Representation, Group, Permutation

OFFENBARKEIT

April 1, 2024

Preface

Fearless Symmetry is an expository book for non-specialists, aimed at an understanding of mod(p) linear representations of Galois groups. The following are notes, of a very non-special student, derived from study of Fearless.

1 Representations

This introduction to a bare notion of representation lays out the concept using the counting toy model. The represention concept will become richer and more powerful when we begin the later discussion of Galois Groups.

1.1 Motivation

The definition of representation depends on the usual definitions for set, function, 1-1 correspondence, and morphism. A **morphism** is an abstract correspondence between sets that preserves structure. A **representation** is a morphism between an abstract object about whose structure we want to learn, and a model object whose structure is well-understood.

1.2 Counting Toy Model

Counting is a 1-1 function (bijection) between an abstract object to be counted, set S with n elements, and the model object $\mathbb{N}_n$, the set of natural numbers with the same number of elements (cardinality) $\{1, 2, 3, \ldots, n\}$, where one uses $\{\}$ to enclose the elements in a set.

The preserved structure under the 1-1 counting morphism is the cardinality of the represented set.

In the notation of representations, $A \to B$ states that model object B with well-known structure represents abstract object A via a morphism (arrow). Thus, a representation has three components, two objects and a morphism. Facts regarding the abstract structure can now be inferd from the model structure. These structural facts are considered to be the common form of the objects.

One may indicate by $S \to \mathbb{N}_n$ that the natural numbers $1, 2, \ldots, n$ represent (count) a set with n elements, S.

1.3 Aside: Morphisms in Specific Contexts

Morphism is a term suited to this abstracted discussion in Fearless. But more specific object-related terminology is generally used, as in the following concrete realizations of morphism.

If the object is a set, a morphism is simply a **function** that preserves structure, e.g. a function on an ordered set that preserves order.

If the object is a group or vector space, morphisms are called **homomorphisms or transformations**. For example, a linear transformation on a vector space preserves vector addition and scalar multiplication.

The homomorphisms on Euclidean space, preserving both distance and a given point, form the group of orthogonal transformations of space.

A homomorphism that establishes a 1-1 correspondence between all the elements in the source and target sets (that maps the source onto the target) is called an **isomorphism**.

Only within discussions of the abstract object called a **category** is the naked term morphism likely to be encountered.

2 Groups

Sets with group structure are the most common mathematical objects for formalizing the concept of symmetry. In the remainder, the objects under discussion most often will be groups.

2.1 Motivation

When S and T are sets, one writes a direct product $S \times T$ to mean the larger set formed from all possible pairs of elements, taking one from S and one from T. A binary operator $\odot$ is associative if $x \odot (y \odot z) = (x \odot y) \odot z$. All morphisms are associative.

A set S forms a group under the following conditions:

- an associative binary composition operator $\odot : S \times S \to S$
- an identity element e_S, where $s \odot \mathrm{e}_S = \mathrm{e}_S \odot s = s$ for each element s in S
- inverse elements s^{-1} for each element s, where $s \odot s^{-1} = s^{-1} \odot s = \mathrm{e}_S$
- commutative group operator (optional), if $s \odot s' = s' \odot s$ for all elements s, s'

2.2 Group Examples

- $SO(3)$, the Lie (continuous) group of rotations of a sphere, is a non-commutative group. One means by the group operation on two rotations, $r_1 \odot r_2$, that r_2 is done first, then r_1. These morphisms initiate continuous (arbitrarily small) transformations, which can be summed (integrated).
- $\mathbb{Z}$, the integers under addition, is a discrete commutative group.

2.3 Further Group Notions

A typical notation for the composition operator is: $\odot$ for non-commutative groups; $+$ for commutative (Abelian) groups. Often one just writes ab, rather than $a \odot b$, which can be referred to generically as 'multiplication'. One says the group is closed under the group operator because it maps pairs of elements of S back into S.

