Intersection Theory in Algebraic Geometry and Applications: An Introductory Series

Adam B Block

13 July 2018

This three part series will focus on the basics of intersection theory in algebraic geometry. An emphasis will be placed on developing intuition and application as opposed to the technical, rigorous proofs that are somewhat beyond the scope of a few short lectures. The interested reader is referred to [Fula, Fulb, EH] for more detail. In particular, due to the time constraints, critical parts of the theory have been left out, most especially the theory of characteristic classes of vector bundles. Due to the level of the audience, we restrict our focus to varieties and as such, a working knowledge of [Har, Chapter 1] should suffice for most of the series. Occasionally, more advanced concepts are required, especially for the proofs, but they can all found in [Har]. In the sequel, we assume that all varieties are smooth.

1 An Introduction

Intersection theory, tautologically, is the study of intersections. The theory has a long history, laid out in great detail in [Fulb, Chapter 1]. Much of the modern theory was developed by Fulton in [Fula], which remains the standard reference text. Many of the ideas come from algebraic topology, especially regarding characteristic classes. The Chow ring, in particular, can be thought of as being given by cellular cohomology. In this first section, we introduce the basics of the theory and give some combinatorial applications.

1.1 Basic Definitions

We fix a variety X, over some field k.

Definition 1. A k-cycle is a finite, formal sum $\sum a_i[V_i]$ where $V_i \subset X_i$ are k-dimensional subvarieties. This forms an abelian group, Z_kX. Given a $(k+1)$-dimensional subvariety $W \subset X$, and a rational function $r \in K(W)^\times$, we define

$$\operatorname{div} r = \sum_{V \subset W} \operatorname{ord}_V(r)[V] \in Z_kX$$

if A is the ring of integers in $\mathcal{O}_{V,W}$ then $\operatorname{ord}_V r = \ell_A(A/(r))$. We say that a divisor is rationally equivalent to 0 if it is the sum of these $\operatorname{div} r$. The group $\operatorname{Rat}_k X \subset Z_kX$ is the subgroup of those divisors rationally equivalent to 0. We define the Chow group $A_kX = Z_kX/\operatorname{Rat}_k X$.

Remark 2. Note that in the cases that we are considering, we have a better notion of order than in the above definition. We have that $\mathcal{O}_{V,W}$ is a just $\mathcal{O}_V$ locally localized by the ideal defining W, but $\operatorname{codim}(W, V) = 1$ and we may take W a regular embedding, so $\mathcal{O}_{V,W}$ is valuation ring, with valuation given by some uniformizer π. Thus we have that $\operatorname{ord}_V(r)$ can be taken to be the π-valuation of r.

We may think of the elements of Z_kX as cells in some cellular decomposition of X as a CW-complex if $X/\mathbb{C}$. Then we may think of $\operatorname{Rat}_k X$ as the image of the boundary map in cellular homology. Thus we may consider A_*X as the homology groups of our variety if $X/\mathbb{C}$. In fact, we see many of the same functorial properties. For instance, it follows immediately from the definitions that

$$A_*(\coprod X_i) = \bigoplus A_*X_i$$

Clearly, however, we have greater generality, as there is not an obviously similar notion for char $k > 0$ without more advanced notions.

Remark 3. Note that from the above definitions, we see that if $\dim X = n$ then $A_n X = Z_n X$. We are taking X to be a variety, so we have that $Z_n X = \mathbb{Z} \cdot [X]$. It is also immediate that $A_{n-1} X = \operatorname{Pic} X$. Lower Chow groups are often much harder to characterize.

Now that we have a group, we might wonder about how these Chow groups interact with morphisms. For general morphisms, there is little that we can see, but, as we shall see, there are certain classes of morphisms that induce morhpisms on Chow groups, too.

Let $f : X \to Y$ be a morphism and let $V \subset X$ be a subvariety, with $W = f(V) \subset Y$. We then have $\dim W \leq \dim V$ and a natural inclusion $K(W) \subset K(V)$. If $\dim V = \dim W$, we know that $K(V)/K(W)$ is finite (see [Har]). Thus, let us define

$$\deg(V/W) = \begin{cases} [K(V) : K(W)] & \dim V = \dim W \\ 0 & \dim V > \dim W \end{cases}$$

We then define the following map:

Definition 4. Let $f : X \to Y$ a morphism of varieties. We define $f_* : Z_k X \to Z_k Y$ by $f_*[V] = \deg(V/W)[W]$ and extending linearly.

Note that this morphism is clearly functorial by the degree formula for field extensions, i.e., $(fg)_* = f_* g_*$. In fact, we see that if $X/\mathbb{C}$ then this map is just homological pushforward. We might hope that this map defines a map on the Chow group, but unfortunately this is not always the case. We do have, however,

Proposition 5. *Let $f : X \to Y$ be a finite, proper map and let $\alpha \in \operatorname{Rat}_k X$. Then $f_* \alpha \in \operatorname{Rat}_k Y$. Thus, $f_* : A_* X \to A_* Y$ is a well defined morphism.*

Proof. The proposition follows from the following claim. Given f, X, Y as in the statement, let $r \in K(X)^\times$. Then

$$f_*[\operatorname{div} r] = \begin{cases} 0 & \dim Y < \dim X \\ [\operatorname{div} \operatorname{Nm}(r)] & \dim Y = \dim X \end{cases}$$

where $\operatorname{Nm} r$ is the field norm.

Note that the first case follows from the definition. We prove the second case. Let $L_1 = K(X)$ and let $L_2 = K(Y)$ and let $W \subset Y$ be a subvariety of codiension 1. Let $A = \mathcal{O}_{W,Y}$ and $\mathcal{I}$ the ideal sheaf cutting out W. We wish to consider those subvarieties $V_i \subset X$ mapping to W. Because they are the same dimension, their structure sheaves will be finite over A. We wish to find some B such that the field of fractions of B is L_1, $B \otimes_A L_2 = L_1$, and the subvarieties $V_i \to W$ correspond to maximal ideals $\mathfrak{m}_i \subset B$. We may do this locally, so suppose $X = \operatorname{Spec} R$, $Y = \operatorname{Spec} S$ and let $A = S_{\mathcal{I}(W)}$ and $B = R \otimes A$. Now, it suffices to show the following identity:

$$\sum_i [K(V_i) : K(W)] \cdot \operatorname{ord}_{V_i} = \operatorname{ord}_W(\operatorname{Nm} r)$$

Because ord., Nm are homomorphisms, we may take $r \in B$. This then follows from some commutative algebra. Letting $\varphi : M \to M$ be a map for some A-module M, we define $e_A(M) = \ell_A(\operatorname{Coker} \varphi) - \ell_A(\ker \varphi)$. If $A \to B$ is a local morphism such that $[\kappa(A) : \kappa(B)] = d$ then we have the following well known identities:

$$e_A(\varphi) = \sum_{\mathfrak{p} \subset A} e_{A_\mathfrak{p}}(\varphi_\mathfrak{p})$$
$$e_A(\varphi) = d \cdot e_B(\widetilde{\varphi})$$

Let φ denote multiplication by r. j Then combining the two identities gives us that the left hand side above is $e_A(\operatorname{Coker} \varphi)$, but because we are working with varieties, r cannot be a zerodivisor so has trivial kernel. Thus we need $\ell_A(\operatorname{Coker} \varphi) = \operatorname{ord}_W \operatorname{Nm} \varphi = \operatorname{ord}_W \det \widetilde{\varphi}$, where $\widetilde{\varphi}$ is the induced morphism. This then follows from elementary commutative algebra. See [Fula] for details. ■

Remark 6. Note that Proposition 5 applies without the finite hypothesis, but the proof is a little bit harder. See [Fula] for details.

Example 7. We will do the computation above explicitly in the case where $Y = \operatorname{Spec} k$ and $X = \mathbb{P}^1_k$. Then we have that $K(X) = k(t)$ with $t = \frac{x_1}{x_0}$. We know that $\operatorname{ord} : K(X)^\times \to \mathbb{Z}$ is a homomorphism so we may assume that r is an irreducible polynomial of degree d in $k[t]$. Then r gives us a prime ideal $\mathfrak{p}$ and $\operatorname{ord}_\mathfrak{p} r = 1$. Letting $s = \frac{1}{t}$ we have $s^d r \in \mathcal{O}^\times_{P_\infty}$ so we have $\operatorname{ord}_\infty = -d$. Because r is irreducible, we have that for all other points $\operatorname{ord}_{P'} r = 0$. Thus we have $\operatorname{div} r = [\mathfrak{p}] - d \cdot [\infty]$. Now we know that $[K(P_\mathfrak{p}) : k] = d$ and $[K(\infty) : k] = 1$ so $f_* \operatorname{div} r = d \cdot [Y] - d \cdot [Y] = 0$.

Note that if k is a field then $A_* \operatorname{Spec} k \cong \mathbb{Z}$. This leads us to the following definition:

Definition 8. Let X be a complete (proper over k) variety with structure morphism $p : X \to \operatorname{Spec} k$. Let $\alpha \in A_0 X$; we define the degree $\deg \alpha = p_* \alpha$. We extend this to higher degrees by 0, i.e., $\deg \alpha = 0$ if $\alpha \in A_k X$ and $k > 0$.

