Symmetry

More Group Theory

SP Status

Atul Singh Arora July 8-12, 2012

This document contains record of my understanding of Chapter 7 More Group Theory, from Artin. I have addressed it to future me so the word choice may not suit everyone.

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, it's 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 $p = (\mathbf{1\,2\,3\ldots k})\ldots$ or $p = (\mathbf{1\,2})(\mathbf{3\,4})\ldots$. 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 it's 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, but its strategy is fairly interesting. <TODO: Complete this section should time permit> □

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.

July 11, 2012

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: Carefully understand section 6.10 (Operations on Subsets), everything used here, including notation makes perfect sense. If it doesn't, read section 6.8 (The operation on Cosets). I got stuck here for a while until clarity was recovered or to be accurate attained.

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** | What is the bracket notation supposed to mean? Is this the set of subsets? **Clarification** The bracket notation implies U is considered an element of the set of subsets.] Then multiplication by H permutes the elements of U, so U is partitioned into H-orbits, which are right cosets (why that happens is because if an element say $u_1 \in U$ can be changed into another, say $u_2 \in U$ by left multiplication by some $h \in H$, both would belong to the same orbit. If for no $h \in H$ this happens, then, they, despite being in the same set, would lie in different orbits). Now since each coset has order $|H|$, thus each orbit has order $|H|$. Now since orbits partition the set, and since each orbit is of the same size, $|U| = |\text{orbit}| \times (\text{number of orbits}) = |H| \times (\text{number of orbits})$, we know $|H|$ divides $|U|$. And since H is a subgroup, by the counting formula (or more specifically, by Lagrange's Theorem) $|H|$ divides $|G|$. □

LEMMA 7.7.10 Let n be an integer of the form $p^e m$, where $e > 0$ and p doesn't divide m. The number N of subsets of order p^e in a set of order n is not divisible by p.

Proof. N is basically ${}^nC_{p^e}$ which is

$$\binom{n}{p^e} = \frac{n\,(n-1)\ldots(n-k)\ldots(n-p^e+1)}{p^e(p^e-1)\ldots(p^e-k)\ldots 1}$$

$N \not\equiv 0 \mod p$ simply because every time p divides a term $(n-k)$ in the numerator of N, it divides the term $(p^e - k)$ of the denominator just as many times (proved in just a moment).

So for those who still don't understand why it makes any difference, consider q, f_1 and f_2 s.t. $p \nmid f_1$, $(n-k) = p^q f_1$ and $(p^e - k) = p^q f_2$ since the second term is divisible by p as many times as the first. Now when you divide these, viz. first over the second, the result no longer has p in the numerator and is hence not divisible by p and since this happens for all possible numerator terms divisible by p, $p \nmid N$.

Now for the proof of the statement, write k as $p^i l$, where $p \nmid l$, then $i < e$. Replace this for k and it makes both terms divisible by p^i but not by p^{i+1} [**Find Out** Why the second assertion and how?] □

We are now ready to prove the first Sylow theorem. Lets start.

Proof of the First Sylow Theorem. What is given in Artin, is straight forward, yet for confirming I have understood, I am redoing the proof.

STRATEGY We start by considering the set $\mathcal{S}$ of all subsets of G of order p^e. If the theorem were assumed true, then one of these subsets will be the Sylow's p-subgroup. However, instead of finding this explicitly directly, we show that for some element of $\mathcal{S}$, say $[U]$, the stabilizer would have order p^e and gotchya, that would be the Sylow's p-subgroup we intended to find.

First thing we note here is that according to Lemma 7.7.9, we know that p will not divide the order of $\mathcal{S}$. Now we split the set $\mathcal{S}$ into orbits for the group action of left multiplication by G. Since orbits partition the set, we have

$$N \text{ (as in the lemma) } = |S| = \sum_{\text{orbits } O} |O|$$

Now obviously, at least one orbit must have an order which is not divisible by p. Let that orbit be $O_{[U]}$ of the element $[U] \in \mathcal{S}$. Let H be the stabilizer of $[U]$. Now using the counting formula for orbit and stabilizer, we have $|G| = p^e m = |H|.|O_{[U]}|$. Since $|O_{[U]}|$ is not divisible by p, it must equal m according to the equation. Thus, $|H|$ must be equal to p^e and therefore H my friend is the Sylow's p-subgroup. □

Before moving to the proof of the second Sylow's theorem, there's a 'pseudo' lemma which is elementary, but must be proven for avoiding any confusion. It's as follows.

