SYMMETRY AND GROUP THEORY

ATUL SINGH ARORA

Mathematics

Prof. Kapil Hari Paranjape
Indian Institue of Science Education and Research, Mohali

May 28 - July 28, 2012

Atul Singh Arora: *Symmetry and Group Theory,* Mathematics,

Every honest researcher I know admits he's just a professional amateur. He's doing whatever he's doing for the first time. That makes him an amateur. He has sense enough to know that he's going to have a lot of trouble, so that makes him a professional.

— Charles F. Kettering (1876-1958) (Holder of 186 patents)

ACKNOWLEDGEMENTS

I express my sincere gratitude to my project guide, Prof. Kapil Hari Paranjape for his time, effort and guidance, which he provided, even during the busiest of his schedules. I owe my interest in the topic, to him as it was during his course that I got the opportunity to explore this unseen beauty of the subject.

I also thank Vivek Sagar (MS11017) for sharing his progress during the summers, as he'd also worked on a very similar topic.

CONTENTS

1 BRIEF OUTLINE 1
- 1.1 Introduction 1
- 1.2 Summary 1

2 SUBGROUPS OF THE ROTATION GROUP 7
- 2.1 Pole of Group Element: 7
- 2.2 G-Orbits and Poles: 7
- 2.3 Spin: 8
- 2.4 Deriving a Famous Formula: 8
- 2.5 Application of the Famous Formula: 10

3 MORE GROUP THEORY 19
- 3.1 Corollary 5.1.28 19
- 3.2 **7.4 The Class Equation of the Icosahedral Group** 19
  - 3.2.1 Simple Groups 20
  - 3.2.2 Lemma 7.4.2 20
  - 3.2.3 Theorem 7.4.3 20
  - 3.2.4 post Theorem 7.5.4 (statement) 21
  - 3.2.5 Lemma 7.5.5 21
  - 3.2.6 Theorem 7.5.4 21
- 3.3 **7.6 Normalizers** 22
  - 3.3.1 Proposition 7.6.3 22
- 3.4 **7.7 The Sylow Theorems** 22
  - 3.4.1 Sylow p-subgroups 22
  - 3.4.2 **The Theorems** 23
  - 3.4.3 Proofs 23
- 3.5 **7.9 The Free Group** 28
  - 3.5.1 Proposition 7.9.2 28
  - 3.5.2 Proposition 7.9.3 28
  - 3.5.3 Definitions 29
  - 3.5.4 Proposition 7.9.4 29
- 3.6 **7.10 Generators and Relations** 29
  - 3.6.1 Definition 7.10.1 29
  - 3.6.2 Lemma 7.10.3 30
  - 3.6.3 Definition 7.10.4 30
  - 3.6.4 Example 7.10.7 31
  - 3.6.5 Example 7.10.11 32
  - 3.6.6 Proposition 7.10.12 Mapping Property of the Free Group 32
  - 3.6.7 Proposition 7.10.13 Mapping Property of Quotient Groups 32
- 3.7 **7.11 The Todd-Coxter Algorithm** 34
  - 3.7.1 Rules 7.11.3 34

1 BRIEF OUTLINE

1.1 INTRODUCTION

My summer project consisted of two parts. The first was about reading Linear Algebra in greater depth than was covered in the course, and the second was about exploring Knot theory. For the former, I used the second edition of Michael Artin's Linear Algebra, and for the latter various books were referred to. The most interesting part of the project was the very beauty of mathematical abstraction. It was exceedingly fascinating for me to follow the author's flow and to apply abstractions at various levels to achieve unusual, striking results. Apart from the mainstream mathematics, during the exploration period, I read a little about mathematical history, the development of sigma delta definitions, quarternions and spent significant time on understand mathematical developments on the understanding of Knots. Overall, it was a very enriching experience, the mathematical part of which has been documented in detail using LaTeX, learning which, for typecasting the report, turned out to be another very rewarding skill.

1.2 SUMMARY

Following is a date-wise summary of my work. All numbers that seem arbitrary are sections from the aforesaid Artin's book.

1. May 28
   a) Product Groups
   b) Correspondence Theorem
   c) Prime fields
2. May 29
   a) 3.3 3.5
   b) Computing with bases
   c) Direct Sum
   d) Infinite Dimensional Spaces
   e) Python mod p
3. May 30
   a) 4.2
   b) Linear Operators

   c) Eigen Vectors
   d) Characteristic Polynomials
   e) Triangular and Diagonal Forms
   f) Jordan Form (not completed)

4. May 31
   a) Jordan Form (continued)
   b) Applications of Linear Operators

5. June 1
   a) Proof of Euler's Theorem
   b) Isometries
   c) Change of coordinates
   d) Isometries of the plane
   e) 6.3.5
   f) 6.3.8
   g) Difference between Points and Vectors
   h) Finite groups of Orthogonal Operators on the plane
   i) Fixed Point theorem
   j) Lemma 6.4.9 Corollary 6.4.1
   k) 6.5 intiated

6. June 2
   a) Translation Groups
   b) Theorem 6.5.5
   c) The Point Group
   d) Crystallographic Restriction
   e) Theorem 6.5.12, discrete H

7. June 3

Sunday

8. June 4
   a) Revision
   b) Read about Encryption from Michael J Jacobson and Hugh C Williams
   c) Revised change of coordiantes + application in isometries
   d) revising proof of theorem 6.4.1
   e) 6.5 Re analysis of Discrete Groups of Isometries
   f) Crystallographic Restriction

9. June 5
    a) Stuck at Claim of Prop 6.6.4
    b) Understood 6.6.4
    c) 6.7 Abstract Symmetry
    d) 6.8 Operations on Cosets
10. June 6
    a) Built a Telescope for transition of Venus
    b)
    c) June 7
    d) Revisited the Correspondence Theorem
    e) 6.8 again
    f) 6.9 The counting formula
    g) stuck, trouble with partitioning with orbit using subgroups
    h) 6.9 Completed
    i) 6.10 Operation on subsets
    j) 6.11 Permutation Representation
    k) 6.11.3 Done
    l) 6.12 Finite Subgroups of the Rotation Group
    m) completed till 6.12.6
11. June 8
    a) Revisited Example 6.12.3
    b) LaTeX installation and setup research initiated
    c) 6.12 with latex
    d) Poles with latex
12. June 9
    a) Application of the Famous Formula, Latex
13. June 10

Sunday

14. June 11
    a) 6.12, Finite subgroups of the rotation group
    b) Documenting the k-gon orbit of poles
    c) Case 2 with 3 more subcases initated
    d) Thought about the second case
15. June 12

