1.2 Subgroups

Last updated: 2020–08–30

A substructure is one of the most basic ideas in algebra. Applying the philosophy of reductionism, one understands algebraic objects by describing their substructures.

1.2.1 Definition. Let G be a group. A subset H of G is a ***subgroup*** if the restriction of the operation on G is a group operation on H.

For any group G, the set G itself is a subgroup of G and the subset $\{e\}$ consisting of the only the identity element is a subgroup of G.

1.2.2 Lemma. *A nonempty subset H of a group G is a subgroup if and only if, for all $g, h \in H$, we have $g\,h^{-1} \in H$.*

Proof.
($\Rightarrow$) Since H is a group, each element in H has an inverse and the product of two elements is an element in H.
($\Leftarrow$) Since associativity is inherited from the group G, the binary operation on G induces a group structure on H if and only if the following three conditions are satisfied.
(closure) For all $g, h \in H$, the product $g\,h$ belongs to H.
(identity) The identity element $e \in G$ belongs to H.
(inverse) For all $h \in H$, the inverse h^{-1} belongs to H.
Since H is nonempty, there exists $h \in H$, so $e = h\,h^{-1} \in H$. For all $h \in H$, we have $h^{-1} = e\,h^{-1} \in H$. Finally, if $g, h \in H$, then we have $g\,h = g\,(h^{-1})^{-1} \in H$. □

1.2.3 Example. Each inclusion in the chains $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ and $\mu_n \subset S^1 \subset \mathbb{C}^\times$ defines a subgroup. Although the nonzero rational numbers $\mathbb{Q}^\times$ form a group under multiplication, this subset is not a subgroup of the rational numbers. ✧

1.2.4 Example. The ***special linear group***

$$\mathrm{SL}(n, \mathbb{R}) := \{\text{real } (n \times n)\text{-matrices } \mathbf{A} \text{ such that } \det(\mathbf{A}) = 1\}$$

is a subgroup of $\mathrm{GL}(n, \mathbb{R})$ because the determinant of a product is the product of determinants. ✧

1.2.5 Proposition. *Let X be a subset of a group G. The set of elements in G that commute with all of the elements in X forms a subgroup of G. This subgroup is called the* **centralizer** *of X in G and is denoted by $C_G(X)$.*

Proof. An element $g \in G$ lies in the centralizer $C_G(X)$ if and only if, for all $x \in X$, we have $g\,x = x\,g \Leftrightarrow x = g^{-1}\,x\,g \Leftrightarrow x = g\,x\,g^{-1}$. Given two elements $f, g \in C_G(X)$, we see that

$$(f\,g^{-1})^{-1}\,x\,(f\,g^{-1}) = g\,f^{-1}\,x\,f\,g^{-1} = g\,x\,g^{-1} = x$$

for all $x \in S$. Thus, Lemma 1.2.2 shows that $C_G(X)$ is a subgroup. □

1.2.6 Definition. The ***center*** of a group G is the centralizer of the group itself; $Z(G) := C_G(G) = \{g \in G : f\,g = g\,f \text{ for all } f \in G\}$.

A group G is abelian if and only if it is equal to it center; $Z(G) = G$.

1.2.7 Lemma. *For any family $\{H_j \mid j \in J\}$ of subgroups of a group G, the intersection $H := \bigcap_{j\in J} H_i$ is also a subgroup of G.*

Proof. Since $e \in H_j$ for all $j \in I$, it follows that $H \neq \varnothing$. Suppose that $f, g \in H$. The definition of the intersection implies that $f, g \in H_j$ for all $j \in J$. Since H_i is a subgroup of G, we deduce that $f\,g^{-1} \in H_j$ for all $j \in J$. Thus, we conclude that $f\,g^{-1} \in H$ and Lemma 1.2.2 shows that H is a subgroup of G. □

The group μ_n of nth roots of unity is cyclic, generated by $\zeta := e^{2\pi \mathrm{i}/n}$. Corollary 1.1.5 establishes that the symmetric group $\mathfrak{S}_n$ is generated by the $\binom{n}{2}$ transpositions.

1.2.8 Definition. For any subset X of a group G, the ***subgroup generated*** by X, denoted by $\langle X\rangle$, is the intersection of all subgroups of G that contain X. The group G is ***finitely generated*** if there exists a finite subset X such that $G = \langle X\rangle$. Similarly, the group G is ***cyclic*** if there exists an element $g \in G$ such that $G = \langle\{g\}\rangle$.

Proposition 1.1.1 proves that $\mathfrak{S}_n$ has order $n!$. The group μ_n has order n and the Klein 4-group has order 4.

1.2.9 Definition. The ***order*** $|G|$ of a group G is the cardinality of its underlying set.

1.2.10 Lemma. *Let G be a group. Fix an element $g \in G$ and set $H := \langle g\rangle$.*

(i) *The cyclic subgroup H has infinite order if and only if, for all positive integers n, we have $g^n \neq e$.*

(ii) *When the subgroup H has finite order, the order $|H|$ is the smallest positive integer m such that $g^m = e$.*

(iii) *There exists a positive integer k such that $g^k = e$ if and only if the order $|H|$ divides k.*

Proof.

