

Topics: Main points

Section 0: Sets, functions and nomenclature.

$f : A \mapsto B$. A_i and B_i are subsets of A and B , respectively. f^{-1} may or may not exist as a function, but $f^{-1}(B_i)$ is always defined.

$f(\cup_i A_i) = \cup_i f(A_i)$, **but** $f(\cap_i A_i) \neq \cap_i f(A_i)$ in general.

$f^{-1}(\cup_i B_i) = \cup_i f^{-1}(B_i)$ **and** $f^{-1}(\cap_i B_i) = \cap_i f^{-1}(B_i)$.

Domain, range, co-domain. Functions may be “injective” (1:1), “surjective” (onto), or both (bijective).

Equivalence relation on a set S . $\sim : S \times S \mapsto \{0, 1\}$. That is, “true” (1) or “false” (0).

Definition: Must be Reflexive, Symmetric and Transitive.

Section 1: Examples. Not covered formally.

Section 2: Binary operations and structures.

(S, \star) , where S is a set and $\star : S \times S \mapsto S$. Written as $s_1 \star s_2$, for $s_1, s_2 \in S$. \star is a binary operation.

Concepts: Associative, commutative, identity.

Identity, e , is unique, if it exists.

Section 3: Functions and binary structures.

Two binary structures. (S, \star) and (S', \star') .

$\varphi : S \mapsto S'$.

HOMOMORPHISM $\varphi(s_1 \star s_2) = \varphi(s_1) \star' \varphi(s_2)$ for all $s_1, s_2 \in S$.

ISOMORPHISM φ is a homomorphism **and** a bijection.

Note: If two binary structures are isomorphic, φ is not, in general, unique. It is often **difficult** to show that two binary structures are **not** isomorphic.

If e is an identity for (S, \star) and φ is a homomorphism, then $\varphi(e)$ is an identity for (S', \star') .

Section 4: Groups. (G, \star) .

G is a non-empty set. \star is a binary relation. A group is often as G ; the binary relation being “understood”.

How does a group differ from a binary structure? Answer: It satisfies extra conditions.

1. \star is associative.
2. G has an identity, e .
3. For any $g \in G$, there is some $g' \in G$ such that $g \star g' = g' \star g = e$.

The inverse of $g \in G$ is unique and is written as g^{-1} . (When the group operation is denoted by $+$, the inverse of g is denoted by $-g$.)

An Abelian group is a group where \star is also commutative.

Note: Not covered: Left & right inverses, semi-groups and monoids.

Group table for a finite group. $|G| = n$.

\star	e	g_1	g_2	\dots	g_j	\dots	g_n
e	e	g_1	g_2	\dots	g_j	\dots	g_n
g_1	g_1	$g_1 \star g_1$	$g_1 \star g_2$	\dots	$g_1 \star g_j$	\dots	$g_1 \star g_n$
g_2	g_2	$g_2 \star g_1$	$g_2 \star g_2$	\dots	$g_2 \star g_j$	\dots	$g_2 \star g_n$
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots
g_i	g_i	$g_i \star g_1$	$g_i \star g_2$	\dots	$g_i \star g_j$	\dots	$g_i \star g_n$
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots
g_n	g_n	$g_n \star g_1$	$g_n \star g_2$	\dots	$g_n \star g_j$	\dots	$g_n \star g_n$

Each row of the group table contains a permutation of the elements of G and each column of the group table contains a permutation of the elements of G .

Section 5: Subgroup.

(G, \star) is a group. (H, \star) is a subgroup of G , written as $H \preceq G$. There are two requirements.

1. $H \subseteq G$, $H \neq \emptyset$.
2. H is **closed** under \star . That is, if $h_1, h_2 \in H$, then $h_1 \star h_2 \in H$.

Note: The notation $H \prec G$ means that $H \subset G$ ($H \neq G$). Note that $\{e\}$ is always a subgroup of a group. It is the “trivial” subgroup.

Cyclic subgroup: $a \in G$, $H = \{a^n \mid n \in \mathbb{Z}\}$, where $a^0 = e$ and $a^{-n} = (a^n)^{-1}$.

Section 6: Cyclic Groups.

(G, \star) is a cyclic group if $G = \{a^n \mid n \in \mathbb{Z}\}$ for some $a \in G$. The notation $\langle a \rangle$ is used to denote $\{a^n \mid n \in \mathbb{Z}\}$. Note that if \mathfrak{G} is any group, and $g \in \mathfrak{G}$, then $\langle g \rangle$ is a subgroup of \mathfrak{G} .

Cyclic groups are Abelian.

Note: A full discussion of the “division algorithm” is useful here.

A subgroup of a cyclic group is cyclic.

Structure of Cyclic Groups. Full Classification.

Section 7: Generating Sets & Cayley Digraphs.

Preamble: The intersection of any collection of subgroups is a subgroup.

If $A = \{a_i \mid i \in I\}$ (e.g., $I = \mathbb{Z}$, or $I = \{1, 2, \dots, n\}$.) is a subset of a group, G , then the intersection of all subgroups that contain A is called the subgroup generated by A , $\langle A \rangle$.

Examples.

1. $A = \{a\}$.
2. $A = \{a_1, a_2, \dots, a_n\}$ and G is Abelian. Then

$$\langle A \rangle = \{a_1^{k_1} a_2^{k_2} a_3^{k_3} \dots a_n^{k_n} \mid k_1, k_2, \dots, k_n \in \mathbb{Z}\}.$$

3. G is not Abelian. $A = \{a, b\}$.

$$\langle A \rangle = \{a^{k_1} b^{h_1} a^{k_2} b^{h_2} \dots a^{k_m} b^{h_m} \mid k_i \in \mathbb{Z} \text{ for } i = 1, 2, \dots, m\}.$$

Example: The dihedral group of the regular n -gon, $n \geq 3$.