- a) Symmetries of an Octahedron
- b) Documenting that
- c) Icosahedron
- d) *Finished the Symmetry Chapter*

16. June 13
    - a) Worked on an interesting physics problem | Motion of water pipe
    - b) Looked for books related to Braid groups
    - c) Got a book by Christian Kassel issued
    - d) Corresponding with sir

17. June 14, 15
    - a) Reading Knots: Mathematics with a Twist
    - b) Till Chapter 5

18. June 17

Sunday

19. June 26-30, 2012 (Tuesday, the day I returned till Saturday) done on paper
    - a) Revised chapter 5 from the book Knots
    - b) Completed reading chapter 6, 7 and 8.
    - c) Sent a very brief report
    - d) Initiated and completed the following Symmetry problems
    - e) 3.6 (a,b)
    - f) 4.1
    - g) 4.2 (a)
    - h) 4.2 (b)
    - i) 4.2 (c)
    - j) 4.3 (a), (b), (c)
    - k) 5.1
    - l) 5.5
    - m) 5.6
    - n) 5.7
    - o) 5.8 (a)
    - p) 5.9
    - q) 5.11 (a)
    - r) 5.11 (b)

- s) 5.11 (c)
- t) Worked on understanding the precise difference between a vector and a point.
- u) PRoved independently Vivek's theorem about the number of elements necessary and sufficient to generate a symmetric group of order n.
- v) Attempted classification of wallpaper patterns and their symmetry
- w) Getting Certification for KVPY

20. July 2-7, 2012 (Monday to Friday, Saturday omitted) mostly on paper, and reading
    - a) Redid section 6.8, operation on coset, to gain further familiarity
    - b) Met with Prof. Paranjape to discuss the project.
    - c) Attempted Problem 7.3 (non-transitive action of S3 on a set of 3 elements)
    - d) Initiated chapter 7 and completed till section 7.3
21. July 8-13, 2012 (Sunday to Friday, Saturday omitted) reading and documenting in LaTeX
    - a) Studied Chapter 7 till section 7.9 (still left to complete)
22. July 16-22, 2012 (Monday to Sunday) reading | working on a parallel project
    - a) Studied about the History of the delta sigma definition of limits and development of rigorous calculus.
    - b) Studied about the development of Quaternions by Hamilton and inspiration because this seemed very unnatural to me at the first glance.
23. July 23-28, 2012 (Monday to Friday)
    - a) Read and Typesetted till section 7.10
    - b) Read section 7.11
    - c) Completed Todd-Coxter's Algorithm

2 SUBGROUPS OF THE ROTATION GROUP

June 8, 2012

2.1 POLE OF GROUP ELEMENT:

Let G be a finite subgroup of SO_3, of order $N > 1$. For now, consider only the rotation elements (of $\mathbb{R}^3$) $\in G$. Poles for such an element $h(\neq 1) \in SO_3$ are defined as the intersection points of the axis of rotation with the unit sphere $\mathbb{S}^2$. h can't be identity since the definition of pole requires existence of an axis. Clearly, for each such h, there are 2 poles.

POLE OF A GROUP: Similarly in general, pole is defined for an element $g(\neq 1) \in G$. This pole can also be referred to as pole of the group.

Thus, a pole of G, is a point, fixed by a group element $g \neq 1$.

2.2 G-ORBITS AND POLES:

According to Artin, and I quote "The set $\mathcal{P}$ of poles of G, is a union of G-orbits. So G operates on $\mathcal{P}$."

Here's the analysis of the second part of this statement. The set $\mathcal{P}$ of poles is basically a set of points. Each of these points can be "operated" upon by an element of G. In accordance with the definition of the word "operate" in terms of group action, we must verify that the point obtained after multiplication with an element $g(\neq)1 \in G$ is also a pole. The other properties of group action are easy to verify.

Let us prove it before continuing.

Consider a pole $p \in \mathcal{P}$.

Now $\exists\ h(\neq 1)$ s.t. $hp = p$ [from the definition of pole]

Let g be an element of G. We have to show that $gp = q(say)$ is also a pole,

that is, $\exists\ k(\neq 1)$ s.t. $kq = q$

Lets replace q with gp in both sides, and p with hp in the RHS in the equation above.

So we need to solve for k in the equation

$\Rightarrow kgp = ghp$

$\Rightarrow k = ghg^{-1}$

Since G is a group, ghg^{-1} exists and thus k exists, proving gp to also be a pole of the group (specifically of k). Hence, we have shown G operates on $\mathcal{P}$.

Now for the first part of the statement. First, orbits are defined for a particular element of a set. However, if the set is the same as the orbit, then it needn't be specified.

Immediate Context before the doubt | In this case, let's fix a pole. The orbit of this pole under the group action would be the set of all poles obtained by operation of all $g \in G$. We just proved that each element of the group, when operates on a pole, creates another pole (of an element present in the group). Union of all the orbits must therefore be equal to $\mathcal{P}$, as $\mathcal{P}$ was defined to be the set of all poles of G.

Doubt | However, Artin has presented this in the other way as can be seen from the quote. What am I missing here?

2.3 SPIN:

For a given $g \in G$, spin is the number of unordered pairs (g, p), where p is a pole of the group G.

Since each rotation (excluding identity) has two poles, there are two unordered pairs associated, and thus the spin of each such rotation is two.

2.4 DERIVING A FAMOUS FORMULA:

The first objective here is to find a relation between the order of stabilizers for different p, and the order of the group, G.

Now, for a given pole p, all elements $g \in G$, that leave p unchanged, form a set G_H. G_H is a cyclic subgroup and also a stabilizer by definition. The fact that its a subgroup can be verified easily as was done for the kernel. It is cyclic because the group G is finite. It then follows that G_H is generated by rotation by the smallest angle $\theta (> 0)$ present in the group. If the order of the group G_H is given by r_p, then $\theta = 2\pi / r_p$.

Doubt | *(Supplement explanation)* Is it correct to note here that the stabilizers G_H for different poles p, will either form the same subgroup, or be disjoint (can be readily verified). The case would be former if and only if the poles are a result of intersection of the same axis. The latter would happen for all other cases. Also, if such subgroups were created for every pole p of G, their union would exhaust the group G.

Now if all such stabilizers, minus their identity element, are made into a union, they would consequently contain twice as many elements as there are in (G minus the Identity element). i.e.

$$\sum_{p \in \mathcal{P}} r_p - 1 = 2 \times (|G| - 1) \tag{1}$$

It took me a while to get here. This relation is exactly the same as that given in Artin, but I would want to confirm if the reasoning is correct.

