Contents

Chapter 1

Using different page styles

Algebra is generous; she often gives more than is asked of her.Jean d'Alembert

1. Burnside's Lemma

The problem we attempt to solve in this section is the following:
We want to create a necklace, that consists of n beads. Each bead can be one of two different colors. How many such necklaces can we create.
Note that we want to only consider unique necklaces. For example, there is only necklace with $n-1$ black beads and one red bead, not n different necklaces, and so on.

Definition 1.1. The **action** of a group G on a set X is a map with particular properties. Specifically, it is $\phi : G \times X \to X$ that satisfies:

- Identity: $\phi(e, x) = x$ where $x \in X$ and e is the identity of G.
- Compatability: $\phi(g, \phi(h, x)) = \phi(gh, x)$.

This is where the very famous Rubik's Cube example of groups fits. The set of all possible states of the Rubik's cube is the set X, and the set of cube moves is the group G.
Another example of group action is one we have already seen, S_n, the group of permutation actions of a finite set. Here, the set of all permutations is the set X, and the set of permuation actions is the group.
A similar group is the Dihedral Group of regular polygons, D_n. It is the group of symmetries of a regular polygon. It consists of rotational symmetries and reflection symmetries.
Going back to our necklace problem, consider a set of 2^n possible necklaces. We get this number 2^n by considering two choices of colours for each of the n beads.
Define an equivalence relation on this set as follows: cRc' if there is an element of D_n that changes c to c'. The problem of counting the number of necklaces is basically counting the number of such equivalence classes. We call each such equivalence class an **orbit**. The trouble arises since each class is of a different size. Burnside's Lemma gives us a solution to this problem.

Lemma 1.0.1. Let G be a finite group that acts on X. The number of orbits, denoted $|X/G|$ is given by

$$|X/G| = \frac{1}{|G|}\Sigma_{g\in G}|X^g|$$

where for a particular g, X^g is the subset of X that is unchanged by g. For example, $X^e = X$, since the identity leaves every element unchanged.

Proof. The first step we take, is given $x \in X$, to try and find the size of the orbit that x belongs to. Consider the set $G_x = \{gx = x | g \in G\}$. In other words, this is the set of actions that does not change x. This is called the stabilizer of x. This set is a subgroup (proof left as an exercise). Therefore, we can quotient G by G_x to form a quotient group. Consider each element of this quotient group, G/G_x. This element is a set of actions that all map x to the same element, x'. Thus, the number of elements in the orbit of x is simply the size of the group G/G_x, which is $\frac{|G|}{|G_x|}$ by Lagrange theorem, and is denoted by $|G.x|$.
Consider now the sum $\Sigma_{g \in G}|X^g|$. This is simply the cardinality of the set $\{(g,x)|gx = x, g \in G, x \in X\}$ and can thus be equivalently written as a sum over the elements of X. This gives us $\Sigma_{g \in G}|X^g| = \Sigma_{x \in X}|G.x|$.
Substituting, we get $\Sigma_{g \in G}|X^g| = |G|\Sigma_{x \in X}\frac{1}{|G.x|}$. We now use the fact that X is a disjoint union of all its orbits. The sum over X can be reduced as a double summation, one over all the orbits, and an inner summation over all the elements of each orbit. Further, the sum $\Sigma_{x \in A}\frac{1}{|G.x|}$ where A is an orbit is clearly 1, since by definition the orbit contains $|G.x|$ elements, which is same for all $x \in A$. Thus, we get that the summation $\Sigma_{g \in G}|X^g| = |G|\Sigma_{x \in X}\frac{1}{|G.x|} = |G||X/G|$, which completes the proof. □

2. Algebraic Geometry

Algebraic Geometry is the application of abstract algebra to solve geometric problems. The problem we attempt to solve in this section is to find a proof of the following:

Theorem 1.1. Pascal's theorem: The meets of opposite sides of a hexagon inscribed in a conic are collinear.

In other words, if we find the three points of intersections of opposite sides of the hexagon that is inscribed on any conic section, these points will be collinear. In the next section, we set up a mapping between algebra and geometry, and prove the above
theorem in the section after that.

2.1 Mapping

Consider the set $\mathbb{C}^2$ and the set $\mathbb{C}[x,y]$. We build a correspondence between the two.
For **points** in $\mathbb{C}^2$, we have $p = (\alpha, \beta)$. In $\mathbb{C}[x,y]$ we can map this to the set of all curves that vanish at p. Let I be the set of all polynomials $A(x,y)$ such that $A(p) = 0$.

Lemma 1.1.1. I is a maximal ideal of $\mathbb{C}[x,y]$.

Proof. Let $I \subsetneq J$. Then $B_\circ(x,y) \in J$ such that $B_\circ(p) \neq 0$. Let $S_J = \{\widehat{p} \in \mathbb{C}^2 | B(\widehat{p}) = 0, \forall B \in J\}$. We know that $x - \alpha$ and $y - \beta$ both belong to J, since they vanish at p. Therefore, the only point S_J can contain, if at all, is p. However, $B_\circ$ does not vanish at p. Therefore, $S_J = \phi$.
We now state without proof and use a theorem that fundamentally establishes the relationship between algebra and geometry.