This concept immediately yields a classical result in intersection theory:

Theorem 9 (Bezout)**.** *Let $C_1, C_2 \subset \mathbb{P}^2$ be general curves of degrees d_1, d_2 over $k = \overline{k}$. Counting with multiplicity, they intersect in $d_1 d_2$ points.*

Proof. We may assume that C_1 is irreducible. Otherwise, we may add the points of intersection with each irreducible factor, counting with multiplicity. Let $C_i = V(F_i)$. If G, G' are polynomials both of degree d then $\frac{G}{G'} = r \in K(C_1)^\times$ and $[C_1 \cap V(G)] - [C_1 \cap V(G')] = [\operatorname{div} r] = 0$ in the Chow group. Thus we may assume that C_2 is just d_2 lines and so it suffices to consider the case where C_2 is one line. But $\#\{C_1 \cap L\} = d_1$ by the fact that $k = \overline{k}$. ■

While our definition of rational equivalence emphasizes the connection with homology, we might choose another definition, perhaps more in the flavor of algebraic geometry. Consider a variety X and consider

$$\begin{tikzcd} X \times \mathbb{P}^1 \arrow[r, "p_2"] \arrow[d, "p_1"] & \mathbb{P}^1 \\ X & \end{tikzcd}$$

Let $V \subset X \times \mathbb{P}^1$ such that $p_2|_V$ is dominant (has dense image). If $p \in \mathbb{P}^1$, define $V(p)$ to be $f^{-1}(p) \subset X \times \{p\}$ the scheme-theoretic fiber. The map p_1 is proper ([Har, II.4.8]) and we have $p_*[V(p)] \in Z_k X$. Now, $f : V \to \mathbb{P}^1$ given by p_2 gives a rational function $f \in K(V)^\times$ and we have $[\operatorname{div} f] = [f^{-1}(0)] - [f^{-1}(\infty)]$. Thus we have $p_*[\operatorname{div} f] = [V(0)] - [V(\infty)]$. The upshot of this is the following proposition:

Proposition 10. *Let X be a variety over k and let $\alpha \in Z_k X$. Then $\alpha \in \operatorname{Rat}_k X$ if and only if there exist $(k+1)$-dimensional subvarieties $V_i \subset X \times \mathbb{P}^1$ that project dominantly to $\mathbb{P}^1$ such that*

$$\alpha = \sum_i [V_i(0)] - [V_i(\infty)]$$

Proof. One way follows immediately from the above remarks. For the other, it suffices to suppose that $\alpha = \operatorname{div} r$ for $r \in K(W)^\times$. Then r defines a rational map $W \to \mathbb{P}^1$ and letting $\Gamma_r = \{(u, r(u)) \in X \times \mathbb{P}^1\}$ the graph of the map, we let $V = \overline{\Gamma}_r$. From the remarks above, it is clear that $\operatorname{div} r = [V(0)] - [V(\infty)]$. ■

Remark 11. Some people would quote Proposition 10 as the original definition. In fact, it is very useful to form intuition into the idea of 'moving' that is so important in classical intersection theory. The role of $\mathbb{P}^1$ can be though of as the role of the unit interval in a homotopy, so, morally, rational equivalence in nice cases can be though of a homotopic deformation. This is especially important in the context of the original definition of the intersection product, where, instead of the definition below, the idea was to move a variety until one had two varieties that intersected generically transversely. See Figure 1 for a visual illustration of the concept. See Example 12 for an application of this definition.

Example 12. We will use the definition of rational equivalence provided by Proposition 10 to show that the Chow groups of $\mathbb{A}^n$ vanish for $k < n$ over algebraically closed fields. Note that the conclusion holds for all fields (as we prove in Proposition 17) Let $Y \subset \mathbb{A}^n$ be a proper subvariety and thus there exists some point

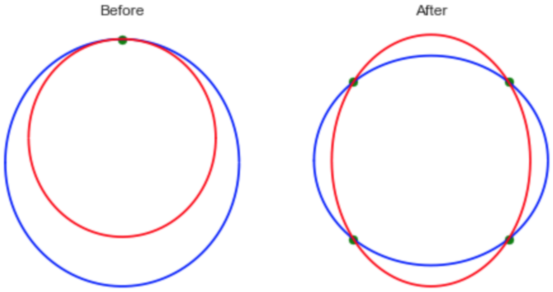

Figure 1: In the left hand side the two curves do not meet transversely. On the right the inner circle has been moved so that they do.

that is not in Y. Without loss of generality, we can choose coordinates $z_1, \ldots, z_n$ such that the origin is not on Y. Let

$$W^o = \{(t, tz) \subset (\mathbb{A}^1 \setminus \{0\}) \times \mathbb{A}^n | z \in Y\} = V(\{f(\frac{z}{t}) | f(z) \text{ vanishes on } Y\})$$

Then it is clear that $W^o_t = t \cdot Y$. Let $W = \overline{W^o} \subset \mathbb{P}^1 \times \mathbb{A}^n$. Because W^o is irreducible we know that W is irreducible. Moreover, the fiber over 1 of W is just Y by the Nullstellensatz, and the fiber over ∞ is empty, so $Y \sim 0$.

This may seem complicated, but it helps in proving that the following concept is well-defined. Let $f : X \to Y$ be a morphism. We have already seen that this induced $f_* : A_*X \to A_*Y$, but a natural next question is whether there is a pullback map, $f^* : A_*Y \to A_*X$. Just as in the case of pushforwards, we will restrict to a certain class of maps. Let $f : X \to Y$ be a flat map of relative dimension n. Then we define for $V \in A_kY$, $f^*[V] = [f^{-1}(V)] \in A_{k+n}X$. We moreover have functoriality, $(fg)^* = g^*f^*$.

Remark 13. Technically speaking, we need to verify that if $Z \subset Y$ is a subscheme, rather than a subvariety, that $f^*[Z] = [f^{-1}(Z)]$ if f is flat, but we will ignore this technicality. The interested reader is referred to [Fula].

As in the case of proper pushforward, this map descends to the Chow group.

Proposition 14. *Let $f : X \to Y$ be flat of relative dimension n and let $\alpha \in \operatorname{Rat}_k Y$. Then $f^*\alpha \in \operatorname{Rat}_{k+n} X$.*

Proof. By Proposition 10, it suffices to consider $\alpha = [V(0)] - [V(\infty)]$ for some $V \subset Y \times \mathbb{P}^1$ that projects dominantly to $\mathbb{P}^1$. Note that this automatically gives us that the projection, p_2, is flat. Let $W = (f \times 1)^{-1}(V) \subset X \times \mathbb{P}^1$ and consider the following diagram:

$$\begin{tikzcd}
\mathbb{P}^1 & X \times \mathbb{P}^1 \arrow[l, "\widetilde{p}_2"'] \arrow[r, "f \times 1"] \arrow[d, "\widetilde{p}_1"] & Y \times \mathbb{P}^1 \arrow[r, "p_2"] \arrow[d, "p_1"] & \mathbb{P}^1 \\
& X \arrow[r, "f"] & Y &
\end{tikzcd}$$

Then we diagram chase:

$$f^*\alpha = f^*p_{1*}([p_2^{-1}(0)] - [p_2^{-1}(\infty)]) = \widetilde{p}_{1*}(f \times 1)^*([p_2^{-1}(0)] - [p_2^{-1}(\infty)]) = \widetilde{p}_{1*}([p_2|_W^{-1}(0)] - [p_2|_W^{-1}(\infty)])$$

Let $[W] = \sum a_i[W_i]$ with W_i varieties. Let $g = \widetilde{p}_2|_W$, $g_i = \widetilde{p}_2|_{W_i}$ and so we have $[g_i^{-1}(0)] - [g_i^{-1}(\infty)] = [\operatorname{div} g_i]$. Thus it will suffice to prove the following statements:

$$[g^{-1}(0)] = \sum_i a_i[g_i^{-1}(0)]$$

$$[g^{-1}(\infty)] = \sum_i a_i[g_i^{-1}(\infty)]$$

Note that both statements follow from technical computations in length with elementary commutative algebra. See [Fula] for details. ■

We now proceed to consider some analogies with the homology groups.

1.2 Exact Sequences and Analogies

Just as in cellular homology, we have several exact sequences associated with our Chow groups. The most important is excision.

Proposition 15 (Excision). *Let $V \subset X$ a (closed) subvariety and let $W = X \backslash V$ with $i : V \to X$, $j : W \to X$ be the inclusions. Then for all k we have the exact sequence*

$$A_kV \xrightarrow{i_*} A_kX \xrightarrow{j^*} A_kW \longrightarrow 0$$

Proof. We may extend any subvariety $W' \subset W$ to $W'' \subset X$ a subvariety (see [Har]) and so

$$Z_kV \xrightarrow{i_*} Z_kX \xrightarrow{j^*} Z_kW \longrightarrow 0$$

is exact. Now, suppose that $\alpha \in Z_kX$ and $j^*\alpha \in \operatorname{Rat}_k W$. Then we have $j^*\alpha = \sum \operatorname{div}(r_i)$ for $r_i \in K(Y_i)^\times$ with $Y_i \subset W$ subvarieties. Taking $Y_i' = \overline{Y}_i$ we let r_i' be the rational function on Y_i' corresponding to r_i. Then

$$j^*(\alpha - \sum \operatorname{div}(r_i')) = 0 \in Z_kW$$

By exactness of the cycle sequence, then, we have $\alpha - \sum \operatorname{div}(r_i) = i_*\alpha'$ for some $\beta \in Z_kV$. ∎

This yields Mayer-Vietoris in the usual way:

Corollary 16 (Mayer-Vietoris). *Let $V, W \subset X$ be subvarieties whose union is all of X. Then we have*

$$A_k(V \cap W) \longrightarrow A_kV \oplus A_kW \longrightarrow A_kX \longrightarrow 0$$

is exact for all k.

Proof. We may actually prove the slightly more general statement that if

$$\begin{tikzcd} U \arrow[r, "j"] \arrow[d, "p'"] & W \arrow[d, "p"] \\ V \arrow[r, "i"] & X \end{tikzcd}$$

is a fiber square with i closed embedding, p proper and such that $p'|X' \setminus Y'$ is an isomorphism onto $X \setminus Y$ then we have an exact sequence

$$A_kU \xrightarrow{(p'_*, -j_*)} A_kV \oplus A_kW \xrightarrow{i_*+p_*} A_kX \longrightarrow 0$$

which follows from Proposition 15. Now let j be a closed embedding and we are done. ∎

Proposition 17. *Let $p : E \to X$ be varieties such that there is a cover of open sets $U_\alpha \subset E$ such that $p^{-1}(U_\alpha) \cong X \times \mathbb{A}^n$ and $p|U_\alpha$ is projection. Then $p^* : A_kX \to A_{k+n}E$ is surjective.*

Proof. We first prove the special case where $E = X \times \mathbb{A}^1$. Let $V \subset E$ be a $(k+1)$-dimensional subvariety and so it suffices to show that $[V] \in p^*A_kX$. We may restrict X to $X = \overline{p(V)}$ and so V projects dominantly onto X. Letting $A = \mathcal{O}_X$ and $\mathfrak{p} \subset A[t]$ such that $V = V(\mathfrak{p})$ we have two cases. Either $\dim X = k$ or $\dim X = k+1$. In the former case we must have $V = X \times \mathbb{A}^1$ and so $V = E = p^{-1}(X)$ and the result is obvious. Suppose $\dim X = k+1$ and so $\mathfrak{p} \neq 0$; let $\mathfrak{p} = (r)$. Then we have $(k+1)$-dimensional subvarieties $V_i \subset E$ that project nondominantly to X, and let $W_i = p(V_i)$. Then $[W_i] = p^*[V_i]$. Thus we have

$$[V] - [\operatorname{div} r] = \sum_i a_i[V_i] = \sum_i a_i p^*[W_i]$$

as desired.