(i) (⇒) If there were positive integers r and s such that $r < s$ and $g^r = g^s$, then we would have $g^{s-r} = e$ which contradicts our hypothesis. We conclude that $|\{g^n \mid n \in \mathbb{N}\}| = |\mathbb{N}|$ so the cyclic subgroup H has infinite order.

(⇐) Suppose there is a positive integer n such that $g^n = e$. For any integer s, there are integers q and r such that $s = qn+r$ and $0 \leqslant r < n$. It follows that $g^s = g^{qn+r} = (g^n)^q\,g^r = g^r$. We deduce that $H \subseteq \{e, g, g^2, \dots, g^{n-1}\}$, so the group H has finite order.

(ii) Let m be the minimum positive integer such that $a^m = e$. If we were to have $g^r = g^s$ for some $0 \leqslant r < s \leqslant m-1$, then we would obtain $g^{s-r} = e$ contradicting our choice of m. Hence, we must have $H = \{e, g, \dots, g^{m-1}\}$.

(iii) Suppose that $g^k = e$ and set $m := |H|$. There exists integers q and r such that $k = qm + r$ with $0 \leqslant r < m$. Since we have $e = g^k = g^{qn+r} = (g^n)^q\,g^r = g^r$, part (ii) implies that $r = 0$. □

1.2.11 Remark. The ***order*** of an element $g \in G$, which by definition is the cardinality of the subgroup it generates, equals the smallest positive integer m such that $g^m = e$.

1.3 Automorphism Groups

Last updated: 2020–08–31

Why would any sensible person introduce the abstract concept of a group? In practice, groups arise as the symmetries of some object.

1.3.1 Definition. A ***morphism*** is a structure-preserving map from one object to another having the same mathematical structure. We write $\varphi : X \to Y$ for a morphism φ with source X and target Y. The composition of two morphisms φ and ψ is defined precisely when the target of φ is the source of φ. Composition satisfies two axioms:

(associativity) For any three morphisms $\omega : W \to X$, $\varphi : X \to Y$, and $\psi : Y \to Z$, we have $\psi \circ (\varphi \circ \omega) = (\psi \circ \varphi) \circ \omega$.

(identity) For every object X, there exists a morphism $\mathrm{id}_X : X \to X$, called the ***identity morphism*** on X such that, for any morphism $\varphi : X \to Y$, we have $\mathrm{id}_Y \circ \varphi = \varphi = \varphi \circ \mathrm{id}_X$.

1.3.2 Example. A morphism between sets is an arbitrary map, between vector spaces is a linear map, between topological spaces is a continuous function, and between differentiable manifolds is differentiable function. ✧

1.3.3 Definition. A morphism $\varphi : X \to Y$ is an ***isomorphism*** if there exists a morphism $\psi : Y \to X$ such that $\psi \circ \varphi = \mathrm{id}_X$ and $\varphi \circ \psi = \mathrm{id}_Y$. An ***automorphism*** is an isomorphism whose source and target are identical.

1.3.4 Example. An isomorphism between sets is a bijective map, between vector spaces is an invertible linear map, between topological spaces is a homeomorphism, and between differential manifolds is a diffeomorphism. ✧

As follows immediately from the definitions, the automorphisms of a given mathematical object form a group.

1.3.5 Definition. The ***automorphism group*** of a mathematical object X is the group consisting of all automorphisms of X.

1.3.6 Example. The automorphism group of a set X is precisely the symmetric group $\mathfrak{S}_X$. ✧

1.3.7 Example. For any positive integer n, the ***dihedral group*** D_n is the automorphism group of a regular polygon with n edges. The group D_n has order $2n$ because a regular polygon with n edges has $2n$ different automorphisms, namely n rotational symmetries and n reflection symmetries. ✧

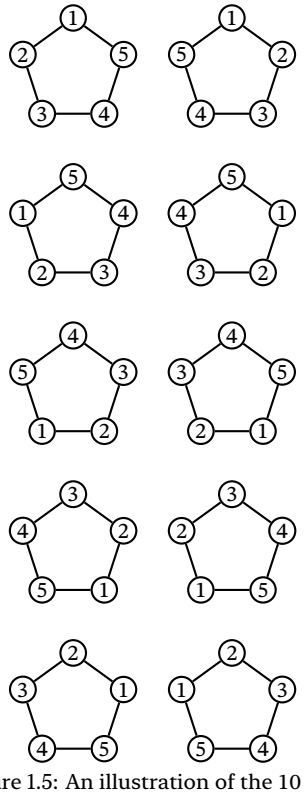

Figure 1.5: An illustration of the 10 elements in the dihedral group D_5

1.3.8 Example. The ***orthogonal group***, which is defined to be

$$\mathrm{O}(n, \mathbb{R}) := \{A \in \mathrm{GL}(n, \mathbb{R}) \mid \mathbf{A}^{\mathsf{T}} \mathbf{A} = \mathbf{I}\},$$