(Textbook method explained) Now since p is a pole, the stabilizer G_H will contain at least one element other than identity, and thus $r_p > 1$. Consequently $r_p - 1$ elements (since we're excluding identity), stabilize p. Each of these elements thus has a spin two.
So every group element except the identity has two poles, implying its spin is 2. Taking $|G| = N$, there are $2(N-1)$ spins. Recalling that spin means the number of unordered pairs (g, p) for a given p, total spins would be the total number of unordered pairs (g, p). Now if we sum over all $r_p - 1$ (for excluding identity), then also we are counting all such pairs.
So the same relation (equation 1) follows from this school of thought.

So lets move forward. To simplify the LHS of equation 1, we will use the counting formula.

We already know from the counting formula (Size of a Group G= Order of coset of H× Number of Cosets) that

$$|G| = |G_H| \times |\text{Orbit of } G_H| \tag{2}$$

since there is a bijective map between the orbit of G_H and the cosets of G_H.

Let n_p denote |Orbit of G_H|. Rewriting both equations in terms of N, r_p and n_p, we get

$$N = r_p \times n_p \tag{3}$$

Now we can see that if two poles p and p' are in the same orbit, then the order of their orbits is the same, i.e. $n_p = n_{p'}$. Equation 3 demands the order of their Stabilizers to also be the same, i.e. $r_p = r_{p'}$. Let's us arbitrarily denote different orbits by $O_1, O_2, ... O_k$. Now we note that if $n_i = n_p$ (note that the p is the same as it was in the previous context, a particular pole in the summing, although this result is not dependant on it) so by equation 3 we have $r_i = r_p$.

It is right here that I got stuck, which caused me to initiate writing like this in the first place. Now the trick here is to realize this very essential fact which is as follows.
We are summing over all poles p in equation 1. Now if $\exists\, p$ s.t. $p \in O_i$, then $\exists\, n_i$ poles in the orbit, each with the same number of stabilizers, i.e. $(r_p - 1) = (r_i - 1)$ since $r_p = r_i$.
Now we can, from the left side of the equation, take out the contribution of all such poles to the total spin, and express it as $n_i \times (r_i - 1)$.

Also, each pole must belong to some orbit, therfore the entire sum (the LHS) may be written as

$$\sum_{i=1}^{k} n_i \times (r_i - 1) = 2 \times (N - 1) \tag{4}$$

Take r_i common from LHS and divide by N on both sides, to obtain

$$\sum_{i=1}^{k} (1 - \frac{1}{r_i}) = 2 \times (1 - \frac{1}{N}) \tag{5}$$

And that was the 'famous' formula I'd never even seen before! As the book says, this formula might look small, but its a very strong tool.

The power of this function will be explored tomorrow.

June 9, 11 & 12, 2012

2.5 APPLICATION OF THE FAMOUS FORMULA:

The famous formula is:

$$\sum_{i=1}^{k} (1 - \frac{1}{r_i}) = 2 \times (1 - \frac{1}{N}) \tag{6}$$

Recalling that N is the order of the group which is not trivial, hence $N > 1$. Also, N is an whole number, and therefore the smallest value it can have is 2. So the RHS $\geqslant 1$. Also, as $N \to \infty$, the RHS $\to 2$, but remember N is finite. So effectively the $1 \leqslant \text{RHS} < 2$. Also, each term in the LHS $\geqslant \frac{1}{2}$, since $r_i \geqslant 1$.

Now since the LHS must equal the RHS, there can't be more than 3 terms of LHS, else the sum would become $\geqslant$ 2, which the RHS can't reach for any value of N.

Dividing this into 3 and classifying, we get

One orbit:

So for a single orbit, $k = 1$. So, the LHS becomes

$$1 - \frac{1}{r} < 1 \tag{7}$$

while the RHS

$$2 \times (1 - \frac{1}{N}) \geqslant 1 \tag{8}$$

So this case is impossible.

Two orbits:

For two orbits, we would have

$$(1 - \frac{1}{r_1}) + (1 - \frac{1}{r_2}) = 2 - \frac{2}{N} \tag{9}$$

which is the same as

$$\frac{1}{r_1}+\frac{1}{r_2}=\frac{2}{N} \tag{10}$$

Doubt | From this itself, Artin concludes that since r_i divides N, the equation will hold only when $r_1 = r_2 = N$. I was unable to see why this was so. However, a little manipulation got me to the same result, but it still doesn't seem obvious to me. What am I missing?
Here's what I'd done.
Replaced N once with r_1n_1 and one with r_2n_2 to get

$$\frac{1}{r_1}+\frac{1}{r_2}=\frac{1}{r_1n_1}+\frac{1}{r_2n_2} \tag{11}$$

rearranged

$$\frac{1}{r_1}(1-\frac{1}{n_1})=\frac{1}{r_2}(\frac{1}{n_2}-1) \tag{12}$$

simplified

$$\frac{1}{r_1n_1}(n_1-1)=\frac{1}{r_2n_2}(1-n_2) \tag{13}$$

since $r_1n_1 = r_2n_2$

$$n_1+n_2=2 \tag{14}$$

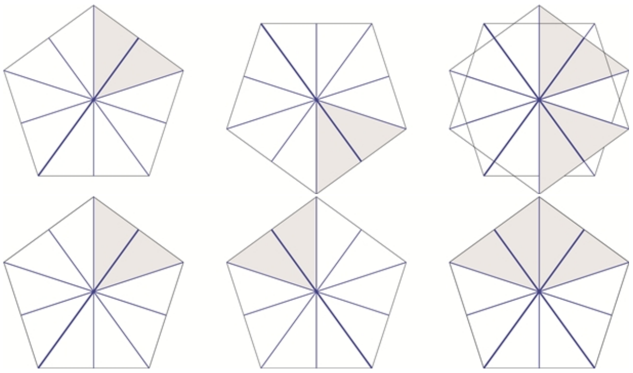
And since each orbit must contain atleast one element, $n_i \geqslant 1$. So the only possible solution is
$n_1 = n_2 = 1$
$\Rightarrow r_1 = r_2 = 1$.
So since there are only two poles, both fixed by all elements in G hence, the only possibility (of the type of elements in the group) is rotation about a single axis, passing through both these poles (read points!).