If $E = X \times \mathbb{A}^n$ then we have a factoring of $p : E \to X$ through $X \times \mathbb{A}^{n-1}$; thus this case reduces to the above paragraph. Finally, let E be arbitrary and let $U \subset X$ be a local trivialization with $U' = X \setminus U$. Then by Proposition 15, we have the following diagram with exact rows:

$$\begin{tikzcd}
A_*U' \arrow[r] \arrow[d, "p^*"] & A_*X \arrow[r] \arrow[d, "p^*"] & A_*U \arrow[r] \arrow[d, "p^*"] & 0 \\
A_*p^{-1}(U') \arrow[r] & A_*Y \arrow[r] & A_*p^{-1}(U) \arrow[r] & 0
\end{tikzcd}$$

Applying some variant of the 5-lemma, we see that it suffices to prove the result for U, U'. We may repeat the process with U' and so it suffices to prove the result for $U = X \times \mathbb{A}^n$ and we are done. ■

We will use Proposition 17 to compute our first Chow group in the following example.

Example 18. Consider first the case of $E = \mathbb{A}^n$ and $X = \operatorname{Spec} k$. Then we see that for $k < n$ we must have $A_k E = 0$. We will use this to compute that Chow group of projective space. Note first that there is a copy of $\mathbb{P}^{n-1} \subset \mathbb{P}^n$ and that $\mathbb{P}^n \setminus \mathbb{P}^{n-1} = \mathbb{A}^n$. Thus we have an exact sequence for all k:

$$\begin{tikzcd}
A_k\mathbb{P}^{n-1} \arrow[r] & A_k\mathbb{P}^n \arrow[r] & A_k\mathbb{A}^n \arrow[r] & 0
\end{tikzcd}$$

We wish to show that $A_k\mathbb{P}^n = \mathbb{Z}$ for $k \leq n$ and 0 otherwise. For $k > n$ this is obvious. For $k = 0$ this follows from Remark 3. We may apply induction then. Note that for $k \leq n$ we have that the image of $\mathbb{Z} \cdot H^k$ where H^k is a k-plane in $\mathbb{P}^{n-1}$ generates $A_k\mathbb{P}^n$ by our earlier result that $A_k\mathbb{A}^n = 0$ for $k < n$. For $k = n$ we may apply Remark 3. Now from our knowledge of $\operatorname{Pic}\mathbb{P}^n$ (see [Har, II.6]) we know that $A_{n-1}\mathbb{P}^n = \mathbb{Z} \cdot H^{n-1}$. For $k < n-1$ suppose that $d\zeta = \sum a_i \operatorname{div} r_i$ for $r_i \in K(V_i)^\times$ and let $Z = \bigcup V_i$. Because $k < n-1$, $n-k-2 \geq 0$ and there exists a $(n-k-2)$-dimensional linear subspace of $\mathbb{P}^n$ disjoint from Z. Let $f : Z \to \mathbb{P}^{k+1}$ be projection from this subspace. This is proper, so by Proposition 5, we have $0 = f_*(d\zeta) = df_*\zeta$. But we have $k+1 < n$ and so, by induction, $d = 0$. Thus we have

$$A_*\mathbb{P}^n = \mathbb{Z}[\zeta]/(\zeta^{n+1})$$

as a graded abelian group.

We will see in the next section that this is true as a ring as well, thus the reason for the reversal of degree in the grading.

1.3 The Intersection Product and a Combinatorial Application

While the connection to homology may seem cool, so far we have not really produced anything interesting from all of our hard work. That changes with the introduction of the intersection ring, or the Chow ring. Consider first that there is a naïve product on Z_*X. Namely, if $V, W \subset X$, can we just define $[V] \cdot [W] = [V \cap W]$? There are a few problems with this. Recall in our statement of Theorem 9 that we required our point counting to be 'with multiplicity.' The reason for this is that we may run into a situation such as Figure 2 where if we move our curves a little bit, we get more intersections. This is the reason for our

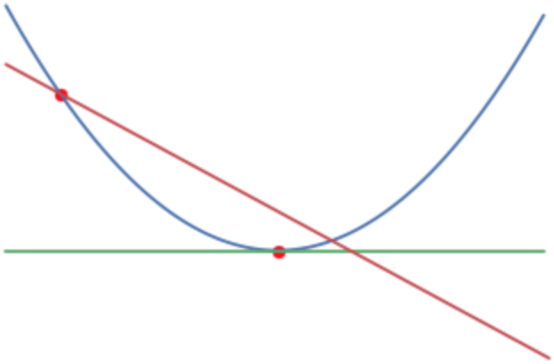

Figure 2: Transverse and not-transverse intersection

introduction of the Chow groups; we might hope that rational equivalence will allow us to always 'move' our varieties so that they intersect generically transversely. Results of this form, called moving lemmata, are explored in [EH]. A much more general approach is that of deformation to the normal cone, described in [Fula, Fulb]. Unfortunately, this bit of genius is beyond the scope of our talk. Instead, we restrict ourselves to smooth varieties, which allows us to make use of a slightly easier construction. We first define

Definition 19. Let X, Y be varieties and let $\alpha \in Z_k X$ and $\beta \in Z_\ell Y$. We define $\times : Z_k X \otimes Z_\ell Y \to Z_{k+\ell}(X \times Y)$ to be $[V] \times [W] = [V \times W]$.

We have the following result:

Proposition 20. *If $\alpha \in \operatorname{Rat}_k X$ or $\beta \in \operatorname{Rat}_\ell Y$ then $\alpha \times \beta \in \operatorname{Rat}_{k+\ell} X \times Y$. If f, g are proper morphisms out of X, Y respectively, then $(f \times g)_*(\alpha \times \beta) = (f_*\alpha) \times (g_*\beta)$ and similarly with flat pullback. The exterior product is associative, i.e., $(\alpha \times \beta) \times \gamma = \alpha \times (\beta \times \gamma)$.*

Proof. These are elementary. See [Fula] for the details. ∎

With Proposition 20, we have an induced map $A_k X \otimes A_\ell Y \to A_{k+\ell} X \times Y$. Now, suppose we have a fibre square

$$\begin{tikzcd}
Y \arrow[r, "f'"] \arrow[d, "g'"] & W \arrow[d, "g"] \\
V \arrow[r, "f"] & X
\end{tikzcd}$$

We claim that if f is a regular embedding of codimension d and g is proper and flat of relative dimension n, then for $\alpha \in A_k W$,

$$f^* g_* \alpha = g'_* f'^* \alpha \in A_{k-d} V$$

and if $\alpha \in A_k X$ then

$$g'^* f^* \alpha = f'^* g^* \alpha \in A_{k+n-d} Y$$

If, in addition, g is a regular embedding in codimension e then we have

$$g'^* f^* \alpha = f'^* g^* \alpha \in A_{k-d-e} Y$$

We refer the interested reader to [Fula, Fulb] for details.

The reason for all of this setup, is that we may now introduce an intersection product on X a smooth variety.

Definition 21. Let X be a smooth variety and let $\alpha \in A_k X$ and $\beta \in A_\ell X$. Let $\Delta : X \to X \times X$ be the diagonal embedding. We define the product $\cdot : A_k X \otimes A_\ell X \to A_{k+\ell-n} X$ as $\alpha \cdot \beta = \Delta^*(\alpha \times \beta)$.

Because X is smooth, we have that $\Delta : X \to X \times X$ the diagonal is a regular embedding of codimension $n = \dim X$ and so this makes sense from our above remarks. The fact that this is commutative and associative, as well as distributing over addition is easily checked from above. We leave it as an exercise to check this, or see [Fula].

We may reindex our grading and let $A^k X := A_{n-k} X$. we see that this turns $A^* X$ into a graded ring in that the product takes $A^k X \otimes A^\ell X \to A^{k+\ell} X$. Note that if we have subvarieties $V, W \subset X$ that intersect generically transversely, then $[V] \cdot [W] = [V \cap W]$ as we wanted in our naïve attempt at a product. This allows us to do explicit calculations in certain cases.

Example 22. As an example, we will compute the Chow ring of $\mathbb{P}^n$. Recall from the discussion following Proposition 17 that the group structure is given by $\bigoplus_{j=0}^n \mathbb{Z} \cdot H^j$, where H^j is a j-plane. Thus it suffices to compute $H^j \cdot H^i$. First note that if $i + j > n$ then the sum of the dimensions of H^i and H^j is $2n - i - j <$

$2n-n=n$ and so if H^i and H^j are chosen sufficiently generally then they do not intersect and their product will be zero. This matches our knowledge that $A^kX=0$ for $k>\dim X$. Now suppose that $i+j\leq n$. Then we know that an r-dimensional plane intersects a general s-dimensional plane in $\mathbb{P}^n$ in $r+s-n$ dimensions. Thus the intersection of general H^i and H^j is a plane of dimension $n-i+n-j-n=n-i-j$. But this is just the class of H^{i+j}. Thus we see that if ζ is a $(n-1)$-plane in $\mathbb{P}^n$ then ζ generates $A^*\mathbb{P}^n$ as a ring and we get that $A^*\mathbb{P}^n=\mathbb{Z}[\zeta]/\zeta^{n+1}$. Note that in the complex case, this is exactly what we expected for the cohomology ring. We do have a significant generalization, however, because our result holds in arbitrary characteristic.

Moreover, this leads us to a generalization of Theorem 9.

Proposition 23. *Let $X_1,X_2,\dots,X_k\subset\mathbb{P}^n$ be subvarieties of codimensions c_i such that $\sum c_i=c\leq n$ and such that their intersection, Z, has pure dimension $n-c$. Then $\deg[Z]=\prod\deg X_i$*

Proof. This follows immediately from our description of $A^*\mathbb{P}^n$ and the fact that $\deg\zeta^n=1$. ■

We now give an example application of our work above. First we state a quick proposition

Proposition 24. *For any m,n we have $A^*(\mathbb{P}^m\times\mathbb{P}^n)=A^*\mathbb{P}^m\otimes_{\mathbb{Z}}A^*\mathbb{P}^n$.*

Proof. For the group structure, we may apply induction and Proposition 15 to the sequence

$$A_*(\mathbb{P}^{m-1}\times\mathbb{P}^n)\longrightarrow A_*(\mathbb{P}^m\times\mathbb{P}^n)\longrightarrow A_*(\mathbb{A}^n\times\mathbb{P}^n)\longrightarrow 0$$

and then apply Proposition 17. For the multiplicative structure, the discussion above generalizes immediatley. ■

Remark 25. The formula above may look familiar as a Künneth type formula from cohomology. Do not be fooled, however, because this does *not* apply in general for Chow rings. This is a very special property of $\mathbb{P}^n$. See [EH] for more details.

Consider, now, the following question. Given general degree d homogeneous polynomials $A,B,C\in\mathbb{C}[t_0,t_1,t_2]$, how many points $t=(t_0:t_1:t_2)\in\mathbb{P}^2$ are there such that $(A(t):B(t):C(t))=t$? We will provide an answer to this. The techniques that we will use, undetermined coefficients and intersecting a graph with a diagonal, will return in more important applications later on.