The order of a finite group $G, |G|$, is the cardinality of the set G. For every element g in finite group G, there is some power of g, say c, that is the least positive integer such that $g^c = \mathrm{e}_G$. Each element g thus defines a cycle, and c is the order (or period) of element $g, o(g)$.

A cyclic group consists of the identity and one cyclic element: $G = \{\mathrm{e}_G, g, g^2, g^3, \ldots, g^{c-1}\}$. One says G is generated by g, and $|G| = o(g)$. A cyclic group is Abelian. For every finite group G

containing element g, $o(g)$ is a factor of $|G|$. A group G with prime $|G|$ is necessarily cyclic, and has no proper subgroups.

Group structures may be identified by their element cycles as follows, where e is the identity, $a, b, ,$, are abstract elements, and C^n is a cyclic group of order n. The direct products of cyclic groups below is a shorthand notation. For example, the Klein vierergruppe (four group or quadratic group), written $C^2 \times C^2$, is a way of writing the 4-element group $\{\mathrm{e}, a, b, ab = ba\}$ obtained by $\{\mathrm{e}, a\} \times \{\mathrm{e}, b\}$. Similarly, the other direct product representations above can be expanded.

2.4 Aside: Canonical Group Forms Up To Order 8

Abelian (11):

e C^2 C^3 C^4 C^5 C^6 C^7 C^8
$\{C^2 \times C^2\}$ $\{C^4 \times C^2\}$ $\{C^2 \times C^2 \times C^2\}$

Non-Abelian (3):

dihedral order 6: D_6 (aka S_3) : $a^3 = b^2 = (ab)^2 = \mathrm{e}$
dihedral order 8: $D_8 : a^4 = b^2 = (ab)^2 = \mathrm{e}$
dicyclic quaternion order 8; $Q : a^4 = \mathrm{e}, a^2 = (ab)^2 = b^2$

2.5 Subgroups and Cosets

If H is a subset of group G, H is called a subgroup of G if H is closed under the group operator of G. A subgroup contains the parent group identity element and all of its own inverse elements. G itself, and the group consisting only of e_G, are the improper subgroups of G. All other subgroups are called proper.

Let G be a group and H a subgroup, and a an element in G. The left coset of H in G determined by a is defined as aH, and the right coset of H in G determined by a is Ha, where a is called the representative of each coset. G/H, the coset space of H in G, is the set of left cosets (or right cosets) of H. All the cosets of H have the same cardinality as H. The index of H in G, $[G : H]$ is the number of left cosets (or right cosets) of H, the cardinality of G/H. Lagrange proved for finite G that $[G : H] = |G|/|H|$, and$|H| \mid |G|$ ($|$ means divides).

A subgroup N of G is said to be normal (invariant), written $N \lhd G$, if $aNa^{-1} = N$ for all a in G. If G is Abelian, every subgroup is normal. Given N a normal subgroup, the coset space G/N is a subgroup called the quotient group of G by N. The identity of G/N is N. For example, if $G = Z$ and $H = 2Z$, the cosets of H are the even and odd integers. The quotient group $Z/2Z$, read the integers mod the even integers, is a group with two elements, isomorphic to $\{0, 1\}$ using addition (mod 2) [see Chapt. 4, Modular Arithmetic].

2.6 Group Homomorphisms

Given groups G and H, a group homomorphism, $f : G \to H$ is structure-preserving, meaning $f(ab) = f(a)f(b)$. Define the kernel of f:

$Ker(f) = \{a \in G : f(a) = \mathrm{e}_H\}$

and the image of f:

$Im(f) = \{h \in H : h = f(a), a \in G\}$

where : means such that and $\in$ means contained in. Then $Ker(f)$ is a subgroup of G, $Im(f)$ is a subgroup of H, $Ker(f) \lhd G$, every normal subgroup of G is the kernel of some group homomorphism on G, and $G/Ker(f) \cong Im(f)$ ($\cong$ means is isomorphic to).

3 Permutations

This chapter defines properties of permutations, and the representation of abstract groups by their corresponding permutation groups.