Doubt Context | Now as Artin says, is the most interesting case.
Three orbits: What the text says till Case 1: $r_1 = r_2 = 2$ and $r_3 = k$ s.t. $N = 2k$, is clear. For further clarity its given as
$r_i = 2, 2, k; \quad n_i = k, k, 2; \quad N = 2K$
It goes on to then say that there's one pair of poles p, p' making the orbit O_3. So far so good as it readily follows from the value of n_3.
Doubt | This is where I'm stuck.
It asserts, *Half* of the elements of G fix p, and the other *half* interchange p and p'.
Elephant in the room is, why Half?
This is what I had in mind, but I'm not sure.

My Analysis:
Now we know that O_3, contains 2 elements since n_3 is 2. For a pole in this orbit, say p as used above, $r_p = r_3$ [terms have the meaning as per their prior definition]. This means that the stabilizer of the pole, has order k and these are rotations about the axis passing through the origin and the pole (read point) p. Since there are only two poles, the other pole p' must lie on this very axis. Thus, the same K stabilizers,

stabilize it. However the group has 2K elements. The other elements are NOT stabilizers and hence MUST interchange p and p'. So they are 'reflections' which in $\mathbb{R}^3$ become rotations by π about a line perpendicular to the line containing the poles. So half of them are fix p, other half interchange p and p'.

So effectively, there are K rotations about the axis $p\,p'$. The rest of the rotations have their axis contained in a plane perpendicular to the $p\,p'$ axis and passing through its mid point. This is so that each such rotation does infact swap the poles p and p'. **Doubt I** This is where the story gets even more interesting. I initially thought like so. I imagined a point in the said plane. Then I pictured it getting rotated by an angle $\theta = 2\pi/K$ (why this, the rigorous proof is given in the text, basically its because the group [since they're stabilizers] of rotations is finite) along the $p\,p'$ axis. The orbit of the point makes the vertices of a regular K-gon. Then I went on to imagined "reflecting" the K-gon, for the orbit is obtained by operating the point with all group elements. However, here's the mistake I made. I ended up reflecting the pentagon (that's what I'd imagined for simplicity) along an axis which doesn't exist in the group! This resulted in expansion of the orbit and that kept me startled for a while, until I realized that the pentagon must be "reflected", and by that I mean, rotate by π along one of the axis contained in the plane. The result in that case of the "reflection" is again the same pentagon. So the orbit obtained in general will be K-gon.



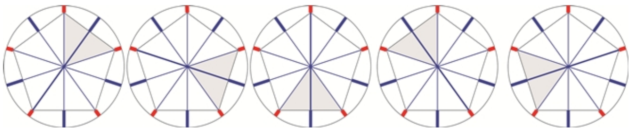
The trouble however is that there are supposed to be two distinct orbits, each with K distinct elements, with 2 stabilizers. Now one stabilizer is identity, and so the other must be rotation by *some* angle (the angle must actually be π, since p and p' are the only points in their orbit) along an axis containing the element.

As has been shown, one of the orbits consists of the poles corresponding to the vertices of the k-gon. (I've come back to poles since poles are what we derived the "famous formula" using.)

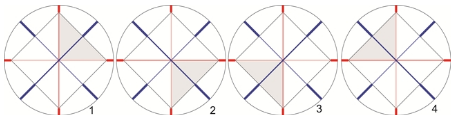
The text says that the vertices & the centres of the faces of the K-gon *correspond* to the remaining poles.

So essentially, the centre of faces, which in this case may even be taken to be the centre of the edges, also form an orbit such that each

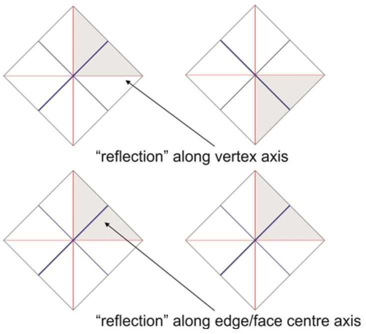
element has 2 stabilizers (one is identity, the other rotation by π [effectively a reflection along the chosen axis]).
Now two interesting cases arise. When K is odd, say 5 for a pentagon, the poles made by opposite face/edge centre and vertex, correspond to the same axis. Yet, when the pentagon is rotated, the vertices go to the vertices, and the face/edge centres go to themselves, preserving 2 different orbits. Take a moment to realize that there aren't any other poles such that their stabilizer is of order two and they restrict the orbit of p and p' to p, p'.
In this case, the reflections as was shown earlier, map the pentagon to a pentagon so the orbits are preserved.



And when K is even, say 4, the poles made by opposite faces/edge centres form an axis, and those made by opposite vertices, form a different axis. And again, the poles made by the faces goto faces (under rotation by $2\pi/K$) & correspondingly the poles made by the vertices, goto vertices. So the orbits continue to be separate!



NOTE: I did not include reflection in the analysis above since again, the reflections along both kind of axis, map the square to a square, and the orbits are thereby preserved.


“reflection” along vertex axis

“reflection” along edge/face centre axis

With that done, lets move on to the next case.
The arguments in the book are easy to follow. The conclusion is given as follows:

A. $r_i = 2, 3, 4;\ n_i = 6, 4, 4;\ N = 12$

The poles in the orbit O_3 are the vertices of a regular tetrahedron, and G is the tetrahedral group T of its 12 rotational symmetries.

B. $r_i = 2, 3, 4;\ n_i = 12, 8, 6;\ N = 24$

The poles in the orbit O_3 are the vertices of a regular octahedron, and G is the octahedral group O of its 24 rotational symmetries.

C. $r_i = 2, 3, 5;\ n_i = 30, 20, 12;\ N = 60$

The poles in the orbit O_3 are the vertices of a regular icosahedron, and G is the icosahedral group I of its 60 rotational symmetries.

Take a note and verify the fact, that r_i represents the number of edges, the number of faces and the number of vertices respectively. Why that's happening (aside from the ordering) is partially answered if one thinks of them as caused by the rotation of different stabilizers (of varied order) to form different orbits.

In Artin the explanation for the number of symmetries for the first two shapes is probably left as an exercise.
However an attempt to understand the concept of "truncated polyhedron" seems futile without first deriving these simpler, more intuitive results.

A. So for a tetrahedron, we can begin the analysis by considering the rotational symmetry about its vertices. Note that the symmetrical axis about a vertex, passes through the centre of the face on the opposite side. So we will not count the rotational symmetry for the faces. So we have a 3 fold symmetry, of which one element in the group will be identity, which will be common, so there are 2 distinct group elements corresponding to each vertex. Also, there are 4 vertices. So there are $2 \times 4 = 8$ non-identity elements in the group, because of symmetry of vertices (and faces). The remaining elements come from the rotation along an axis through the centre of edges, but we must be careful here as well, for each axis of symmetry passes through the centre of 2 edges. Also, the symmetry is 2 fold, and only 1 element is therefore non-identity. There are 6 edges, 3 of which share an axis, so we have $1 \times 3 = 3$ more non-identity elements in the group.
The total then becomes $8 + 3 + 1$ (the identity element) $= 12$ and that's precisely what was expected.