In general, suppose that we have $F_0,F_1,\dots,F_s\in\mathbb{C}[t_0,t_1,\dots,t_r]$ homogeneous polynomials of common degree d with no common zeros and define a map $f:\mathbb{P}^r\to\mathbb{P}^s$ given by $f(t)=(F_0(t):\cdots:F_s(t))$. Let $\Gamma=\{(t,f(t))\in\mathbb{P}^r\times\mathbb{P}^s\}$ be the graph of this morphism. We will calculate $\gamma=[\Gamma]\in A^*(\mathbb{P}^r\times\mathbb{P}^s)$. Note that $\operatorname{codim}\Gamma=r+s-\dim\Gamma=s$. Thus there are coefficients a_i such that

$$\gamma=a_0\alpha^r\beta^{s-r}+\cdots+\alpha_r\beta^s$$

where α,β are the classes of $(r-1)$- and $(s-1)$-planes in $\mathbb{P}^r$ and $\mathbb{P}^s$ respectively. Consider $\alpha^{r-i}\beta^{s-r+i}\cdot\alpha^j\beta^{s-j}$. If $r-i+j>r$ then this is zero and similarly if $2s-r+i-j>s$ by Proposition 24. Thus this product is nonzero if and only if $i=j$. Taking degrees, we see that $a_i=\deg(\gamma\cdot\alpha^i\beta^{r-i})$. Let $\Lambda\subset\mathbb{P}^r$ be a codimension i plane and let $\Lambda'\subset\mathbb{P}^s$ be a codimension $r-i$ plane. Then if they are chosen sufficiently geneerally, $a_i=\#\{\Gamma\cap(\Lambda\times\Lambda')\}$. But this is just the intersection of $(r-i)$ linear combinations of the F_j and, applying Proposition 23, we get that this number is just d^{r-i}. Thus

$$\gamma=\sum_{i=0}^{r}d^i\alpha^i\beta^{s-i}$$

Now, consider $\Delta\subset\mathbb{P}^r\times\mathbb{P}^r$ the diagonal and let $\delta\in A^*(\mathbb{P}^r\times\mathbb{P}^r)$ represent it. Note that Δ is the graph of the identity and so has dimension $r+r-r=r$. Moreover, the identity has degree 1 so we apply the above and thus we have

$$\delta=\sum_{i=0}^{r}\alpha^i\beta^{r-i}$$

Now, we note that the number of fixed points of f, if $r = s$, is just the degree of $\gamma \cdot \delta$. By our computations above, we see that $\gamma \cdot \delta = d^r + d^{r-1} + \cdots + 1$. In our question above, we have $r = 2$, so the number of fixed points is just $d^2 + d + 1$.

We have introduced the basics of Intersection theory. We will now proceed to an analysis of the Chow ring of the Grassmannian, work that will allow us to answer all sorts of questions in combinatorial geometry.

2 Grassmannians and their Chow Rings

We will apply the results and theory from Section 1 to a vary concrete set of varieties: the Grassmannians. As remarked above, in most cases we do not have a good way of actually describing the Chow ring of a general variety. The Chow ring of a Grassmannian, however, is very explicit, allowing us to do computations. Moroever, because the Grassmannian parametrizes natural geometric objects, the computations that we conduct have very real meanings in geometry. We will first introduce a Grassmannian before proceeding to describe the Chow ring and doing a few examples of computations.

2.1 Grassmannians and Schubert Cells

Before doing anything, we must first define a Grassmannian.

Definition 26. Given a vector space, V, a Grassmannian is

$$G_k V = \{\Lambda \subset V | \Lambda \text{ is a linear subspace and } \dim \Lambda = k\}$$

When the vector space is irrelevant, we write $G(k, n)$ for the Grassmannian of k-planes in n-dimensional space. By $\mathbb{G}(k, n)$ we mean the Grassmannian of k-dimensional linear subspaces of $\mathbb{P}^n$.

A few elementary facts jump out immediately. Note first that $G_k V = G_{n-k} V^*$ by dualing the exact sequence for $\Lambda \in G_k V$:

$$\begin{tikzcd} 0 \arrow[r] & \Lambda \arrow[r] & V \arrow[r] & \Lambda' \arrow[r] & 0 \end{tikzcd}$$

If we do not care about any additional structure on the vector space, then we may write this as $G(k, n) = G(n-k, n)$. Note also that $\mathbb{G}(k-1, n-1) = G(k, n)$. We will use this fact in our applications, for intersection theory is much more natural in projective space than in affine space. We will equivocate between the two often.

Example 27. Note that $G_1 V = \mathbb{P}^1 V$. Indeed, this follows immediately from the definition of $\mathbb{P}^n$. We have already computed the Chow ring of $\mathbb{P}^n$ in Example 18 and we will see later that this is just a special case of the more general construction.

We will not go into too much detail, but the Grassmannian can be embedded into projective space (and so is a projective variety) by means of the plücker embedding. Let $\Lambda \in G_k V$ be a k-plane and consider the inclusion $\bigwedge^k \Lambda \hookrightarrow \mathbb{P} \bigwedge^k V$. This is clearly injective. Moreover, choosing a basis for V of $e_1, \ldots, e_n$, we may write $v_i = \sum x_{i,j} e_j$ and so $v_1 \wedge v_2 \wedge \cdots \wedge v_k = \sum p_{i_1,\ldots,i_k} e_{i_1} \wedge \cdots \wedge e_{i_k}$ over all tuples $1 \leq i_1 < i_2 < \cdots < i_k \leq n$ where the $p_{i_1,\ldots,i_k}$ are called Plücker coordinates. Clearly the embedding can be described as the vanishing of polynomials in these coordinates.

Example 28. The simplest nontrivial Grassmannian is $G(2, 4)$. One way to achieve the plücker embedding is to consider the row space of a generic matrix and consider the vanishing of the minors (note that a vast generalization of this consisting in the study of degeneracy loci is a rich and beautiful theory. We will unfortunately not have the time to cover vector bundles, but the interested reader is referred to [Fula, Fulb, EH] for details). So consider the matrix given by

$$\begin{pmatrix} x_{1,1} & x_{1,2} & x_{1,3} & x_{1,4} \\ x_{2,1} & x_{2,2} & x_{2,3} & x_{2,4} \end{pmatrix}$$

To find the relations of the Plücker coordinates that vanish, we may just double the matrix and take the determinate:

$$\begin{pmatrix} x_{1,1} & x_{1,2} & x_{1,3} & x_{1,4} \\ x_{2,1} & x_{2,2} & x_{2,3} & x_{2,4} \\ x_{1,1} & x_{1,2} & x_{1,3} & x_{1,4} \\ x_{2,1} & x_{2,2} & x_{2,3} & x_{2,4} \end{pmatrix}$$

and replacing $p_{i,j} = x_{i,i}x_{j,j} - x_{i,j}x_{j,i}$ we get the relation

$$p_{1,2}p_{3,4} - p_{1,3}p_{2,4} + p_{1,4}p_{2,3} = 0$$

But $\dim V = 4$ so $\mathbb{P}(\Lambda^2 V)$ is of dimension $6 - 1 = 5$. We see then that $G(2, 4)$ is of dimension 4. This is a special case of the general fact that $\dim G(k, n) = k(n - k)$.

The fact that Grassmannians are smooth algebraic varieties is proven in some detail in [EH, Chapter 3] and we will not prove it here. Instead, we will jump immediately to the Chow groups. Recall from Example 18 that we computed the Chow groups of $\mathbb{P}^n$ by finding subspaces whose complements were affine. This can be viewed as a special case of a more general method. Let X be a variety and consider a filtration $X_1 \subset X_2 \subset \cdots \subset X_n$ such that $X_i \setminus X_{i-1} = \bigcup_j \mathbb{A}^{i_j}$. We may apply the same method of using Proposition 17 to show that the classes of these $\mathbb{A}^{i_j}$ generate (not necessarily freely) the Chow group of X. Note that this method is very similar to computing cellular homology. The X_k can be thought of as the k-skeletons and the analogy becomes clear. In the case of the Grassmannian $G_k V$, let

$$\mathcal{F} : \{0\} = V_0 \subset V_1 \subset V_2 \subset \cdots \subset V_n = V$$

denote a full flag, i.e., $\dim V_i/V_{i-1} = 1$ for all i. For a k-tuple $a = (a_1, a_2, \dots, a_k)$ such that $n - k \geq a_1 \geq \cdots \geq a_1 \geq 0$, we define the Schubert cell

$$\Sigma_a \mathcal{F} = \{\Lambda \in G_k V | \dim V_{n-k+i-a_i} \cap \Lambda \geq i\}$$

Remark 29. While at first sight it may seem like this definition depends on the choice of flag $\mathcal{F}$, it does not. Indeed, choosing a different flag $\mathcal{F}'$, we see that there is some element $g \in \mathrm{GL}(V)$ such that $g \cdot \mathcal{F} = \mathcal{F}'$ and so the schubert cells are defined up to automorphism of the homogeneous space. Thus we will often omit the flag from our notation and write Σ_a as the schubert cell.

This definition may seem very ad hoc, but with a little bit of thought it should make sense. Consider the (in general not strict) filtration for a general k-plane $\Lambda \subset V$

$$0 \subset V_1 \cap \Lambda \subset V_2 \cap \Lambda \subset \cdots \subset V_n \cap \Lambda = \Lambda$$

Let $W_i = V_i \cap \Lambda$. Then either $W_i = W_{i-1}$ or $\dim W_i/W_{i-1} = 1$. In the latter case we may consider the dimension jumping up by 1. Because $\dim \Lambda = k$ there must be k 'jumps.' By dimension counting, we see that $\dim V_i \cap \Lambda \geq i + k - n$. Thus, in a sense, $\Lambda \in \Sigma_{a_1,\dots,a_i,\dots a_k}$ means that the i^{th} dimension jump happens a_i steps earlier than necessary. We give some examples.

Example 30. Consider the case where our partition a consists of just one element. We have then

$$\Sigma_{n-k+1-\ell} = \{\Lambda | \Lambda \cap V_\ell \neq 0\}$$

so this consists of those k-planes that intersect V_ℓ. In particular, Σ_1 is the set of those planes that intersect V_{n-k}.