Cayley Digraphs: Not covered.

Section 8: Permutation groups.

Standard nomenclature. Bijections on a set, S , form a group under function composition. If $|S| < \infty$, this group is called the permutation

group on S . If $|S| = n$, it is called the permutation group on n objects. It can be denoted by (Π_n, \circ) , where \circ is function composition. Lower case Greek letters are often used to denote specific permutations. ($\sigma\pi$ is $\sigma \circ \pi$, and so on.)

$$\begin{aligned}\pi &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 3 & 5 & 2 & 1 & 6 \end{pmatrix} \\ \sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 4 & 2 & 7 & 6 & 3 & 5 \end{pmatrix} \\ \sigma\pi &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 2 & 6 & 4 & 1 & 3 \end{pmatrix} \\ \pi\sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 7 & 6 & 1 & 3 & 2 \end{pmatrix}.\end{aligned}$$

The dihedral group of the regular n -gon.

Cayley's Theorem: Any group, G , is isomorphic to a permutation group.

The proof is simple, since each row of a group table gives a different permutation of the elements of G . (Same for columns.)

Section 9: Orbits, Cycles & Alternating groups.

ORBITS Any permutation, σ , on S breaks S into equivalence classes, where $a, b \in S$ are equivalent if $b = \sigma^n(a)$ for some $n \in \mathbb{Z}$. The equivalent classes are called "orbits".

CYCLES Assume $S = S_n$ (permutations on n objects)

Each orbit of a permutation, σ , defines a new permutation on S_n . Within an orbit, the permutation is given by σ . All other elements of S_n remain fixed.

Cycle decomposition. Disjoint cycles. Length of a cycle is cardinality of the orbit.

A cycle of length 2 is called a "transposition" ("swap").

ALTERNATING GROUP Any permutation is a product of transpositions.

If π is a permutation, then $T_\pi = \sum_{1 \leq i < j \leq n} \delta(\pi(i) > \pi(j))$, is the "number of inversions" induced by π . $\delta()$ is 1 if the expression is true and otherwise is 0.

A permutation is even or odd if T_π is even or odd, respectively.

Theorem: If τ is a transposition, $\tau\pi$ is odd if π is even, and even if π is odd.

A_n is the subgroup of even permutations on n objects.

Section 10: Cosets and Lagrange's Theorem

$H \triangleleft G$. H defines an equivalence relation on G by $a \sim_H b$ if $ab^{-1} \in H$. If the number of equivalence classes is finite, G may be partitioned into LEFT cosets: $H, g_1H, g_2H, \dots, g_{m-1}H$, or right cosets: $H, Kg'_1, Hg'_2, \dots, Hg'_{m-1}$.

Lagrange's Theorem: $|G| = m|H|$. m is the "index", $(G : H)$ of H in G .

(From section 13: H is called "normal" if $aH = Ha$ for all $a \in G$.)

Section 11: Direct products and Classification of Finitely generated Abelian groups.

Direct product of groups.

Set is Cartesian product. $G_{i=1}^n$. $G = \prod_{i=1}^n G_i$.

Group operation is defined for each co-ordinate. $(a_1, a_2, \dots, a_n) \star (b_1, b_2, \dots, b_n) = (a_1 \star_1 b_1, a_2 \star_2 b_2, \dots, a_n \star_n b_n)$.

Finitely generated Abelian groups are isomorphic to direct products of \mathbb{Z} or \mathbb{Z}_k ($k > 1$). There are two unique ways to do this.

Section 12: Plane Isometries.

Not covered.

Section 13: Group homomorphisms.

$\phi : (G, \star) \mapsto (G', \star')$.

ϕ is a homomorphism on the underlying binary structure.

What more? Nothing more need be assumed. $e' = \phi(e) = \phi(a \star a^{-1}) = \phi(a) \star' \phi(a^{-1})$, so $\phi(a)^{-1} = \phi(a^{-1})$.

For any $H \leq G$, $\phi(H)$ is a subgroup of G' . (Author writes $\phi[H]$ etc.)

For any $K \leq G'$, $\phi^{-1}(K)$ is a subgroup of G .

Special subgroup relating to φ . $\text{Ker}(\varphi) = \varphi^{-1}(\{e'\})$. $\text{Ker}(\varphi)$ is a normal subgroup of G .

Restate condition for isomorphism. φ is an isomorphism if it is a homomorphism **and** if it is a bijection. The injective requirement is equivalent to $\text{Ker}(\varphi) = \{e\}$. Note that if $|G| < \infty$, φ is surjective if and only if it is injective.

Section 14: Factor Groups

$H \preceq G$. We know that H induces an equivalence relation and partitions G into equivalence classes.

If H is normal, then a group operation can be defined on equivalence classes by $(aH) \star (bH) = (a \star b)H$ (or $(aH)(bH) = (ab)H$). This group is denoted by G/H ($G \bmod H$, or modulo). It is called a factor group or a quotient group.

The function taking a into aH is a group homomorphism.

If $\varphi : G \mapsto G'$ is a homomorphism, then $H = \text{Ker}(\varphi)$ is a normal subgroup. The map that takes aH to $\varphi(a)$ is an isomorphism between G/H and $\varphi(G)$.

Included topics: Section 15, and sections 18 to 23. Would like to cover 24, 26 and 27. Section 29 would be great.