Hilfsätze

Theorem A. Let H be a subgroup of G. A left coset of H is a set of the form $aH = L_a(H) = \{ah \mid h \in H\}$ for some $a \in G$.

(a) Any two left cosets of H in G are disjoint or equal. G is the union of the left cosets of H in G.

(b) All left cosets of H in G have the same size.

(c) (Lagrange's theorem) If G is finite, then $|H|$ divides $|G|$.

Definition A′. The number of left cosets of H in G is called the *index* of H in G, written $[G : H]$. If G is finite, then $[G : H] = |G|/|H|$.

Theorem E. Let $f : G \to H$ be a homomorphism. Then each preimage $f^{-1}(h)$, $h \in H$, is either empty, or it is the same size as $\ker(f)$.

Theorem F (Spin-Orbit Theorem). Let $G \times X \to X$ be an action of the group G on the set X. The *orbit* of an element $x \in X$ is the set $G \cdot x = \{gx \mid g \in G\}$. The *stabilizer* of x is the subgroup $G_x = \{g \in G \mid gx = x\}$.

(a) Any two orbits are disjoint or equal.

(b) (Spin-orbit formula) If G is finite, then for each $x \in X$, $|G| = |G{\cdot}x|\,|G_x|$.

(c) If x and y are in the same orbit, then their stabilizers G_x and G_y are conjugate. Conversely, every subgroup conjugate to G_x is the stabilizer of some point y in the orbit of x.

Theorem M.

(a) Every permutation σ can be written as a product of transpositions:

$$\sigma = \tau_1 \cdots \tau_k,$$

where $\tau_j = (a_j\ b_j)$ is a transposition, $a_j \neq b_j$, $j = 1, \ldots, k$.

(b) A permutation cannot be both even and odd: if

$$\tau_1 \cdots \tau_k = \tau_1' \cdots \tau_{k'}',$$

then $k = k' \pmod 2$.

Corollary M′.

(a) The even permutations form a subgroup A_n in S_n.

(b) There is a parity homomorphism $\mathrm{sgn} : S_n \to \{\pm 1\}$ with kernel A_n.

Definition N. Let $\phi(x) = Ax + b$ be an isometry of $\mathbb{R}^n$, where $A \in \mathbb{R}^{nxn}$ is an orthogonal matrix and $b \in \mathbb{R}^n$ be an isometry of $\mathbb{R}^n$. Define

(a) ϕ is *orientation-preserving* $\iff \det(A) > 0 \iff \det(A) = 1$.

(b) ϕ is *orientation-reversing* $\iff \det(A) < 0 \iff \det(A) = -1$.

Corollary N′.

(a) The orientation-preserving isometries form a subgroup $\mathrm{Isom}_+(\mathbb{R}^n)$ in $\mathrm{Isom}(\mathbb{R}^n)$.

(b) There is an orientation homomorphism $\mathrm{Isom}(\mathbb{R}^n) \to \{\pm 1\}$, $\phi \mapsto \det(A)$, with kernel $\mathrm{Isom}_+(\mathbb{R}^n)$.

Theorem Y. Every isometry ϕ of $\mathbb{R}^n$ has the form

$$\phi(x) = Ax + b,$$

where $A \in \mathbb{R}^{nxn}$ is an orthogonal matrix and $b \in \mathbb{R}^n$.

An *affine subspace* of $\mathbb{R}^n$ is a set of the form

$$L = V + b$$

where V is a linear subspace of $\mathbb{R}^n$ and $b \in \mathbb{R}^n$. If V has dimension k we call L a *k-plane.* A set of k points in Euclidean space is called *affine independent* if they are not contained in a common $(k-2)$-plane.

Theorem Z. Two isometries of $\mathbb{R}^n$ that agree at $n+1$ affine independent points agree everywhere.

Theorem X. The fixed point set of an isometry of $\mathbb{R}^n$ is a k-plane for some $k \in \{0, \ldots, n\}$, or it is empty.

Theorem B. Every isometry of $\mathbb{R}^n$ of order 2 is a reflection through a k-plane, for some $k \in \{0, \ldots, n-1\}$.

Theorem C. Every isometry of $\mathbb{R}^3$ of finite order is either

(Rotation) Rotation by an angle $2\pi/m$ about an axis A, or

(Rotary Reflection) Rotation by an angle $2\pi/m$ about an axis A, followed by reflection in a plane E normal to A.

Theorem D. A finite group of isometries of $\mathbb{R}^n$ has a fixed point. (This is proven in another handout.)