Example 31. In the opposite extreme, consider that

$$\Sigma_{n-\ell,n-\ell,\dots,n-\ell} = \{\Lambda | \Lambda \subset V_\ell\} \cong G(k, \ell)$$

where $n - \ell$ is repeated k times, and, similarly

$$\Sigma_{n-k,n-k,\dots,n-k} = \{\Lambda | V_\ell \subset \Lambda\}$$

Our notation has some advantages. Three of them are summarized in the proposition below

Proposition 32. *Consider $G = G_kV$. The following are true:*

1. *Put a partial order on the set of partitions where $a \leq a'$ if and only if $a_i \leq a'_i$ for all i. Then $\Sigma_a \subset \Sigma_{a'}$ if and only if $a \geq a'$.*
2. *Let $|a| = a_1 + a_2 + \cdots + a_k$. Then $\operatorname{codim} \Sigma_a = |a|$.*
3. *Let $i : G(k,n) \hookrightarrow G(k+1, n+1)$ given by fixing an element of $v \in k^{n+1}/k^n$ and taking $\Lambda \mapsto \Lambda \oplus v$ and let $j : G(k,n) \hookrightarrow G(k, n+1)$ be the inclusion. Then $i^*\sigma_a = j^*\sigma_a = \sigma_a$. In particular, if an identity involving σ_a is known in the Chow ring for $G(k,n)$ then it is known in $G(k', n')$ if $k' \leq k$ and $n' - k' \leq n - k$.*

Proof. These statements are all immediate from the definitions. See [EH] for examples. ■

The reason that we introduce these cells is that we can now apply our 'cellular' decomposition and define

$$W^o_\lambda = \bigcup_{\mu > \lambda} \Sigma_\mu$$

and note that this is an affine stratification. This leads to the following proposition

Proposition 33. *Let $\sigma_a = [\Sigma_a] \in A^*G(k,n)$ be Schubert cycles, the classes of Schubert cells. Then the $\{\sigma_a\}$ generate $A^*G(k,n)$ as a graded group.*

Proof. The method follows from the preceding discussion. For details see [EH, Fula, Fulb]. ■

Example 34. Consider the example of $\mathbb{P}^n = G(1, n+1)$. Here we have $n + 1 - 1 = n$ and $k = 1$ so we have $n \geq a \geq 0$. Thus the cells are of the form Σ_i for $0 \leq i \leq n$, each one corresponding to $\mathbb{P}^{n-i}$.

In fact, we will see that the schubert cells freely generate the group. To do this, we will consider the multiplicative structure. We need the following lemma:

Lemma 35. *Let $\mathcal{F} = \{V_i\}, \mathcal{G} = \{W_j\}$ be flags such that $V_i \cap W_{n-i} = 0$, $\dim V_i \cap W_j = \max(0, i + j - n)$ and there exists a basis $\{e_k\}$ for V such that V_i is the span of $e_1, \ldots, e_i$ and W_j is the span of $e_{n-j+1}, \ldots e_n$. Let a, b be partitions such that $|a| + |b| = k(n-k)$. Then $\Sigma_a\mathcal{F}$ and $\Sigma_b\mathcal{G}$ intersect transversely. Moreover they intersect in a unique point if $a_i + b_{k+1-i} = n - k$ for all i and are disjoint otherwise. Thus if σ_a, σ_b denote the respective Schubert cells, we have*

$$\deg \sigma_a \sigma_b = \begin{cases} 1 & b = a* \\ 0 & \textit{otherwise} \end{cases}$$

Remark 36. We say that flags $\mathcal{F}, \mathcal{G}$ as in the lemma are *transverse flags.* Because of the special property of these intersections, we say that b is the dual partition and denote $b = a^*$ if it satisfies the condition for nonempty intersection above.

Proof. The fact that the intersection is generically transverse is not difficult. Details can be found in [EH, Chapter 4]. The last statement follows from transversality and the point counting. Thus it suffices to show the incidence relation and find the cardinality of

$$\{\Sigma_a\mathcal{F} \cap \Sigma_b\mathcal{G}\} = \{\Lambda | \dim \Lambda \cap V_{n-k+i-a_i} \geq i \text{ and } \dim \Lambda \cap W_{n-k+i-b_i} \geq i\}$$

Considering the conditions, we have for all i

$$\begin{aligned} \dim V_{n-k+i-a_i} \cap \Lambda &\geq i \\ \dim W_{n-k+i+1-b_{k-i+1}} \cap \Lambda &\geq k - i + 1 \end{aligned}$$

But $i + k - i + 1 > k$ so the spaces above must have nontrivial intersection in Λ and so we then must have $V_{n-k+i-a_i} \cap W_{n-i+1-b_{k-i+1}}$ is nontrivial. We have chosen $\mathcal{F}, \mathcal{G}$ to be general, though, so we must have the sum of their dimensions sufficiently large:

$$n - k + i - a_i + n - i + 1 - b_{k-i+1} > n$$

Rearranging, we have $a_i + b_{k-1+1} \leq n - k$. Thus, by generality of our choice in flags, if $a_i + b_{k-1+i} < n - k$ then the cells will be disjoint. On the other hand, we have that a, b are of complementary codimension and we know that the dimension of $G(k, n)$ is $k(n - k)$ so we have

$$k(n-k) = |a| + |b| = \sum_i a_i + b_{k+1-i} \leq \sum_i n - k = k(n-k)$$

and the result follows. ■

With this result in hand, we will be able to compute the general Chow ring of Grassmannians. In princple, we can use our method from the first section of undetermined coefficients to do computations in the Chow ring. In fact, if we have

$$\alpha = \sum_{|a|=i} \beta_a \cdot \sigma_a$$

then we have $\beta_a = \deg \alpha\sigma_{a^*}$. Often, we will be able to geometrically evaluate this. In princple, we can use these methods to find the entire multiplicative structure. Fore instance, consider

$$\sigma_\lambda \cdot \sigma_\mu = \sum_{|\nu|=|\lambda|+|\mu|} N^\nu_{\lambda\mu}\sigma_\nu$$

where $N^\nu_{\lambda\mu} = \deg(\sigma_\lambda\sigma_\mu\sigma_{\nu^*})$.

Example 37. Continuing the example of $\mathbb{P}^n$, we see that $\sigma_i \cdot \sigma_j = 1$ if $i + j = n$. There is only one cell for each codimension and these cells have dual partitions associated to them. In fact, we see that for any i, j, $\sigma_i\sigma_j = a_{i,j}\sigma_{i+j}$. Multiplying by σ_{n-i-j} and taking degrees gives us from Lemma 35 that $a_{i,j} = 1$ for all i, j and thus we recover the structure of the Chow ring of $\mathbb{P}^n$.

The numbers $N^\nu_{\lambda\mu}$ are called the *Littlewood-Richardson coefficients* and they show up in representation theory and combinatorics as well. In point of fact, there are many deep connections between representations of $\mathrm{GL}(V)$ and the Grassmannians of V. This connection is explored in great detail in [Fulc], but is unfortunately beyond the scope of this talk. We proceed to do a detailed computation.

2.2 Lines in $\mathbb{P}^3$ and Enumerative Geometry

In this section we do the detailed computation of the Chow ring of the smallest nontrivial example. Let $G = \mathbb{G}(1,3) = G(2,4)$. We have $\dim G = 4$. We first fix a flag $\mathcal{F} = \{p\} \subset L \subset H \subset \mathbb{P}^3$. We have the following generators:

$$\begin{array}{rrr}
A^0G = \langle\sigma_{0,0}\rangle & & \Sigma_{0,0} = \mathbb{G}(1,3) \\
A^1G = \langle\sigma_1\rangle & & \Sigma_1 = \{\Lambda | \Lambda \cap L \neq \emptyset\} \\
A^2G = \langle\sigma_2, \sigma_{1,1}\rangle & \Sigma_{1,1} = \{\Lambda | \Lambda \subset H\}, & \Sigma_2 = \{\Lambda | p \in \Lambda\} \\
A^3G = \langle\sigma_{2,1}\rangle & & \{\Lambda | p \in \Lambda \subset H\} \\
A^4G = \langle\sigma_{2,2}\rangle & & \Sigma_{2,2} = \{L\}
\end{array}$$

We first compute products of cells of complimentary dimension. We will identify $A^0G \cong \mathbb{Z}$ using degree and henceforth write $\sigma_{0,0} = 1$. We see that $n - k = 2$. Thus $(1,0)^* = (2,1)$, $(2,0)^* = (2,0)$ and $(1,1)^* = (1,1)$.

We may ignore products $\sigma_a\sigma_b$ where $|a|+|b|>4$ because these must be 0. Thus from Lemma 35, we have immediately the following relations:

$$\sigma_{1,1}^2 = \sigma_2^2 = \sigma_1\sigma_{2,1}\sigma_1 = \sigma_{2,2} \qquad\qquad \sigma_2\sigma_{1,1} = 0$$

Now we calculate $\sigma_1\sigma_2$. Let $\mathcal{F}, \mathcal{G}$ be transverse flags and so we have

$$\Sigma_1\mathcal{F} \cap \Sigma_2\mathcal{G} = \{\Lambda | \Lambda \cap L \neq \emptyset, \quad p' \in \Lambda\}$$

Where p' is the point in $\mathcal{G}$. Let $\mathcal{F}' = \{p'\} \subset \widetilde{L} \subset \widetilde{H}$ where $\widetilde{H}$ is the plane containing p' and L and $\widetilde{L}$ is any line containing p' and contained in $\widetilde{H}$. Then we see immediately that $\Sigma_1\mathcal{F} \cap \Sigma_2\mathcal{G} = \Sigma_{2,1}\mathcal{F}'$ and so $\sigma_1\sigma_2 = \sigma_{2,1}$. Similarly,

$$\Sigma_1\mathcal{F} \cap \Sigma_{1,1}\mathcal{G} = \{\Lambda | \Lambda \cap L \neq \emptyset, \quad \Lambda \subset H'\}$$

Let $\mathcal{G}' = \{\hat{p}\} \subset \hat{L} \subset H'$ where $\hat{p} = L \cap H'$ (which is a unique point given our choice of flags). Then this set is given by $\Sigma_{2,1}\mathcal{G}'$. Thus we have $\sigma_1\sigma_{1,1} = \sigma_{2,1}$. Finally, we compute σ_1^2. We use the method of undetermined coefficients. We have $\sigma_1^2 \in A^2G$ so there are $\alpha, \beta \in \mathbb{Z}$ such that $\sigma_1^2 = \alpha\sigma_2 + \beta\sigma_{1,1}$. We invoke associativity:

$$\begin{aligned} \alpha = \deg \sigma_1^2\sigma_2 = \deg \sigma_1(\sigma_1\sigma_2) = \deg \sigma_1\sigma_{2,1} = \deg \sigma_{2,2} = 1 \\ \beta = \deg \sigma_1^2\sigma_{1,1} = \deg \sigma_1(\sigma_1\sigma_{1,1}) = \deg \sigma_1\sigma_{2,1} = 1 \end{aligned}$$

Thus $\sigma_1^2 = \sigma_2 + \sigma_{1,1}$. We thus have a complete multiplication table:

$$\begin{aligned} \sigma_{1,1}^2 = \sigma_2^2 = \sigma_1\sigma_{2,1}\sigma_1 = \sigma_{2,2} &\qquad\qquad \sigma_2\sigma_{1,1} = 0 \\ \sigma_1\sigma_2 = \sigma_1\sigma_{1,1} = \sigma_{2,1} &\qquad\qquad \sigma_1^2 = \sigma_2 + \sigma_{1,1} \end{aligned}$$

We thus have a complete description of A^*G.