B. Now the next shape is an octahedron. So first let's resolve the simplest rotational symmetries. Consider rotations about the axis joining opposite vertices, which have a 4 fold symmetry. There are 6 vertices and therefore 3 such axis. So total contribution from this rotational symmetry will be $3 \times (4-1) = 9$. Next consider axis created by joining opposite edge centres. There are 12 edges & thus 6 edge centres. The rotational symmetry is 2 fold. Thus their contribution is $6 \times (2-1) = 6$. The last symmetry is easier to visualize if we picture a cube, and its centres of faces forming the octahedron. Now consider the body diagonal of the cube. There are 4 body diagonals and around each there is a 3 fold symmetry. So the final contribution will be $4 \times (3-1) = 8$. So the total number of symmetries becomes $9 + 6 + 8 + 1$ (identity) $= 24$, as was expected and is given in the text.

Doubt I Interesting Observation: As was shown in the discussion for the k-gon, poles corresponding to vertices (or edge centres) do NOT span the entire set of poles. Similarly in a cube, the edge centres don't span the poles of a cube, but the figure they span is called a *truncated polyhedron*, as claimed by the text.

C. To justify this assertion, Artin uses an entire page. So this won't be quite as straight forward. So let's start. Let V be the orbit O_3 of order 12. Thus, the order of stabilizer of each pole in the orbit will be 5. Now we choose any pole p, present in V and "declare it" to be the north pole of the unit sphere. Now that is sufficient to derive an equator from it (a unit circle with centre at origin, that lies on a plane perpendicular the line containing p and the origin) and also a south pole (diametrically opposite point to p). Now we let H be the stabilizer of p which as stated earlier, must have order 5. Thus H is a cyclic group, generated by a rotation (say x) about p with an angle $2\pi/5$. **Doubt I** At this stage Artin asserts there must be 2 H-orbits of order 1 and then goes on to identifying them as north & south poles.

Continuing with my analysis, since H consists of orthogonal operations, thus if p is stabilized, so will its diametrically opposite point be, i.e. the south pole. So H has 1 orbit with 2 elements.

Now since H has order 5, the remaining poles (i.e. poles that have a stabilizer of order 5), form two H-orbits of order 5. **Doubt I** Now on what rigorous mathematical grounds should I back that argument? I have to somehow show that all poles that have a stabilizer of order 5, under the action of H, form an orbit of order 5.

Back to Artin, by symmetry, either, one of the H-orbits is in the northern hemisphere and one is in the southern hemisphere, or else, both are on the equator. Let us name the orbits as $\{q_0, .., q_4\}$ and $\{q'_0, .., q'_4\}$, where $q_i = x^i q_0$ and $q'_i = x^i q'_0$. (recall x is the generator of H)

Let $|x, y|$ denote the spherical distance between the points x and y on the unit sphere. We note that $d = |p, q_i|$ is independent of $i = 0, ..., 4$.

Doubt I Now the explanation that Artin provides here, is that $\exists\ h \in H$ s.t. $hq_0 = q_i$. I initially couldn't see how the result follows from this, but since H is just rotations along the polar axis, the spherical distance of a point from the pole remains unchanged, under the action of H.

The same argument can be used to prove $d' = |p, q_i'|$ will also be independent of i. Now the only two values $d = |p, p_i|$ can take are: 0, (say) d. Similarly the only two values $d' = |p, q_i'|$ will take would be: (say) d', π. So the values $|p, p'|$ where $p' \in V$ (the orbit), are $0, d, d', \pi$.

By the definition of d (that is the fact that the elements q_i were defined to be the ones between the equator and the north pole, or on the equator), $d \leqslant \pi/2$. Similarly we can say $d' \geqslant \pi/2$.

Now let's show that the orbit with 5 elements does NOT lie on the equator. For this, let's first note that the operation of G on V is transitive (simply because V was one of the orbits, so the conclusion follows from the definition of transitivity). This essentially means that we could've picked any p as the north, and $|p, p'|$ would've had the same 4 possible values. Now this implies, if we choose q_i as our north pole (but following the old notation), then $|q_i, q_{i+1}| = d$ (try visualizing to help your intuition). However, there are 5 poles in the orbit q_i so their angular separation can NOT be $= \pi/2$, for the sum of angles between them MUST add up to 2π (and not $5\pi/2$!). So this implies their angular separation, which we just showed equals d, must be $< \pi/2$ and hence, the poles do NOT lie on the equator.

Since $|p, q_i| = d = |q_i, q_{i+1}|$, the north pole p and points of the orbit q_i, q_{i+1} form equilateral triangles! Since all the triangles share a point p, their are five congruent triangles with a common vertex, forming the face of an Icosahedron.

Doubt I Artin concludes from the above that poles of the group, correspond to the vertices of an Icosahedron. However to me it seems incomplete since the relation between q and q' hasn't explicitly been derived, although calculation of d and d' (which can be easily computed) should be sufficient to show that the rest of the faces are also built off of the same equilateral triangles.

The images of the polygons used in this document were specifically created for this purpose.

3 MORE GROUP THEORY

July 8-12, 2012

July 8, 2012

3.1 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 $\rho_{(u',\alpha)}$.

3.2 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

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

3.2.1 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.

3.2.2 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)

3.2.3 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 15, 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>

3.2.4 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.

3.2.5 Lemma 7.5.5

1. For $n \geqslant 3$, A_n is generated by 3-cycles.
2. For $n \geqslant 5$, 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 $k \geqslant 3$ or a product of atleast two 2-cycles. Since numbering the indices doesn't change anything, we suppose $p = (\mathbf{1\,2\,3} \dots \mathbf{k}) \dots$ or $p = (\mathbf{1\,2})(\mathbf{3\,4}) \dots$. Now let $q = (\mathbf{3\,2\,1})$. Calculate qp and you'll see something startling. The product fixes the index $\mathbf{1}$. Why that works can be observed from the simple fact that whatever $\mathbf{1}$ is mapped to in p, gets mapped back to $\mathbf{1}$ in q. That simple!

