Symmetry

More Group Theory

SP Status

Atul Singh Arora July 8-11, 2012

This document contains record of my understanding of Chapter 7 More Group Theory, from Artin.

Areas marked with a **Doubt** or **Find out** are ones I am not absolutely clear about. Perhaps reiterating later would help.

July 8, 2012

Corollary 5.1.28 Let M be the matrix in SO_3 that represents the rotation $\rho_{(u,\alpha)}$ with spin (u, α). Now let B be another element of SO_3, and let $u' = Bu$. The conjugate $M' = BMB^T$ represents the rotation $\rho_{(u',\alpha)}$.

7.4 The Class Equation of the Icosahedral Group

Let $\theta = 2\pi/3$. Rotation by θ about a vertex v, represented by $\rho_{(v,\theta)}$, $\in I$, the icosahedral group (the group of rotational symmetries of a dodecahedron). If v' is another vector, then rotation about this vector, represented by $\rho_{(v',\theta)}$ can be related to the rotation $\rho_{(v,\theta)}$ if in accordance with corollary 5.1.28, we could find a suitable B. But the vertices form different orbits under a given rotation. To transform v to v', both simply need to be in the same orbit for some rotation ρ and this indeed happens, as can be seen geometrically (and can also be derived with mathematical rigour). However, its easier to note that the 20 vertices of a dodecahedron, form a single orbit under the action of I. So always, $\exists$ a $B \in I$ s.t. $v' = Bv$. The interest in this discussion arises form the conjugation relation between rotations. The existence of B makes $\rho(v, \theta)$ and $\rho(v', \theta)$ conjugate elements. So if we take a rotation $\rho(v, \theta)$ and conjugate it with any element $B \in I$, then the result is also a rotation. Similarly if we take a vertex v and operate it with all B, it generates the orbit of order 20. Since the only spins that can represent the same rotation as (v, θ) must be $(-v, -\theta)$ and since $-\theta \neq \theta$, therefore the number of elements in the conjugacy class of $\rho(v, \theta)$ is same as the number of elements in the orbit of v under action of I, viz. 20.

Using the same analysis, we can take $\theta = 2\pi/5$ for faces and conclude with the same reasoning, the number of elements in its conjugacy class to be 12. When $\theta = \pi$ for centre of edges, we can use the same reasoning, but taking caution to account for the fact that rotation by π is the same as rotation by $-\pi (= -\pi + 2\pi = \pi)$. So the number of distinct rotation elements will be half the number of edges, viz. 15.

Find out: Why do we have $\theta = 4\pi/5$ included without which the count goes wrong. And why don't we have other angles, since $4\pi/5$ is a multiple of $2\pi/5$.

The class equation of the icosahedral group then becomes

$$60 = 1 + 20 + 12 + 12 + 15 \tag{1}$$

Simple Groups

Groups that do NOT contain proper normal subgroups, i.e. no normal subgroup other than $< 1 >$ and G. Cyclic groups of prime order don't contain any proper subgroup and are hence simple.

Lemma 7.4.2 Let N be a normal subgroup of a group G.

1. If $x \in N$ then, $C(x) \in N$ (by definition of normal subgroup and conjugacy class)

2. N is a union of conjugacy classes (for each element, there would be a conjugacy class)
3. The order of N is sum of order of the constituent conjugacy classes. (summing the number of elements)

THEOREM 7.4.3 The icosahedral group I is a simple group.

Let's assume there exists a proper normal subgroup of I. It's order must be a proper divisor of 60. Further, as follows from the lemma, the order of the subgroup must equal the sum of some of the terms on the RHS of 1, but necessarily including the term 1 (order of conjugacy class of the identity element). A look at the elements reveals that the sum can't be made divisible. Thus the assumption was wrong, the group must be simple.

July 9, 2012

<I have skipped a big chunk for I didn't have computer access when I studied it>
POST THEOREM 7.5.4 (STATEMENT) A_2 is trivial, A_3 is cyclic with prime order, only elements being $(\mathbf{1\,2\,3})$ and $(\mathbf{1\,3\,2})$ apart from identity, so it contains no subgroup, let alone a normal subgroup. A_4 has a kernel for homomorphism from $S_4 \to S_3$ which lies in the alternating group, and is hence a proper normal subgroup (see 2.5.13). This makes A_4 a non-simple group.

LEMMA 7.5.5

1. For $n \geq 3$, A_n is generated by 3-cycles.
2. For $n \geq 5$, the three cycles form a single conjugacy class in A_n

Proof. The first is supposed to be anologous to the method of row reduction. Given any even permutation p, not the identity, that fixes m of the indices, we can left multiply a suitable 3-cycle q, so that the product qp fixes atleast $m + 1$ indices. Don't worry we haven't yet shown this. It can be easily understood by considering the following.

Let p be a permutation, other than identity. Now it will either contain a k-cycle with $k \geq 3$ or a product of atleast two 2-cycles. Since numbering the indices doesn't change anything, we suppose $p = (\mathbf{1\,2\,3\,...\,k})...$ or $p = (\mathbf{1\,2})(\mathbf{3\,4})....$ Now let $q = (\mathbf{3\,2\,1})$. Calculate qp and you'll see something startling. The product fixes the index **1**. Why that works can be observed from the simple fact that whatever **1** is mapped to in p, gets mapped back to **1** in q. That simple!