We will now use our computation above to answer some questions in enumerative geometry. Our first question is very classical. Given 4 general lines in $\mathbb{P}^3$, how many lines intersect all 4 of these lines? This is the sort of question for which Schubert calculus was designed. From the definition, G parametrizes lines in $\mathbb{P}^3$ and, moreover, from Example 30, we have that the locus of lines meeting a given line L is just $\Sigma_1\mathcal{F}$ for some flag $\mathcal{F}$ that has L as its line. Our lines are general, so we may take flags $\mathcal{F}_1, \mathcal{F}_2, \mathcal{F}_3, \mathcal{F}_4$ with lines given by L_1, L_2, L_3, L_4 that intersect generically transversely. Thus, the desired number of lines is just given by $\#\bigcap_i \sigma_1\mathcal{F}_i = \deg[\sigma_1]^4 = \deg \sigma_1^4$. However, we have already done this computation.

$$\sigma_1^4 = (\sigma_1^2)^2 = (\sigma_2 + \sigma_{1,1})^2 = 2 \cdot \sigma_{2,2}$$

and has degree 2. Thus there are exactly two lines that intersect all 4 general lines.

We can further generalize the above by considering curves C_i of degree d_i. The question is the same: how many lines in $\mathbb{P}^3$ intersect all four of these general curves? Now, we consider the set

$$\Theta_C = \{L \in G | L \cap C \neq \emptyset\}$$

where C is a curve of degree d. Note that this is a generalization of the above, as $\Theta_C = \Sigma_1$ if $\deg C = 1$ and C is a line. Consider the set

$$\Gamma = \{(p, L) \in C \times G | p \in L\}$$

equipped with

$$\begin{tikzcd} \Gamma \arrow[r, "p_2"] \arrow[d, "p_1"] & G \\ C & \end{tikzcd}$$

Then for all $p \in C$, denoting by Γ_p the fiber of p_1 over p, we have $\Gamma_p \cong \Sigma_2 = \mathbb{P}^2$ because Σ_2 is defined to be the set of lines containing a point p from Example 30 and $\Sigma_2 = G(2,3) = G(1,3) = \mathbb{P}^2$ from Example 31. Thus we have that $\dim \Gamma = 3$. Now, note that p_2 is generically one-to-one because lines and curves are both codimension 2 and so the general line does not intersect C in $\mathbb{P}^3$. Thus we have that $\dim \Theta = 3$. We have seen that $\dim G = 4$ so we let $\theta = [\Theta] \in A^1 G$. Then $\theta = \alpha\sigma_1$ and $\alpha = \deg \theta \cdot \sigma_{2,1}$. Let $p \in H \subset \mathbb{P}^3$ be a general flag. Then we have

$$\alpha = \#\{\Theta \cap \Sigma_{2,1}(p,H)\} = \#\{\Lambda \in G | p \in L \subset H, \quad L \cap C \neq \emptyset\} = d$$

where the last equality follows from the fact that a degree d curve intersects H in d points and if our choice is sufficiently general, no pair of these points will be colinear with p. Thus we have $\theta = d\sigma_1$ and we have that the number of lines that intersect four curves $C_1, \dots, C_v \subset \mathbb{P}^3$ with degrees $d_1, \dots, d_4$ is given by $2\prod d_i$. Note that in the case of all $d_i = 1$ we specialize to the above example.

We now proceed to discuss a few general formulas for computation in $A^*G(k,n)$.

2.3 Pieri and Giambelli: Computing in the General Case

We digress slightly to discuss some combinatorics. A thorough treatment of the theory of Young Tableaux is given in [Fulc]. Note that given $G = G(k,n)$, our cells are parametrized by sequences λ such that $n-k \geq \lambda_1 \geq \cdots \geq \lambda_k \geq 0$. Recall that an *integer partition* is a nonnegative descending sequence of integers. Associated to any partition, there is a *Young diagram* that consists of boxes, where the top row has λ_1 boxes, the second row has λ_2 boxes, and the i^{th} row has λ_i boxes. An example is given in Figure 3. Clearly partitions are in bijective correspondence to Young diagrams. One reason to introduce this notation is to be able to clearly visualize certain properties of the partitions. For instance, if λ shows up as a cell in G, we see that $\lambda_i \leq n-k$ for all i and, moreover, all $\lambda_i = 0$ for all $i > k$. Thus the Young diagram of λ can fit into a $k \times (n-k)$ box with k rows and $(n-k)$ columns. This immediately gives that the dimension of G is $k(n-k)$ because the maximal codimension of any cell is when the our box is completely full; our box has $k(n-k)$ squares so $\dim G = k(n-k)$.

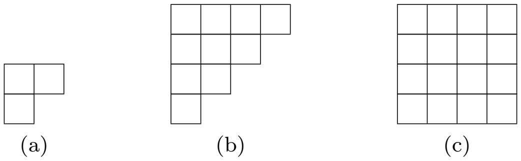

Figure 3: Examples of Young diagrams associated to (a) $\lambda = (2,1)$, (b) $\lambda = (4,3,2,1)$ and (c) $\lambda = (4,4,4,4)$

Example 38. We may also use the above to count the rank of $A^*G(k,n)$. Consider the right boundary of some partition λ in the big $k \times (n-k)$ box consisting of each square that is rightmost in each row, or the left hand boundary if $\lambda_i = 0$. Then the set of these paths is in bijection with the set of λ that fit into our big box; just let λ be the partition given by the Young diagram of every square to the left of our path. Thus it suffices to count the number of these paths. Starting from the bottom left corner and going up to the top right, we make exactly k 'up' moves and exactly $n-k$ 'right' moves and the orderings of these moves correspond bijectively to the set of paths. Thus the rank of $A^*G(k, n-k)$ is given by $\binom{n-k+k}{k} = \binom{n}{k}$.

Example 39. The Young diagrams also behave well with respect to dualization. Recall the isomorphism $G_k V \cong G_{n-k}V^*$. This map sends $\lambda \mapsto \mu$ where μ is the conjugate partition.

Example 40. The Young diagrams help one visualize the concept of duality of partitions as well, seen in Lemma 35. If λ is a partition, then λ^* the dual partition is given by taking the complement of λ in the big $k \times (n-k)$ box.

For those that are familiar with the representation theory of $\mathrm{GL}(V)$, much of the preceding discussion should begin to look familiar. This sense of *déjà vu* should only grow stronger with the introduction of Pieri and Giambelli. We show two formulas that allow one to compute arbitrary products in $A^*G(k,n)$.

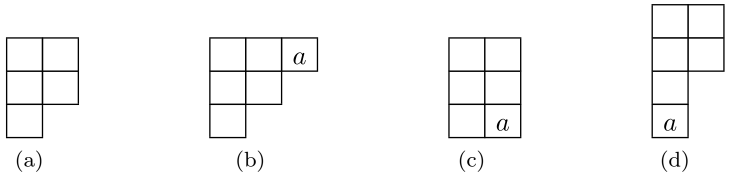

Figure 4: (a) is the original partition $\lambda = (2, 2, 1)$ and (b), (c), (d) are the admissible partitions according to Proposition 41 with the extra square marked with an a

Proposition 41 (Pieri)**.** *Let λ be a partition that corresponds to $\sigma_\lambda \in A^*G(k, n)$ and let $1 \leq a \leq n - k$. Then we have the following formula*

$$\sigma_\lambda \sigma_a = \sum_{\substack{|\mu|=|\lambda|+a \\ \lambda_i \leq \mu_i \leq \lambda_{i-1}}} \sigma_\mu$$

Remark 42. Another way to think about this is via Young tableaux. The admissible μ that appear in the right hand side above are those that can be obtained from λ by adding a total boxes with at most one being added to each column. See Figure 4 for an example.

Proof of Proposition 41. By Lemma 35, we need only show the following:

$$\deg(\sigma_\lambda \sigma_a \sigma_{\mu^*}) = \begin{cases} 1 & \lambda_i \leq \mu_i \leq \lambda_{i-1} \\ 0 & \text{otherwise} \end{cases}$$

Let $\mathcal{F}, \mathcal{G}, \mathcal{H}$ be flags of subspaces V_i, W_i, U_i respectively. By definition

$$\Sigma_\lambda \mathcal{F} = \{\Lambda |\dim \Lambda \cap V_{n-k+i-\lambda_i} \geq i\}$$
$$\Sigma_{\mu^*} \mathcal{G} = \{\Lambda |\dim \Lambda \cap W_{i+\mu_{k+1-i}} \geq i\}$$

and let

$$A_i = V_{n-k+i-\lambda_i} \cap W_{k+1-i-\mu_i}$$

by the above, we have for $\Lambda \in \Sigma_\lambda \mathcal{F} \cap \Sigma_{\mu^*} \mathcal{G}$ that $\Lambda \cap A_i \neq 0$. If we have $\mu_i < \lambda_i$ for some i then we have by choosing our flags to be sufficiently general that $A_i = 0$ because of dimension counting:

$$n - k + i - \lambda_i + k + 1 - i - \mu_i - n \leq 1 + \mu_i - \lambda_i \leq 0$$

and so $\deg \sigma_\lambda \sigma_a \sigma_{\mu^*} = 0$ as desired.

Now, let A be the span of all the A_i. We have

$$\dim A \leq \sum \mu_i - \lambda_i + 1 = k + |\mu| - |\lambda| = k + a$$

with equality if and only if we have $\mu_i \leq \lambda_{i-1}$ for all i. Now, we know that

$$\Sigma_a \mathcal{H} = \{\Lambda |\dim \Lambda \cap U_{n-k+1-a} > 0\}$$

from Example 30. If Λ exists such that it is in the intersection of all three varieties, then we must have $A \cap U_{n-k+1-a} \neq 0$ and so $\dim A \geq k + a$ because we need $n - k + 1 - a + \dim a > n$. If $\mu_i > \lambda_{i-1}$ for any i then we have $\dim A < k + a$ and so our intersection is empty as desired.

It remains to show that if $\dim A = k + a$ then we do have a point of intersection. Note that in this case we have $\dim U_{n-k+1-a} \cap A = n - k + 1 - a + \dim a - n = 1$. Let $v \neq 0 \in U_{n-k+1-a} \cap A$ and write $v = \sum v_i$ for $v_i \in A_i$. We have that $\Lambda \subset A$ and $\Lambda \cap U \neq 0$ so we must have $v \in \Lambda$. But $\Lambda = \text{Span}(\Lambda \cap A_i)$ so $v_i \in \Lambda$ for all i. Thus the desired intersection $\Sigma_\lambda \cap \Sigma_a \cap \Sigma_{\mu^*} = \{\Lambda\}$, a unique point of degree 1, as desired. ■

We conclude this section with the last ingredient to calculating general products of schubert cycles, the formula of Giambelli.