Now for the second, more interesting part. Suppose $n \geqslant 5$. 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 $n \geqslant 5$. 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 $\in A_n$. □

3.2.6 Theorem 7.5.4

For every $n \geqslant 5$, 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> □

July 10, 2012

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

3.3.1 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 □

3.4 7.7 the sylow theorems

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

3.4.1 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.

3.4.2 The Theorems

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

3.4.2.1 Theorem 7.7.2 First Sylow Theorem

G contains a Sylow p-subgroup.

3.4.2.2 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.

3.4.2.3 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.

3.4.2.4 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. □

3.4.2.5 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. □

3.4.3 Proofs

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 1** 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

$$\begin{pmatrix} n \\ p^e \end{pmatrix} = \frac{n(n-1)\dots(n-k)\dots(n-p^e+1)}{p^e(p^e-1)\dots(p^e-k)\dots 1}$$

$N \not\equiv 0 \mod p$ 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?] □

July 12, 2012

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 $|G| = |\text{stabilizer}| \; |\text{orbit}|$. Now $|G| = p^e$ for some p and e. The order of an orbit must be a number and therefore $|\text{stabilizer}|$ would be a power of prime, and consequently, $|\text{orbit}|$ would be p^k for some $k \leqslant e$. So $|\text{orbit}|$ is either 1 or a multiple of p.
Using the next formula, we break the set S into orbits. We have

$$|S| = |O_1| + |O_2| + |O_3| + ...$$

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

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 $|G| = |H| \mid \text{number of cosets of } H \mid$
And by definition of $\mathcal{C}$, we have $\mid \text{number of cosets of } H \mid = |\mathcal{C}|$
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,

$$m = [G : H] = \frac{|G|}{|H|} \tag{16}$$

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.

$$|N(H)| \equiv 0 \mod |H| \tag{17}$$

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,

$$s = [G : N(G)] = \frac{|G|}{|N(H)|} \tag{18}$$

Using equations 16, 17 and 18, 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. □

3.5 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*.

3.5.1 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. $w_0 = w'_0$.

July 24 & 25, 2012

3.5.2 Proposition 7.9.3

Products of equivalent words are equivalent, viz. if $w\ w'$ and $v\ v'$ then $wv\ w'v'$.

Proof. Essentially, we just note that we can convert both w and w' to w_0, its reduced form. Similarly for v and v' we have v_0. Now to prove $wv\ w'v'$, we convert both to their reduced forms to obtain $w_0v_0\ w_0v_0$ which proves the statement. □

3.5.3 Definitions

for the proposition to follow:

(i) $S = a, b, c..$ is an arbitrary set of distinct symbols

(ii) $S' = a, a^{-1}, b, b^{-1}, c, c^{-1}, ..$ is the set consisting of symbols for every $a \in S$

(iii) W' be a the semigroup of words made by juxtaposition of symbols from S' and following the law of cancellation ($aa^{-1} = 1$).

3.5.4 Proposition 7.9.4

The set $\mathcal{F}$ of equivalence classes of words in W' is a group, with the law of composition induced from multiplication (juxtaposition) in W'.

Proof. Existence of identity and associativity of multiplication follows from W'. We just need to show the inverses exist. For any element $w \in \mathcal{F}$, the corresponding equivalent class (represented by the reduced form) would be expressable as the product $xy..z$ (arbitrary). The inverse of these would exist (by the definitions above) and thus the product $z^{-1}...y^{-1}x^{-1}$ would also exist. This is the inverse of w. Thus $\mathcal{F}$ is a group. □

3.6 **7.10 generators and relations**

3.6.1 Definition 7.10.1

A *relation* among elements $x_1, x_2, x_3 ... x_n$ of a group G is defined as a word r in the free group of the set $x_1, x_2 .... x_n$ that evaluates to 1 in G.

As an example, consider the dihedral group D_n, where x represents rotation by angle $2\pi/n$ and r represents a reflection about x-axis. Then from prior derivation, we know that (see page 164 of Artin's Text Second Edition) x and y will satisfy the following relations

$$x^n = 1, \; y^2 = 1, \; xyxy = 1$$

Using these relations, one can convert any given element of D_n into the form $x^i y^j$ where $0 \leqslant i < n$ and $0 \leqslant j < 2$. (Note the third relation is the same as $yx = x^{-1}y$). This means we can derive the multiplication table for D_n using these relations and thus these relations are also called *defining relations*.

Now it may not be simple to explicitly find the multiplication table, yet using the free group and a lemma, we will define a group generated by a given set of elements, with a given set of relations.

3.6.2 Lemma 7.10.3

Let R be a subset of a group G. We can always find a unique smallest normal subgroup N of F that contains R. N is called *the normal subgroup generated by* R.

Proof. A non-empty subset of a group is a normal subgroup if and only if it is closed under law of composition (in our convention multiplication), inversion and conjugation (with an element of the given group) & contains the identity element. [**Confusion** What does conjugate of an element of R' mean? **Clarification** Its grg^{-1} and not restricted to $r'rr'^{-1}$.] Thus we define N to consist of those elements of G which can be obtained from R using a finite sequence of multiplication, inversion and conjugation. Uniqueness and being smallest follow readily. □

Alternate Proof. We borrow the first statement from the previous proof. Let R' consist of r and r^{-1} for every r in R. An element of G is in N if it can be written as a product $y_1...y_b$ of arbitrary but finite length, where each y_ν is a conjugate of an element of R'. Showing N is closed under multiplication is trivial. A little thought suffices to see inverses also exist. We show that the group is closed under conjugation also. Consider an element in n in N. Now the group would be normal if gng^{-1} is also in N. Since n can be written as $y_1y_2...y_r$. Let it equal $g_{k_1}r_1g_{k_1}^{-1}\; g_{k_2}r_2g_{k_2}^{-1}\; ...g_{k_b}r_bg_{k_b}^{-1}$. Now gng^{-1} should also be in N. To prove this it would suffice to show that gng^{-1} can also be expressed as a product $y_1'y_2'$... for some arbitrary length (the symbol y_ν' also represents conjugate of an element or R', but its used to avoid collision of variables). So, we have

$$\begin{aligned} gng^{-1} &= g(\,g_{k_1}r_1g_{k_1}^{-1}\; g_{k_2}r_2g_{k_2}^{-1}\; ...g_{k_b}r_bg_{k_b}^{-1}\,)g^{-1} \\ &= (gg_{k_1}r_1g_{k_1}^{-1}g^{-1})\,(gg_{k_2}r_2g_{k_2}^{-1}g^{-1})\,...(gg_{k_b}r_bg_{k_b}^{-1}g^{-1}) \\ &= y_1'y_2'...y_b' \end{aligned}$$

where $y_\nu' = gy_\nu g^{-1} = gg_{k_\nu}r_\nu g_{k_\nu}^{-1}g^{-1} = (gg_{k_\nu})\,r_\nu\,(gg_{k_\nu})^{-1}$. This proves that N is closed under conjugation as well, and that in turn completes the proof. □

The empty set generates the trivial subgroup {1}.