Theorem 1.2. Hilbert's Nullstellensatz. Let I be an ideal of $\mathbb{C}[x,y]$. Let S_I be the locus of curves in I. Let $B(x,y)$ be a curve that passes through all the points in S_I. Then $B^m \in I$ for some $m \geq 1$. If $S_I = \phi$, then $m = 1$.

Continuing with the proof of lemma

Lemma 1.2.1. Every maximal ideal has a single point as its locus.

Proof. Assume that the locus had two or more points. We could then add to the ideal all the curves that pass through one of the two points, and get a bigger ideal.
Assume that the locus had no points. Then, by Nullstellensatz, the ideal is the whole ring. □

Further, the ideal of all curves that pass through the point p is generated by $(x-\alpha)$ and $(y-\beta)$. Now that we have a mapping for points, we move on to **curves**. A good first guess is that curves $A(x,y)$ map to ideals generated by $A(x,y),(A(x,y))$. We try and prove this.

Proof. Consider $I_A = \{B(x,y)|B(p)=0, p \in S_A\}, S_A = \{p|A(p)=0\}$. In other words, I_A is the ideal of all curves that are zero at all points along the curve $A(x,y)$.
By definition, $(A(x,y)) \subseteq I_A$. We now need to show that $I_A \subseteq (A(x,y))$ to show that $I_A = (A(x,y))$.
Applying the Nullstellensatz: We have $I = (A(x,y)), S_I = S_A$ and the set of all $B(x,y) = I_A$. Thus, a power of every element of I_A is in $(A(x,y))$. If A is irreducible, then if $B_1 \times B_2 \in (A)$, then $A|B_1 \times B_2 \Rightarrow A|B_1$ or $A|B_2 \Rightarrow B_1 \in (A)$ or $B_2 \in (A)$. In way, if $B^m \in (A(x,y)), B \in (A(x,y))$. □

The above gives that if irreducible curves map to prime ideals.
Further, consider **functions defined on the curve** $A(x,y)$. They can be mapped to $\mathbb{C}[x,y]/(A(x,y))$. This is called the coordinate ring of $A(x,y)$ and is represented by $\mathrm{T}(A)$.
Finally, **rational functions defined on the curve** $A(x,y)$ can be mapped to $A(\mathbb{C})$, the field of fractions of $\mathrm{T}(A)$. This is called the functional field of $A(x,y)$.

Theorem 1.3. Coordinate rings are Dedekind domains.

Proof. Let I be an ideal of $\mathrm{T}(A)$. Elements of I are of the type $p(x,y)+(A(x,y))$. Maximal ideals still correspond to points. Therefore, every $(B(x,y)) \in \mathrm{T}(A), B \neq 0$, can be written uniquely as a product of prime ideals. □

Armed with this, we move on to the proof of the Pascal's Theorem.

2.2 Proof of Pascal's Theorem

Let $F(x,y)$ be a conic, so $deg(F)=2$. Consider the hexagon inscribed on the conic. Let its lines, in sequence, be l_1,l_2,l_3,l_4,l_5,l_6. Let $G = l_1l_3l_5$ and $H = l_2l_4l_6$. Then $deg(G) = deg(H) = 3$. Let $R = \mathbb{C}[x,y]/(F,g) = \mathrm{T}(F)/G$. F and G intersect at exactly six points, therefore $\mathbb{C}[x,y]/(F,G)$ is the function defined exactly on those six points.

Lemma 1.3.1. $R \cong \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C}$

We have $H \in R$. In particular, $H = (0,0,0,0,0,0)$.
Therefore, $H \in (F,G) \Rightarrow H = AF + BG$ for $A, B \in \mathbb{C}[x,y]$. H, G have degree three, and F has degree two. Lets say $deg(A) = d$. Then $deg(B) = d-1$, since we need the high order terms to cancel.
Let A_d be the degree d term of A and B_{d-1} the degree $d-1$ term of B. Define F_2, F_1, G_3 similarly. The highest degree term on the RHS, $A_dF_2 + B_{d-1}G_3 = 0$. Assuming that the lines of G are not tangent to F or intersect F only at infinity, it follows that $gcd(F_2, G_3) = 1$. Therefore, $B_{d-1} = cF_2$ and $A_d = -cG_3$. So $H = AF + BG + cGF - cGF = (A+cG)F + (B-cF)G$. We have written H as a linear combination with different coefficients. These two coefficients have degree one less than the previous. This way, we keep reducing the degree till $H = \widehat{A}F + \widehat{B}G$, where $\widehat{A}, \widehat{B}$ have degrees one and zero respectively.
H and G intersect at nine points, six on the conic and three more on the intersections of the opposite sides of the hexagon, outside the conic(the very same three points we want to prove are collinear). On each of the three outside points, $H = 0, G = 0$, but F is clearly non-zero. This is only possible if $\widehat{A} = 0$ on all these three points. However, since $\widehat{A}$ has degree one by construction, $\widehat{A}$ is a line that passes through all those three points.
This completes the proof.