The dihedral group D_n is a finite subgroup of $\mathrm{O}(2,\mathbb{R})$.

consists of the distance-preserving linear maps on the Euclidean space $\mathbb{R}^n$ because $\|\mathbf{A}\mathbf{v}\|^2 = (\mathbf{A}\mathbf{v})^{\mathsf{T}}(\mathbf{A}\mathbf{v}) = \mathbf{v}^{\mathsf{T}}\mathbf{A}^{\mathsf{T}}\mathbf{A}\mathbf{v} = \mathbf{v}^{\mathsf{T}}\mathbf{v} = \|\mathbf{v}\|^2$. Thus, the orthogonal group $\mathrm{O}(n,\mathbb{R})$ is the automorphism group of the normed vector space $\mathbb{R}^n$. ✧

To justify the group axioms, we demonstrate that every group is the automorphism group of some mathematical object. To reduce the mathematical prerequisites, we use directed graphs.

1.3.9 Definition. An automorphism of an edge-coloured directed graph is a permutation σ of its vertex set such that an ordered pair of vertices (u,v) forms an arrow from u to v that is assigned the coloured c if and only if the ordered pair $\big(\sigma(u),\sigma(v)\big)$ forms an arrow from $\sigma(u)$ to $\sigma(v)$ that is assigned the coloured c.

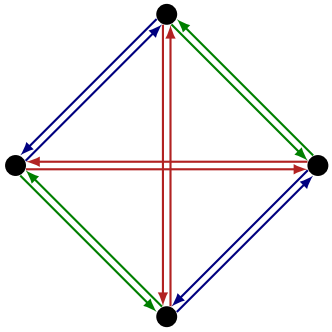

Figure 1.6: The Cayley diagram of the Klein group

1.3.10 Theorem. *Every group is the automorphism group of some edge-coloured directed graph.*

Proof. Let G be a group. The ***Cayley diagram*** Γ of this group is the edge-coloured directed graph constructed as follows:

- The vertex set $V(\Gamma)$ is identified with the underlying set of the group G.
- Each arrow is assigned a colour from the set $G \setminus \{e\}$.
- For all $v \in V(\Gamma)$ and all $c \in G \setminus \{e\}$, the ordered pair (v, vc) forms an arrow from v to vc that is assigned the coloured c.

By design, the colour of an arrow (v, vc) in Γ can be reconstructed from the appropriate product its tail and head: $v^{-1}(vc) = c$. We claim that the group G is the automorphism group $\mathrm{Aut}(\Gamma)$.

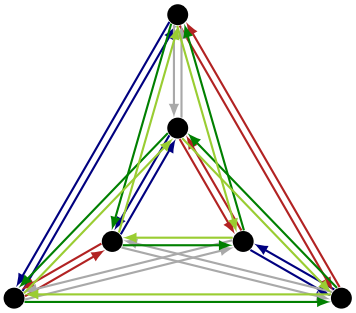

Figure 1.7: The Cayley diagram of $\mathfrak{S}_3$

We first show that each element in the group G determines an automorphism of the Cayley diagram Γ. For any $g \in G$, consider the map $\lambda_g : V(\Gamma) \to V(\Gamma)$ defined by $\lambda_g(v) := gv$. The associativity property of the group G establishes that, for all $g, h \in G$, we have $\lambda_g \circ \lambda_h = \lambda_{gh}$. Since $\lambda_g \circ \lambda_{g^{-1}} = \lambda_e = \mathrm{id}_{V(\Gamma)}$ and $\lambda_{g^{-1}} \circ \lambda_g = \lambda_e = \mathrm{id}_{V(\Gamma)}$, the map λ_g is a permutation of the set $V(\Gamma)$. Since each element in G has an inverse, it follows that the ordered pair (v, vc) is an arrow in Γ coloured c if and only if the ordered pair $\lambda_g(v, vc) = (gv, gvc)$ is an arrow in Γ coloured c.

For the other direction, suppose that σ is an automorphism of Cayley diagram Γ. For all $c \in G \setminus \{e\}$, the ordered pair (e, c) is an arrow in Γ coloured c if and only if the ordered pair $\big(\sigma(e), \sigma(c)\big)$ is an arrow in Γ coloured c. Hence, we deduce that $\big(\sigma(e)\big)^{-1}\sigma(c) = c$ or $\sigma(c) = \sigma(e)\,c$, so we conclude that $\sigma = \lambda_{\sigma(e)}$. □

In geometric group theory, one identifies the colour classes of c and c^{-1} to convert the directed graph into a graph. This graph is endowed with the structure of a metric space.

1.3.11 Remark. There are many other universality results proving that all groups arise as the automorphism groups of some specific mathematical structure (including graphs, strongly regular graphs, lattices, and fields).