Proposition 43 (Giambelli)**.** *For any partition λ, we have the following identity*

$$\sigma_\lambda = |\sigma_{\lambda_i + j - i}|$$

the determinant of a matrix of special schubert cycles.

Remark 44. Note that using Propositions 41 and 43 together in priniple allows one to multiply arbitrary schubert cycles.

Proof. In the case of $\lambda = (a, b)$, we have

$$\begin{vmatrix} \sigma_a & \sigma_{a+1} \\ \sigma_{b-1} & \sigma_b \end{vmatrix} = \sigma_a\sigma_b - \sigma_{a+1}\sigma_{b-1}$$

$$= \sum_{i=0}^{b} \sigma_{a+i,b-i} - \sum_{j=0}^{b-1} \sigma_{a+1+j,b-1-j} = \sigma_{a,b}$$

where we used Proposition 41 for the penultimate inequality. For the general case, induct on the length of the partition using a cofactor expansion. ■

While combining Propositions 41 and 43 technically allows any computation, these computations quickly become intractable. The study of the Chow rings of Grassmannians and their applications to enumerative geometry is still an area of active research.

3 Point Counting and the Hasse-Weil Bound

In this section, we compute a real life application of intersection theory. The study of the zeta functions of varieties occupied many mathematicians for a long time and inspired the development of etale cohomology. The general results in the theory are incredibly deep. We will be using the theory developed thus far to prove the Hasse-Weil bound for numbers of points on a smooth projective curve of genus g over a finite field $\mathbb{F}_q$, but first we will introduce a number theoretic proof of a special case, following a method from [Was].

3.1 Gauss Sums and the Fermat Curve

While our main goal is to count points for a general smooth curve $C/\mathbb{F}_q$, we might start with an easy case. In general, how many points in $\mathbb{P}^2_{\mathbb{F}_q}$ satisfy $x^d + y^d = z^d$, where $p \nmid d$? Note that if we allowed $p|d$ then we would not be working with a smooth curve and we would have an inseperable extension; this theory lies beyond the scope of this talk. In order to count these, we will introduce the concept of a Gauss sum.

Definition 45. Let ζ_p be a primitive p^{th} root of unity and let $\mathrm{Tr} : \mathbb{F} = \mathbb{F}_q : \mathbb{F}_p$ be the trace. Let $\psi : \mathbb{F} \to \mathbb{C}^\times$ be defined as $\psi(x) = \zeta_p^{\mathrm{Tr}(x)}$. Let $\chi : \mathbb{F}^\times \to \mathbb{C}^\times$ be a multiplicative character extended to $\mathbb{F}$ by $\chi(0) = 0$. We define

$$g(\chi) = -\sum_{a \in \mathbb{F}} \chi(a)\psi(a)$$

We define the Jacobi sum of two characters as

$$J(\chi_1, \chi_2) = -\sum_{a \in \mathbb{F}} \chi_1(a)\chi_2(1-a)$$

It is immediate that $g(1) = 1$ for the trivial character. We have the following elementary properties:

Proposition 46. *We have the following results:*

1. $g(\overline{\chi}) = \chi(-1)\overline{g(\chi)}$
2. *For* $\chi \neq 1$, *we have* $g(\chi)g(\overline{\chi}) = \chi(-1)q$
3. *For* $\chi \neq 1$ *we have* $g(\chi)\overline{g(\chi)} = q$

4. *$J(1,1) = 2 - q$*
5. *For $\chi \neq 1$ we have $J(1,\chi) = 1$*
6. *For $\chi \neq 1$ we have $J(\chi, \overline{\chi}) = \chi(-1)$*
7. *For $\chi_1, \chi_2, \chi_1\chi_2 \neq 1$, we have $J(\chi_1,\chi_2) = \frac{g(\chi_1)g(\chi_2)}{g(\chi_1,\chi_2)}$*
8. *If the orders of χ_1, χ_2 divide m, then $\frac{g(\chi_1)g(\chi_2)}{g(\chi_1\chi_2)} \in \mathcal{O}_{\mathbb{Q}(\zeta_m)}$*

Proof. The first point is obvious and the second follows from the first and third. For the third, we have

$$g(\chi)\overline{g(\chi)} = \sum_{a,b\neq 0} \chi(ab^{-1})\psi(a-b) = \sum_{b,c=ab^{-1}} \chi(c)\psi(bc-b)$$
$$= \sum_{b\neq 0} \chi(1)\psi(0) + \sum_{c\neq 0,1} \chi(c) \sum_{b} \psi(b(-1)) = q - 1 - \sum_{c\neq 0,1} \chi(c) = q$$

The next two are immediate. For the following two points, we compute

$$g(\chi_1)g(\chi_2) = \sum_{a,b} \chi_1(a)\chi_2(b)\psi(a+b) = \sum_{a,b} \chi_1(a)chi_2(b-a)\psi(b)$$
$$= \sum_{\substack{a,b\\ b\neq 0}} \chi_1(a)\chi_2(b-a)\psi(b) + \sum_{a} \chi_1(a)\chi_2(-a)$$

If $\chi_1\chi_2 \neq 1$ then this last sum vanishes by orthogonality of characters. Otherwise it is $\chi(-1)(q-1)$. Letting $c = ab$ we have that the first sum becomes

$$\sum_{\substack{b,c\\ b\neq 0}} \chi_1(b)\chi_2(b)\chi_1(c)\chi_2(1-c)\psi(b) = g(\chi_1\chi_2)J(\chi_1,\chi_2)$$

Then points 6 and 7 fall out of the cases $\chi_1\chi_2$ either being 1 or not respectively. The last point follows from the preceding two. ■

Recall that if $(m,p) = 1$ then $\mathbb{Q}(\zeta_m)$ and $\mathbb{Q}(\zeta_p)$ are disjoint extensions (their intersection is $\mathbb{Q}$). If $b \in \mathbb{N}$ such that $(b,m) = 1$, then we define $\sigma_b \in \mathrm{Gal}(\mathbb{Q}(\zeta_m, \zeta_p)/\mathbb{Q})$ given by fixing ζ_p and raising $\zeta_m \mapsto \zeta_m^b$. We have the following two results:

Proposition 47. *We have the following:*

1. *If $\chi^m = 1$ then $\frac{g(\chi)^b}{\sigma_b g(\chi)} \in \mathbb{Q}(\zeta_m)$ and $g(\chi)^m \in \mathbb{Q}(\zeta_m)$*
2. *For all characters χ, $g(\chi^p) = g(\chi)$*

Proof. For (1) we note

$$\sigma_b \cdot g(\chi) = -\sum \chi(a)^b \psi(a) = g(\chi^b)$$

Let $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_{mp})/\mathbb{Q}(\zeta_m))$. Then $\tau \cdot \zeta_m = \zeta_m$ and $\tau \cdot \zeta_p = \zeta_p^c$ for some $(c,p) = 1$. Then we have

$$\tau \cdot g(\chi) = -\sum \chi(a)\psi(ca) = -\chi(c)^{-1} \sum \chi(a)\psi(a) = \chi(c)^{-1} g(\chi)$$
$$\tau \cdot \sigma_b g(\chi) = \chi(c)^{-b} \sigma_b g(\chi)$$

and thus if we take their ratios we see that τ fixes $\frac{g(\chi)^b}{\sigma_b g(\chi)}$. The second statement follows from applying the above to the case $b = m+1$.

To prove the second point, we note that $\mathrm{Tr}(a^p) = \mathrm{Tr}(a)$ because Frob_p fixes $\mathbb{F}_p$ and finite fields are perfect so we have

$$g(\chi^p) = -\sum \chi(a^p)\zeta_p^{\mathrm{Tr}\, a} = -\sum \chi(a^p)\zeta_p^{\mathrm{Tr}(a^p)} = -\sum \chi(a')\zeta_p^{\mathrm{Tr}(a')} = g(\chi)$$

■

We are now prepared to count the number of points on the curve $x^d + y^d = 1$ for $x, y \in \mathbb{F}_q$. We first consider the case of $d|q-1$. Let $\nu_d(u)$ be the number of $v \in \mathbb{F}_q$ such that $v^d = u$. Let χ be a character of $\mathbb{F}_q^\times$ such that $|\chi|$ exists. Note that this is possible because $\hat{\mathbb{F}_q^\times}$ is a finite abelian group. Then we have

$$\nu_d(u) = \begin{cases} 1 & u = 0 \\ d & u = v^d \\ 0 & u \neq v^d \end{cases} = \sum_{i=1}^{d} \chi(u)^i$$

where $\chi^i(0) = 0$ if $\chi^i \neq 1$. If $x = 0$ there are d solutions $(0, \zeta_d^i)$ and similarly if $y = 0$. Thus the number of points on the curve over $\mathbb{F}_q$ is given by

$$N_q = 2d + \sum_{\substack{u+v=1 \\ uv \neq 0}} \nu_d(u)\nu_d(v) = 2d + \sum_{u \neq 0,1} \sum_{a,b=1}^{d} \chi^a(u)\chi^b(1-u) = 2d - \sum_{a,b=1}^{d} J(\chi^a, \chi^b)$$

If $a = b = d$ we get a contribution of $2 - q$ from Lemma 46.4. If one of a, b is d and the other is not, we get a contribution of 1 by Lemma 46.5 and there are $2(d-1)$ of these cases. If $a + b = d$ then we contribute $\sum_1^{d-1} \chi^i(-1) = \nu_d(-1) - 1$ by Lemma 46.6. Applying Lemma 46.7 expresses the other sums as gauss sums. Note that $\nu_d(-1)$ is the number of points on the curve over infinity, so if $C : x^d + y^d = z^d$ and $N_q(C)$ is the number of points on C over $\mathbb{F}_q$, then we add the above together and get

$$N_q(C) = q + 1 - \sum_{\substack{a,b=1 \\ a+b \neq d}}^{d-1} J(\chi^a, \chi^b)$$

But note that by Lemma 46.3, we have that $|J(\chi^a, \chi^b)| = \sqrt{q}$. There are $(d-1)(d-2)$ terms in the sum above. Thus we have

$$|N_q(C) - q - q| = |\sum_{\substack{a,b=1 \\ a+b \neq d}}^{d-1} J(\chi^a, \chi^b)| \leq \sum_{\substack{a,b=1 \\ a+b \neq d}}^{d-1} |J(\chi^a, \chi^b)| = (d-1)(d-2)\sqrt{q}$$

as desired. If d is arbitrary, then let $(d, q-1) = e$ and note that if $C_e : x^e + y^e = z^e$ then $N_q(C) = N_q(C_e)$ and clearly $(e-1)(e-2) \leq (d-1)(d-2)$. Finally, recall the degree-genus formula for plane curves that says that $2g = (d-1)(d-2)$ and we get the bound as it can be generalized:

$$|N_q(C) - q - 1| \leq 2g\sqrt{q}$$

In the next two sections, we generalize this to all smooth curves instead of just the Fermat curve in the plane.