3.6.3 Definition 7.10.4

Let $\mathcal{F}$ be the free group on the set $S = \{x_1, ...x_n\}$ and let $R = \{r_1, ...r_k\}$. Let $\mathcal{R}$ be the normal subgroup generated by R. Now the group generated by the set S with the relations given by R is the quotient group $\mathcal{G} = \mathcal{F}/\mathcal{R}$.

The definition will seem natural upon realization of the fact that any element $r \in \mathcal{R}$ is mapped to the coset representing the identity element of $\mathcal{G}$. Also, a coset remains unchanged on multiplication with r. (Quick proof: Let $j\mathcal{R}$ be a coset. $rj\mathcal{R} = r\mathcal{R}j = \mathcal{R}j = j\mathcal{R}$.)

The group $\mathcal{G}$ is also denoted by

$$< x_1, ..., x_n | r_1, ...x_k >$$

July 26 & 27, 2012

3.6.4 Example 7.10.7

(This is given quite clearly in the text) Let T be the tetrahedral group (the group of symmetries of the tetrahedron), and let x and y denote rotations by $2\pi/3$ about the center of a face and about a vertex respectively. Let z be rotation by π about the center of an edge. Look at the text and the following relations will appear to hold naturally.

$$x^3 = 1,\ y^3 = 1,\ z^2 = 1,\ xyz = 1$$

Now following Artin, two questions arise.

1. Are these the defining relations for the group T? Which is the same as asking, is the group

   $$< x, y, z | x^3 = 1,\ y^3 = 1,\ z^2 = 1,\ xyz = 1 >$$

   isomorphic to the group T?

   The answer's yes according to the text. We'll find out how in the next section.

2. (**Doubt** I don't understand the *precise* meaning of the question) How can one compute in a group $\mathcal{G} =< x_1, ...x_n | r_1, ...r_k >$ that's represented by generators and relations?

   Given the elements $x_1, ...x_n$, its simple to find the free group $\mathcal{F}$. Issue is to determine which element w will represent identity in $\mathcal{G}$. As mentioned before, this will happen if and only if w is in the normal subgroup $\mathcal{R}$. This apparently is known as the *word problem* for $\mathcal{G}$. If the word problem can be solved, then we can decide when two elements of the free group represent equal elements of $\mathcal{G}$. To understand how, consider this; If $w_1 = w_2$ in $\mathcal{G}$, then its the same as saying $w_1 w_2^{-1} = 1$ in $\mathcal{G}$. Now we know the only elements of $\mathcal{F}$ that represent identity in $\mathcal{G}$ are those that belong to $\mathcal{R}$, thus $w_1 w_2^{-1}$ must belong to $\mathcal{R}$. Since we can solve the word problem, we already know which elements are in $\mathcal{R}$. We just need to separate them into the product of two elements, say $w_a w_b^{-1}$ and we'll know then that $w_a = w_b$ in $\mathcal{G}$.

   When can or can't the word problem be solved, is according to the text, a question that requires more work to answer. It does assert however, that it can be solved in any finite group.

3.6.5 Example 7.10.11

This is very elementary to follow from the text, yet it is fairly clever and interesting. I am not redoing this here, since I understood it clearly in the first go.

Before we can answer the first question, we must describe certain mapping properties. For that we first discuss the naming conventions that we'll use henceforth (this also is fairly elementary).

There's a canonical homomorphism from $\mathcal{F}$ to $\mathcal{G}$, as with any quotient group, defined by π as follows

$$\pi : \mathcal{F} \to \mathcal{F}/\mathcal{R} = \mathcal{G}$$

which sends w of $\mathcal{F}$ to the coset $\overline{w} = [w\mathcal{R}]$. The kernel of the homomorphism is of course $\mathcal{R}$ (if its not obvious, revise section 2.12). According to the convention we've followed earlier, an overline like $\overline{w}$, represents the coset as an element, and thus the element belongs to $\mathcal{G}$, whereas w by itself belongs to $\mathcal{F}$. However, this distinction is dissolved and we simply remember that w_1 and w_2 of $\mathcal{F}$ are equal in $\mathcal{G}$, if $w_1 w_2^{-1}$ is in $\mathcal{R}$ (as mentioned earlier). So let's start.

3.6.6 Proposition 7.10.12 *Mapping Property of the Free Group*

Let $\mathcal{F}$ be the free group on a set $S = \{x_1, x_2, ...\}$, and let G be a group. Any map of sets $f : S \to G$ extends in a unique way to a group homomorphism $\varphi : \mathcal{F} \to G$. If we denote the image $f(x)$ of an element x of S by $\underline{x}$, then φ sends a word in $S' = \{x_1, x_1^{-1}, x_2, x_2^{-1}, ...\}$ to the corresponding product of the elements $\{\underline{x}_1, \underline{x}_1^{-1}, \underline{x}_2, \underline{x}_2^{-1}, ...\}$ in G.

This is rather trivial but hinges (as pointed out in Artin) on the fact that the free group doesn't satisfy any other relation than those implied by the group axioms.

3.6.7 Proposition 7.10.13 *Mapping Property of Quotient Groups*

Let $\varphi : G' \to G$ be a group homomorphism with kernel K, and let N be a normal subgroup of G' that is contained in K. Let $\overline{G}' = G'/N$, and let $\pi : G' \to \overline{G}'$ be the canonical map $a \rightsquigarrow \overline{a}$. The rule $\overline{\varphi}(\overline{a}) = \varphi(a)$ defines a homomorphism $\overline{\varphi} : \overline{G}' \to G$, and $\overline{\varphi}.\pi = \varphi$.

Proof. First things first, the motivation for the definition of the map $\overline{\varphi}(\overline{a}) = \varphi(a)$. So let $a' = an$ for some $n \in N$, essentially just some element in the coset represented by $\overline{a}$. We define a new map, $\overline{\varphi}'(\overline{a}) = \varphi(a') = \varphi(an) = \varphi(a)\varphi(n) = \varphi(a)(= \overline{\varphi}(a)$ by definition).