3.1 Motivation

A goal of ANT is to formalize information regarding solutions to polynomial equations with integer coefficients. Galois permutation groups permute the roots of polynomials, a useful tool.

3.2 Symmetric Group of Degree n

Given a finite abstract group G (or any finite set) with n elements, the group of $n!$ permutations of the elements of G (bijections : $G \to G$) forms a group called the symmetric group of degree n (called S_G or Σ_G). In particular, when $G = \mathbb{N}_n$, the symmetric

group is written S_n. Because permutations are bijections, they have inverses that undo the corresponding permutation.

A permutation has one or more cycles, where each cycle's elements map in sequence until an element repeats. One expresses a permutation's cycle decomposition by grouping in parentheses the elements in each cycle. E.g., given set $\{a, b, c, d\}$, the permutation

$p : \{a, b, c, d\} \rightarrow \{b, c, d, a\}$

has a single cycle $(abcd)$ where p takes a to b, b to c, c to d, d back to a. Similarly,

$p : \{a, b, c, d\} \rightarrow \{b, a, d, c\}$

has two cycles $(ab)(cd)$, called transpositions, where p takes a to b, b back to a, c to d, d back to c.

$p : \{a, b, c, d\} \rightarrow \{a, c, b, d\}$

has three cycles $(a)(bc)(d)$.

$p : \{a, b, c, d\} \rightarrow \{a, b, c, d\}$

has four cycles $(a)(b)(c)(d)$, the identity permutation. The lengths of the cycles of a permutation reveal useful information about the permutation.

3.3 Notions of Permutations, Symmetry Groups

Disjoint permutation cycles commute. Every element of S_n (permutation) can be written uniquely as the product of disjoint cycles of length greater than 1, and can be written as a product of transpositions (not uniquely, the transpositions are not disjoint). A permutation is even or odd depending on whether it can be written as a product of an even or odd number of transpositions.

One can consider each element of G as a permutation function acting through the group operator. Let g_i be all the elements of G and p be one of these elements also. Then $g_i \rightarrow pg_i$ is a permutation of all elements of G via multiplication by p. The set of permutations so defined form a group isomorphic to G, say G' called the regular representation of G. If G is non-Abelian, one would distinguish right and left regular representations. Cayley showed that any group G is isomorphic to a subgroup of Σ_G. In particular, the regular representation G' is a subgroup of Σ_G. In our representation notation, $G \rightarrow G'$.

The set of even permutations is a normal subgroup of S_n, called the alternating group A_n, where $|A_n| = n!/2$. For $n > 2$, A_n is gen-

erated by the 3-cycles in S_n.

Σ_G, A_n, and the regular representation of G are large and not of much mathematical interest. A smaller permutation representation of G is obtained by considering $\Sigma_{G/H}$ for subgroup H of group G. $\Phi_H : G \to \Sigma_{G/H}$ is a group homomorphism and $Ker(\Phi_H)$ is the largest normal subgroup of G contained in H.

3.4 Triangle Symmetry Groups

Consider symmetries of triangles of varying regularity together with their symmetry groups. Each type of triangle symmetry has a corresponding representation group $T_{triangle}$ consisting of motions in the plane (transformations) that map the triangle onto itself (that preserve the form of the triangle). $T_{non-isoceles}$ consists only of the identity transformation. $T_{isoceles}$ consists of the identity and a reflection about the axis of symmetry. $T_{equilateral}$ consists of identity, two rotations about the center, and three reflections. Thus, the respective symmetry groups have 1, 2, and 6 elements, in order of increasing object symmetry. The group $T_{equilateral}$ is the dihedral group of order 6 above, D_6, and is a special case of a regular n-sided polygon whose transformation group is the dihedral group of order $2n$. $T_{equilateral}$ is isomorphic to S_3, the symmetry group with $|S3| = 3!$, representing abstract groups of order 3. Such transformation groups of regular polygons are subgroups of $\Sigma_{\mathbb{R}^2}$, where $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$, the Cartesian plane.