(1\ k) = \alpha^{k-2}(1\ 2)(\alpha^{k-2})^{-1}$ for $k = 2, 3 \ldots, n$.
It follows that the subgroup H contains all transpositions of the form $(1\ k)$.

Further, for any integers $2 \le k < m \le n$ we have $(k\ m) = (1\ k)(1\ m)(1\ k)$. Therefore the subgroup H contains all transpositions. Finally, every permutation in $S(n)$ is a product of transpositions, therefore it is contained in H.
Thus $H = S(n)$.

Remark. Although the group $S(n)$ is generated by two elements, its subgroups need not be generated by two elements.

Cyclic groups

A **cyclic group** is a subgroup 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 $g^n g^m = g^{n+m} = g^m g^n$ for all $m, n \in \mathbb{Z}$.

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 $H = \langle g^k \rangle$.

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 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 $\{[1]\}$.