That justifies the definition.
Proving $\overline{\varphi}$ is a homomorphism, is now simple.

$$\begin{aligned}\overline{\varphi}(\overline{a}\overline{b}) &= \varphi(ab) && \text{(definition)}\\ &= \varphi(a)\varphi(b) && (\varphi \text{ is a homomorphism})\\ &= \overline{\varphi}(\overline{a})\overline{\varphi}(\overline{b}) && \text{(definition)}\end{aligned}$$

Let's now prove that $\overline{\varphi}.\pi = \varphi$. Assume an arbitrary element $g' \in G'$. The map π will send g' to $\overline{g}'$ representing the coset $g'N$. Now the map $\overline{\varphi}$ will send $\overline{g}'$ to $\varphi(g')$, which is precisely the map φ.
Note: The proof requires the group N to be normal for else $\overline{G}'$ would not be a group and thus π would cease to be a group homomorphism and everything falls apart. □

Corollary 7.10.14

(1) There's a canonical homomorphism $\psi : \mathcal{G} \to G$ that sends $x_i \rightsquigarrow x_i$ | **Doubt** (in "..sends $x_i \rightsquigarrow x_i$"): So much so, that this seems incorrect to me!

(2) ψ is surjective if and only if the set S generates G.

(3) ψ is injective if and only if every relation among the elements of S is in $\mathcal{R}$.

Proof. This section is driven by intuition yet Artin wasn't clear enough for me.
Let's start with the set S' that generates G, in accordance with the prior discussion. Let f be a map from S' to G, viz. $f : S' \to G$. From Proposition 7.10.12, we know that $\exists$ a map $\varphi : \mathcal{F} \to G$. We already know that all relations r_i in R evaluate to identity in G. So R is in the kernel of φ. Also, the kernel is a normal subgroup of G, and hence $\mathcal{R}$ must be contained in the kernel.
That motivates us to talk about the quotient group $\mathcal{G} = \mathcal{F}/\mathcal{R}$. From proposition 7.10.13, we know $\exists$ a homomorphism $\overline{\varphi}$ from $\mathcal{G}$ to G.
(This part has a little repetition, however that's necessary for the discussion as you'll soon discover) All relations r_i in $\mathcal{F}$ (strictly speaking, by relation r_i in $\mathcal{F}$ I mean the equivalence class corresponding to the reduced word of the relation, in $\mathcal{F}$), are mapped to the identity element $\mathcal{G}$ since its the quotient group $\mathcal{F}/\mathcal{R}$. Further, since $\overline{\varphi}$ is a homomorphism, it maps identity to identity. Now the elements in $\mathcal{F}$ that are not in $\mathcal{R}$ but belong to the kernel of φ, will be mapped to their corresponding cosets in $\mathcal{G}$. So let g_{kernel} be such an element in $\mathcal{F}$, then it is sent to its coset $g_{\text{kernel}}N$ in $\mathcal{F}$. Then it becomes quite natural to imagine what would happen if there weren't any such g_{kernel}, viz. kernel of $\overline{\varphi} = \{1\}$. Thus the map would be injective! (read Chapter 2 again if it doesn't sound obvious). So that proves part (3), since the only way kernel of $\overline{\varphi} = \{1\}$ is if all relations are included in $\mathcal{R}$.
Part (3) is obvious because if all symbols used in G are included in S,

then they will also exist in $\mathcal{G}$ (excluding those that are identity in $\mathcal{G}$, but they, obviously, wouldn't be present in G either) and thus there would always be atleast one pre-image associated with every element of G, in $\mathcal{G}$. □

3.7 7.11 the todd-coxter algorithm

This seemed like the most fascinating part of the chapter when I started and now I'm finally here! So I'll start with describing the requirement for application of the Algorithm, which essentially is, and I quote Artin, "an amazing method for determining the operation of a finite group G on the set of cosets of a subgroup H.".
Motivation for the algorithm will become clear as we proceed. So here's what we need to know explicitly (This part again is given quite clearly in Artin, but its re-iterated for clarity & maintaining readability); both G and H. G is given as in the previous section in terms of generators & relations.

$$G \quad = \quad < x_1, \dots, x_m | r_1, \dots, r_k >$$

H is given explicitly by a set of words in the free group $\mathcal{F}$, whose images in G generate the subgroup, as

$$\{h_1, \dots, h_s\}$$

Recall the fact that composition of permutations is read opposite to the way a permutation itself is read. To fix this issue (which will improve readability of the tables used by the algorithm to compute), we define the operation of G on the set of cosets of H by *right multiplication*, viz. right cosets. Thus now we read a permutation like so.

$$\begin{array}{ccccc} \text{first do this} & & \text{then this} & & \\ (234) & . & (123) & = (12)(34) \end{array}$$

It's now time to define a set of mysterious rules (I'll omit the examples as they are very clear in Artin) that suffice for determining the operation of G on the right cosets.

3.7.1 Rules 7.11.3

1. The operation of each generator is a permutation.

2. The relations operate trivially: they fix every coset.

3. The generators of H fix the coset [H].

4. The operation is transitive.

Let's figure why these must hold. We begin with the first.

Proof. The generators, following form the discussion are, $< x_1, \ldots, x_m >$. Let C be an arbitrary coset, represented by cH, where $c \in G$. Now if we operate the coset with any of the generators, say x_n with $n \leqslant m$, we get $x_m cH$. Now since G is a group, and both x_m and $c \in G$, $x_m c = c'(\text{say}) \in G$. So cH is sent to the coset $c'H = x_m cH$. We can now define a bijective map from the set of cosets to itself (since the coset C is arbitrary), viz. show that the operation is a permutation. The map is multiplication by x_m and its bijective because its inverse is multiplication by x_m^{-1}. □

Second is obvious, since relations evaluate to identity in G.
Third is also obvious, for the coset $[H] = h$ s.t. $h \in H$. Multiplication by generator of H with any such h still means $h \in H$.
Fourth is again obvious, because if we fix a coset, say [H], and operate it with all elements in G, we will generate the set of all cosets. That creates one orbit. To show that there's only one orbit, we simply observe the fact that operating by any element $g \in G$ with an arbitrary coset cH where $c \in G$, we get gcH and by definition of a group, $gc \in G$, thus the new coset belongs to the same orbit.

COLOPHON

This document was typeset using the typographical look-and-feel `classicthesis` developed by André Miede, for LaTeX.
The style was inspired by Robert Bringhurst's seminal book on typography "*The Elements of Typographic Style*".

The latest version of this document is available online at:

https://github.com/toAtulArora/IISER_repo