THEOREM 7.3.2 THE FIXED POINT THEOREM Let G be a p-group and let S be a finite set on which G operates. If the order of S is not divisible by p, there is a fixed point for the operation of G on S viz. $\exists$ a point s whose stabilizer is the whole group.

Proof. Basically the proof requires the use of both counting formulae. The first says $|G|$ =|stabilizer||orbit|. Now $|G| = p^e$ for some p and e. The order of an orbit must be a number and therefore |stabilizer| would be a power of prime, and consequently, |orbit| would be p^k for some $k \leq e$. So |orbit| is either 1 or a multiple of p.
Using the next formula, we break the set S into orbits. We have

$$|S| = |O_1| + |O_2| + |O_3| + \ldots$$

$$= \sum (\text{orbits whose orders are multiples of } p) + \sum (\text{orbits with order } 1)$$

Now since $|S|$ is not divisible by p, there must be at least one orbit with order 1. The stabilizer of this orbit will have order p^e and must thus be the whole group. Therefore there must be at least one element in S that is fixed under the action of G. □

Now we are good to go.

Proof of the Second Sylow Theorem. Basically same proof as Artin's, with different language and the 'obvious' unsaid part explained

STRATEGY For a given p-subgroup, say K and Sylow p-subgroup, say H, both of G, we'll show that K is contained in a conjugate H' of H. That would prove part (b). For part (a), if K is a Sylow p-subgroup, then K equals H' since H' contains K and both have the same order.

We start with listing 3 desired properties of a subset of G, say $\mathcal{C}$.

(a) $|C|$ should not be divisible by p

(b) Operation of G on $\mathcal{C}$ should be transitive

(c) $\mathcal{C}$ should contain an element, say c, whose stabilizer is H

Now we must show that such a set exists. Well, the *set* of left cosets of H, possesses all 3 properties. We better confirm that.

(a) The counting formula says $|G| = |H||\text{number of cosets of } H|$
And by definition of $\mathcal{C}$, we have $|\text{number of cosets of } H| = |\mathcal{C}|$
Since by definition of Sylow p-subgroup, if we let $|G| = p^e m$, where $p \nmid m$, then $|H| = p^e$, therefore $|\mathcal{C}|$ is m which means its not divisible by p.

(b) Any coset of H can be written as gH for some $g \in G$. Thus for the action of G, all cosets of $H \in$ the same orbit. Thus, the action is transitive.

(c) Every element of $h \in H$ is stabilized by H because H is a group. So the element $c \in \mathcal{C}$ which is fixed by H is $[H]$.

Now the magic. Restrict the group action of G to the p-subgroup K. Since K is a p-subgroup, and p doesn't divide $|\mathcal{C}|$ (property (a)), we can invoke the fixed point theorem to conclude that under the action of K, $\exists\, c' \in \mathcal{C}$ which remains fixed.
Also, the operation of G is transitive on $\mathcal{C}$ (property (b)), therefore, $c' = gc$ for some $g \in G$. We also know that H is the stabilizer of c (property (c)), therefore $gHg^{-1} = H'$ (say) stabilizes gc which is c' itself (you can quickly verify this by seeing $gHg^{-1}gc = gHc = gc = c'$). Therefore, H' contains K! □

Proof of the Third Sylow Theorem. This theorem has become very close to my heart, at least temporarily. Reason is a confusion which initiated because of my foolish assumption, viz. cosets are subgroups. Don't make that mistake and the proof would appear natural.

