1 Groups and subgroups

In this section elements of the group G are denoted $a, b, c, \ldots$. The group multiplication is $a * b$. The identity element is e. The inverse is a^{-1}, so we have $a * a^{-1} = e$ and $a^{-1} * a = e$.

Consider a group G and subgroup H. Two elements a, b of G are equivalent if $a^{-1} * b$ is in H. The equivalence classes are called left cosets of H. The left coset determined by a (or by b) consists of $a * H$ (or $b * H$). These left cosets are the blocks of a partition of G.

The Lagrange theorem follows from the remark that all left cosets have the same number of elements, which is just the order of H. The bijection from H to $a * H$ is obtained by sending h to $a * h$.

It follows that the order of H times the number of left cosets equals the order of G.

2 Groups actions

Consider a group acting on a set X. The action of a in G on x in X is another element $a(x)$ in X. Then

- $(a * b)(x) = a(b(x))$
- $e(x) = x$.

Given an element x in X, its orbit $\mathrm{orb}(x)$ is defined by

$$\mathrm{orb}(x) = \{a(x) \mid a \in G\}. \tag{1}$$

If we say that y is equivalent to x if y is in the orbit of x, then this defines an equivalence relation. The orbits form a partition of X. Write $\mathcal{O}$ for the blocks of this partition. Our goal is to count $\mathcal{O}$.

Fix attention on one x in X. Let $H_x = \mathrm{stab}(x)$ be the stabilizer subgroup of G defined by

$$\mathrm{stab}(x) = \{c \in G \mid c(x) = x\}. \tag{2}$$

Consider the map from G to X defined that sends a to $a(x)$. This defines a partition of G, and the blocks of this partition are just the left cosets of $\mathrm{stab}(x)$. In fact, the left coset consists of all $a * c$ with $c(x) = x$, and for such an element $(a * c)(x) = a(c(x)) = a(x)$.

This argument shows that the cosets of the subgroup $\mathrm{stab}(x)$ of G are in bijective correspondence with $\mathrm{orb}(x)$. It follows that the order of $\mathrm{stab}(x)$ times the number of points in $\mathrm{orb}(x)$ is the order of G. We may write this as

$$\frac{|G|}{|\mathrm{stab}(x)|} = |\mathrm{orb}(x)|. \tag{3}$$

3 Counting orbits

Define the fixed point set of a group element a in G to be

$$\mathrm{fix}(a) = \{x \mid a(x) = x\}. \tag{4}$$

The CFB theorem states that the number of orbits is the average over the group of the number of fixed points:

$$|\mathcal{O}| = \frac{1}{|G|} \sum_{a \in G} |\mathrm{fix}(a)|. \tag{5}$$

Here is the proof. We have

$$|\mathcal{O}| = \sum_{x \in X} \frac{1}{\mathrm{orb}(x)}. \tag{6}$$

Then use

$$\frac{1}{\mathrm{orb}(x)} = \frac{1}{|G|} |\mathrm{stab}(x)|. \tag{7}$$

to get

$$|\mathcal{O}| = \frac{1}{|G|} \sum_{x \in X} |\mathrm{stab}(x)| = \frac{1}{|G|} \sum_{x \in X} \sum_{a \in G} 1_{a(x)=x} \tag{8}$$

$$= \frac{1}{|G|} \sum_{a \in G} \sum_{x \in X} 1_{a(x)=x} = \frac{1}{|G|} \sum_{a \in G} |\mathrm{fix}(a)|. \tag{9}$$

4 Counting fixed point sets

In this section elements of the group G are denoted $\pi, \sigma, \tau, \ldots$. The identity element is e. The group acts on a set F.

Consider the case when G is a group of permutations of a set A. Let C be a set of colors. Then $F = C^A$ is the set of all colorings of A. If π is in G and f is in C^A, then the action of π on f is

$$\pi(f)(a) = f(\pi^{-1}(a)). \tag{10}$$

There is a theorem that says that f is in $\mathrm{fix}_G(\pi)$ if and only if f is constant on each cycle of π. Thus if there are $k = |C|$ colors, and $\mathrm{c}(\pi)$ is the number of cycles in π, then

$$|\mathrm{fix}_G(\pi)| = k^{\mathrm{c}(\pi)}. \tag{11}$$

So the CFB theorem implies that

$$|(O)| = \frac{1}{|G|} \sum_{\pi \in G} k^{\mathrm{c}(\pi)}. \tag{12}$$

5 Appendix: Some small groups

The unit basis complex numbers are $1, i$. It is required that $i^2 = -1$. These together with their negatives form a cyclic group C_4 of order 4.

The unit basis quaternions are $1, i, j, k$. It is required that $i^2 = -1$, $j^2 = 1$, and $k^2 = -1$. Furthermore it is required that $ij = -ji = k$, $jk = -kj = i$, and $ki = -ik = j$. These together with their negatives form a group Q of order 8.

The cyclic group C_n is generated by the complex number $z = e^{\frac{2\pi i}{n}}$, representing counterclockwise rotation by $2\pi i/n$. This group is of order n.

The dihedral group D_n is generated by the complex number $z = e^{\frac{2\pi i}{n}}$, representing counterclockwise rotation by $2\pi i/n$, together with reflection r across the x axis. This group is of order $2n$.

The dicyclic group Dc_n is generated by the complex number $z = e^{\frac{2\pi i}{2n}}$ together with the unit quaternion j. This group is of order $4n$. A particularly famous example is when $n = 2$. In this case it is the group generated by i, j, which is Q.

The symmetric group S_n consists of all $n!$ permutations of an n-set. The alternating group A_n consists of all $n!/2$ even permutations of an n-set.

1. $C_1 = S_1 = A_2$
2. $C_2 = S_2 = D_1$
3. $C_3 = A_3$
4. $C_4 = Dc_1$, $C_2 \times C_2 = D_2$ (Klein 4-group)
5. C_5
6. $C_6 = C_2 \times C_3$, NONABELIAN: $D_3 = S_3$ (triangle)
7. C_7
8. C_8, $C_2 \times C_4$, $C_2 \times C_2 \times C_2$, NONABELIAN: D_4 (square), $Q = Dc_2$
9. C_9, $C_3 \times C_3$
10. $C_{10} = C_2 \times C_5$, NONABELIAN: D_5 (pentagon)
11. C_{11}
12. C_{12}, $C_2 \times C_6 = C_2 \times C_2 \times C_3$, NONABELIAN: A_4, $D_6 = D_3 \times C_2$ (hexagon), $T = Dc_3$

The number of abelian groups of order n is computed as follows. Factor n into powers of primes. For each power k that occurs, compute the integer partition number $p(k)$. The answer is the product of these partition numbers. Notice that if the power k is one, then the corresponding partition number $p(1)$ is 1.