Now for the second, more interesting part. Suppose $n \geq 5$. Now we've to show that for a given q say $(\mathbf{1\,2\,3})$, the conjugacy class is contained in A_n. What we already know is that $C(q) \in S_n$. So for some other 3-cycle, q', $\exists$ p, s.t. $q' = pqp^{-1}$. Now p can either be even or be odd. If its even, then $p \in A_n$. However if p is odd, then we need to come up with some element $p' \in A_n$ (basically p' is even) such that $p'qp'^{-1} = q'$.
Let $\tau = (\mathbf{4\,5})$ which $\in S_n$ since $n \geq 5$. It's clear that $\tau q \tau^{-1} = q$. Replace q in the conjugation with the aforesaid equation and you'll get $q' = pqp^{-1} = p\tau q \tau^{-1} p^{-1} = p\tau q(p\tau)^{-1}$. Since (and quite cleverly so), $p\tau$ is now even, we have shown that the entire conjugacy class $\in A_n$. □

THEOREM 7.5.4 For every $n \geq 5$, A_n is a simple group.

Proof. The proof is the perfect balance between interesting and simple. Look it in the book and there's really nothing much to explain. <TODO: Complete this section should time allow> □

July 10, 2012

7.6 NORMALIZERS The stabilizer of orbit of a subgroup H of a group G for the operation of conjugation by G is called the normalizer of H, denoted by $N(H)$.

$N(H) = g \in G | gHg^{-1} = H$

PROPOSITION 7.6.3 Let H be a subgroup of G, and let N be the normalizer of H. Then

(a) H is a normal subgroup of N.

Proof. $gHg^{-1} = H \; \forall \; g \in N(H)$. And this follows from the definition of $N(H) = \{g \in G \mid gHg^{-1} = H$ $\}$ □

(b) H is a normal subgroup of G if and noly if $N = G$

Proof. For H to be a normal subgroup, $gHg^{-1} = H \; \forall \; g \in G$. So obviously, for that $N(H) = G$ □

(c) $|H|$ divides $|N|$

Proof. follows from (a) □

$|N|$ divides $|G|$

Proof. follows from the fact that $N(H)$ is a stabilizer of H, and the counting formula □

7.7 THE SYLOW THEOREMS

Notation used: $a \mid b$ means a divides b. $a \nmid b$ means the negative of the statement.

SYLOW p-SUBGROUPS

Let G be a group of order n, and let $p \mid n$ where p is prime. Let p^e be the largest power of p that divides n, i.e.

$$n = p^e m$$

where m is an integer and $p \nmid m$. Subgroups H of G with order p^e are called *Sylow p-subgroups of G*. Invoking the counting formula for the Sylow p-subgroup shows that these subgroups are p-groups whose index in the group is not divisible by p.

THE THEOREMS

Let G be a finite group whose order is n. For a given prime p if $p \mid n$, then

THEOREM 7.7.2 FIRST SYLOW THEOREM G contains a Sylow p-subgroup.

THEOREM 7.7.4 SECOND SYLOW THEOREM

(a) The Sylow p-subgroups of G are conjugate subgroups.

(b) Every subgroup of G that is a p-group is contained in a Sylow p-subgroup.

THEOREM 7.7.6 THIRD SYLOW THEOREM say $n = p^e m$, where $p \nmid m$ and let s denote the number of Sylow p-subgroups. Then $s \mid m$ and $s \equiv 1 \mod p$, i.e. $s = kp + 1$, for some integer k.

Before getting into their proofs, let us look at some corollaries.

COROLLARY 7.7.3 OF THE FIRST SYLOW THEOREM G contains an element of order p.

Proof. Let H be a Sylow p-subgroup. Consider an element $x \neq 1 \in H$. Since G is finite, the subgroup $< x >$ (of H) will be finite. Also, the order of $x = | < x > |$. Invoking the counting formula, we know $| < x > |$ divides $|H|$. This means that order x must also divide $|H|$. So order of x must be a positive power of p, say p^k.
Then $x^{p^k} = 1$, which means $x^{p^{k-1} \times p} = 1 \Rightarrow x^{p^{k-1}}$ has order p. □

COROLLARY 7.7.5 OF THE SECOND SYLOW THEOREM G has exactly one Sylow p-subgroup if and only if that subgroup is normal.

Proof. Using the Second Sylow Theorem, its clear that since the p-subgroups are conjugates, if the conjugates are equal, i.e. p-subgroup is normal, then all p-subgroups would be the same. Hence exactly one p-subgroup would exist. □

Now we begin with two lemmas required for the proof of the first Sylow Theorem.

LEMMA 7.7.9 Let U be a subset of a group G. The order of the stabilizer Stab($[U]$) of $[U]$ for the operation of left multiplication by G on the set of its subsets divides both of the orders, $|U|$ and $|G|$.

Supplementary Explanation of the statement: U is a subset. Think of it as a vertex. Left multiplication by G on this subset, produces more of these subsets, like action on a vertex produces a set of vertices. In that sense, the operation of left multiplication by G is on the set of its subsets, and $[U]$ represents the set of subsets. So by this logic, Stab($[U]$) would mean the stabilizer of set of subsets. Let's look at the proof and understand this better.

Proof. If H is a subgroup of G, the H-orbit of an element u of G for left multiplication by H is the right coset Hu. Let H be the stabilizer of $[U]$. [**Doubt** | is this the set of subsets? Since that doesn't make much sense, we are assuming it to mean the set U and ignoring the brackets.] Then multiplication by H permutes the elements of U, so [and now it gets a wee-bit tricky] U is partitioned into H-orbits, which are right cosets (why that happens is because if an element can be changed into another by left multiplication by H, it would, and thus belong to the same orbit, if not, they would still be in the same set, but lie in different orbits). Now each coset has order $|H|$, so by the stabilizer-orbit counting formula, we know $|H|$ divides $|U|$. And since H is a subgroup, by the counting formula, $|H|$ divides $|G|$. □