As before, let $|G| = p^e m$ where $p \nmid m$. Let H be a Sylow p-subgroup. From the counting formula, we can see that m is the number of cosets of H, which is the same as the index $|G : H|$. So we have,

$$m = [G : H] = \frac{|G|}{|H|} \tag{2}$$

Let S denote the set of Sylow p-subgroups and let $s = |S|$, the number of Sylow p-subgroups. Now the stabilizer of a particular Sylow p-subgroup, say $[H]$ would be the normalizer $N(H)$, since according to the second Sylow theorem, the Sylow p-subgroups are conjugates. Also, H is a normal subgroup of $N(H)$. This means $|H|$ divides $|N(H)|$, viz.

$$|N(H)| \equiv 0 \mod |H| \tag{3}$$

Now the number of Sylow p-subgroups, say s, would equal the number of elements in the conjugacy class of H. The stabilizer of H under conjugation is $N(H)$ by definition. Using the orbit-stabilizer counting formula, we have,

$$s = [G : N(G)] = \frac{|G|}{|N(H)|} \tag{4}$$

Using equations 2, 3 and 4, we have

$$m \equiv 0 \mod s$$

So this proves the first part, viz. s divides m. The next part requires us to show that $s \equiv 1 \mod p$. We proceed by breaking S, the set of all Sylow p-subgroups, into H-orbits, for the action of conjugation by H. Now since H is p-group, the order of any H-orbit should be a power of p. When the power is zero, the order will be 1, implying H fixes the element. One such element is $[H]$. If we are able to show that it is the only element, then we'll have

$$s = \sum (\text{multiples of } p) + 1$$

and therefore

$$s \equiv 1 \mod p$$

Say H stabilizes another element of S, namely $[H']$. Then $H \in N(H')$. Also, $H' \in N(H')$. Using the second theorem for Sylow-p-subgroups H and H' in $N(H')$ (whose order is greater than p^e since it contains H, and is also divisible by p as follows from the counting formula), H must be expressible as a conjugate of H', viz. $H = nH'n^{-1}$ for some $n \in N(H')$. However, H' is normal in $N(H')$, hence $H = nn^{-1}H' = H'$. Thus $[H]$ is the only element stabilized by H. And that concludes the proof. □

July 13, 2012

7.9 The Free Group Here are some difinitions for reference. *Free groups* are those whose generators satisfy no relation other than the ones implied from the group operation, for instance associativity. *Free Semi-groups* are sets that are generated by generators with no relation as in free groups, but they don't have inverses. A word is called *reduced* if no ruther cancellations can be made. If we start with w and reduce it to w_0, then the latter is called the *reduced form.*

Proposition 7.9.2 There's only one reduced from of a given word w.

Proof. We show that each method of cancellation is equivalent, and hence the given word w has a unique w_0. Consier the length of w. If the length can't be reduced, then there's nothing to prove. If the length can be reduced, there exists some pair of symbols that can be cancelled, viz.

$$w = ...xx^{-1}....$$

Let's consider the reduced form w_0. It obviously can't contain the pair xx^{-1}. Now there're two cases. First, the pair got cancelled at some stage during the process. So we can do that at any stage we please, without affecting the cancellation procedure. Second, one of them got cancelled at some stage as

$$...\ \cancel{x}^{-1}\ \cancel{x}x^{-1}... \quad \text{or} \quad ...x^{-1}\ \cancel{x}\ \cancel{x}^{-1}...$$

Notice that the result is the same whether we cancel as above or cancel xx^{-1}, the pair. So this goes back to the first case. This shows that any two cancellation methods can be shown to be equivalent, and hence proves the proposition. □

$w \sim w'$ if they have the same reduced form, viz. $w_0 = w_0'$.

Remarks

July 11, 2012

Lemma 7.7.9 and 7.7.10 despite being fairly elementary, did help me clearly understand the basics from the previous chapter, till the very last moment of documenting them.

Why can't I see the obvious easily?
<TODO: Quote instances>

1. The main argument of Lemma 7.7.10

July 13, 2012

For some reason I just couldn't get myself to study today. Events from the past two days could have had this effect when I'd worked longer than I'd scheduled myself to.