3.2 Intersection Theory and Asymptotics

We will use the intersection theory we have developed to provide a bound on the number of points on a smooth curve. We will do this in two parts. The first part uses intersection theory on a surface and some techniques we developed in the first section to asymptotically bound this number of points. In the second part we will use these asymptotics to get a sharper bound.

We will use the method from the first computation: we will intersect the graph of a function with the diagonal to find the number of fixed points. In particular, let X' be a smooth (projective) curve over $\mathbb{F}_q$ where $q = p^k$ for some k. Let X denote the base change of X' up to $\overline{\mathbb{F}}_q$ and define $X(\mathbb{F}_{q^r})$ to be X' base changed up to $\mathbb{F}_{q^r}$. Given an element $a \in \mathbb{F} = \overline{F}_q$, we know that for any r, $a \in \mathbb{F}_{q^r}$ if and only if $\text{Frob}^r(a) = a^{q^r} = a$. Let $f_r : X \to X$ be the, r^{th} power of $\text{Frob} : X \to X$, i.e., it is a homeomorphism on the underlying topological space and is the frobenius on the structure sheaf (see [Har, IV.2] for details). Then we see that the fixed points of f_r are exactly those points that are $\mathbb{F}_{q^r}$-rational. We may then let Γ_r be the graph of f_r and let $\gamma_r = [\Gamma_r] \in A^*X$. Let $\Delta \subset X \times X$ be the diagonal and $\delta = [\Delta]$ be its rational equivalence class. We will see that the number of points on $X(\mathbb{F}_{q^r})$ is given by $\delta \cdot \gamma_r$. We formalize this below. We let $N_r(X)$ be the number of $\mathbb{F}_{q^r}$-rational points on X. We have

Lemma 48. *Let $\gamma = [\Gamma_r]$ as above. Then $\gamma = ((\mathrm{Frob} \times id)^*)^r \delta$. Moreover, $\gamma_r \cdot \delta = N_{q^r}(X)$ so we have*

$$N_{q^r}(\delta) = \delta \cdot (f_r \times id)^* \delta$$

Proof. For the first statement, by functoriality, it is clear that $((\mathrm{Frob} \times \mathrm{id})^*)^r = ((\mathrm{Frob} \times \mathrm{id})^r)^* = (\mathrm{Frob}^r \times \mathrm{id})^* = (f_r \times \mathrm{id})^*$. This, then follows from Proposition 14. For the second, it is well known that $d\,\mathrm{Frob} = 0$ so $df_r = 0$ and Γ_r, Δ then meet generically transversely. They are both irreducible, dimension 1 schemes, so they meet at closed points (see [Har]). From the discussion above, we have that a point $x \in X$ is $\mathbb{F}_{q^r}$-rational if and only if it is fixed by f_r. Thus the intersection product as it is defined in Definition 21 immediately yields the desired result, as a point $x \in X$ is fixed by f_r if and only if it shows up in $\Delta \cap \Gamma_r$. ■

We digress somewhat to prove the Hodge index theorem. The proof comes directly out of [Har] and is included only for the sake of completeness. We now restrict our intersections to intersections on a surface Y.

Definition 49. Let $\alpha \in A^1 Y$ where Y is a smooth surface. We say that α is numerically equivalent to zero if $\alpha \cdot \beta = 0$ for all $\beta \in A^1 Y$. Let $\mathrm{Pic}^n Y \subset A^1 Y$ be the group of those divisors numerically equivalent to zero and define the group $\mathrm{Num}(Y) = (A^1 Y / \mathrm{Pic}^n Y)$. This group has a nondegenerate inner product given by the intersection form.

Remark 50. The fact that the Neron-Severi group is finitely generated is a very deep theorem. See [Har, V.1] for references, as this is something we shall take on faith.

Theorem 51. *Let $(\cdot, \cdot) : \mathrm{Num}(Y) \times \mathrm{Num}(Y) \to \mathbb{Z}$ given by the intersection pairing. Then the form induced on $\mathrm{Num}\, Y \otimes_{\mathbb{Z}} \mathbb{R}$ can be diagonalized to have one 1 on the diagonal and everything else -1.*

Before we can prove Theorem 51, we prove a lemma:

Lemma 52. *If H is an ample divisor on Y and we have some nonzero $\alpha \in \mathrm{Num}(Y)$ such that $\alpha \cdot H = 0$, then $\alpha^2 < 0$.*

Proof. We first reduce to the case $\alpha^2 > 0$ so suppose $\alpha^2 = 0$. Then let $\beta \in A^1 Y$ such that $\alpha \cdot \beta \neq 0$, which exists because $\alpha \neq 0 \in \mathrm{Num}\, Y$. Possibly replacing β by $H^2 \cdot \beta - (H \cdot \beta) H$, we may assume that $\beta \cdot H = 0$. Let $\alpha' = n\alpha + \beta$. Then $\alpha' \cdot H = 0$ and $\alpha'^2 = 2n\alpha \cdot \beta + \beta^2$. Thus there exists some choice of $n \in \mathbb{Z}$ such that $\alpha'^2 > 0$ and it suffices to consider this case.

Now suppose $\alpha^2 > 0$. Let $\beta = \alpha + nH$. By the fact that H is ample, we have that for all $n \gg 0$, β is ample (see [Har]). But $\alpha\beta = \alpha^2 > 0$ so for all $m \gg 0$ we have $m\alpha$ is effective and so we must have $0 < m\alpha H$ which can only happen if $\alpha H > 0$, which contradicts the fact that $\alpha \cdot H = 0$. ■

Proof of Theorem 51. We know that symmetric, nondegenerate forms can be diagonalized. Moroever, we may take some scaled factor of an ample divisor as one of the basis elements. But then Lemma 52 gives us that all of the other basis elements must have negative squares. Rescaling as necessary, we may take the matrix to be of the form

$$\begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & -1 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & \dots & \dots & -1 \end{pmatrix}$$

as desired. ■

We are now ready to provide our asymptotic bound.

Theorem 53. *For X the base change up to the algebraic closure of a smooth curve over $\mathbb{F}_q$, we have*

$$N_r(X) = q^r + O(q^{\frac{r}{2}})$$

Proof. Let $Y = X \times X$ and let $V = \operatorname{Num} Y \otimes_{\mathbb{Z}} \mathbb{R}$ and let $(\cdot, \cdot)$ be the intersection form as in Theorem 51. Then, as per Theorem 51, we may write $V = V_+ \oplus V_-$ where the intersection form is positive definite on V_+, negative definite on V_- and $\dim V_+ = 1$. Let $U_1 = X \times \{x_0\}$ and let $U_2 = \{x_0\} \times X$ be subvarieties of Y. By the definition of the intersection product, we see that if $\alpha_i = [U_i] \in A^1Y$ then $\alpha_1\alpha_2 = 1$, while $\alpha_i^2 = 0$. Moreover, note that $f_r^*\alpha_1 = q^r\alpha_1$ and $f_r^*\alpha_2 = \alpha_2$. Let $W = \operatorname{Span}(\alpha_1, \alpha_2) \subset V$ and let $V = W \oplus W'$, chosen such that $(W, W') = 0$, i.e., $W' = W^\perp$ with respect to the intersection form. By the above computation, we see that the intersection form on W with respect to the basis α_1, α_2 is given by

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

with characteristic polynomial $\lambda^2 - 1 = (\lambda - 1)(\lambda + 1)$ and so it has a positive eigenvalue. By Theorem 51, we have $V_+ \subset W$ then. Thus W' is negative definite. Note that $f_1^*\alpha_1 = q \cdot \alpha_1$ and $f_1^*\alpha_2 = \alpha_2$ and so by Lemma 48 $\gamma_r = f_r^*\delta$. We can then apply the projection formula, a remnant of the discussion following Proposition 20 (see [Fula, Fulb] for details) to get for general $\alpha, \beta \in A^1Y$,

$$f_r^*\alpha \cdot f_r^*\beta = \alpha \cdot (f_{r*}f_r^*\beta) = \alpha \cdot (q^r\beta) = q^r(\alpha \cdot \beta)$$

where the penultimate equality comes from the degree of f_r. Applying this to our form, we see that for any $v_1, v_2 \in V$, we have

$$(f_r^*v_1, f_r^*v_2) = q^r(v_1, v_2)$$

Now let $\delta = w + w'$ where $w \in W$ and $w' \in W'$. Consdier $(\delta, \alpha_1) = 1 = (\delta, \alpha_2)$ by the fact that $\Delta \cap (X \times \{x_0\}) = \{x_0\} \times \{x_0\}$. Thus we have that $w = \alpha_1 + \alpha_2$. We compute:

$$N_r(X) = \gamma \cdot \delta = f_r^*\delta \cdot \delta = (f_r^*(\alpha_1 + \alpha_2 + w'), \alpha_1 + \alpha_2 + w')$$

Recall that by construction $(\alpha_1, \alpha_2) = 0 = (W, W')$. Thus we have

$$N_r(X) = (f_r^*(\alpha_1 + \alpha_2 + w'), \alpha_1 + \alpha_2 + w') = (f_r^*\alpha_1, \alpha_2) + (f_r^*\alpha_2, \alpha_1) + (f_r^*w', w') = q^r + 1 + (f_r^*w', w')$$

Now, we may apply Cauchy-Schwarz because $W' \subset V_-$ is negative definite to get

$$(f_r^*w', w') \leq \sqrt{(f_r^*w', f_r^*w')(w', w')} = q^{\frac{r}{2}}(w', w')$$

But $(w', w') = C$ is a constant independent of r so the result follows. ■

With the asymptotics out of the way, the remainder of the proof is both elementary and beautiful.

3.3 The Zeta Function on a Variety and the Hasse-Weil Bound

We will introduce the concept of the ζ-function on a variety and do some computations with this function, highlighting some analogies with the ζ-function in number theory. Because we are working on curves, our intersection theory becomes much more classical. We refer to D a divisor as an element of A^1X, where X is a smooth curve of genus g defined over $\mathbb{F}_q$ and base-changed up to $\overline{\mathbb{F}}_1$ as in the previous section. We say that a divisor is *effective* if the coefficients on every prime divisor are nonnegative. Note that because $\deg \operatorname{div}(r) = 0$ the property of being effecctive descends from Z_0X to $A_0X = A^1X$. We define:

Definition 54. For $s \in \mathbb{C}$, $\operatorname{Re}(s) > 1$, we define

$$\zeta(X, s) = \sum_{D \text{ effective}} \operatorname{Nm}(D)^{-s}$$

where $\operatorname{Nm}(D) = q^{\deg D}$

We note that if $D = \sum a_iP_i$ with the P_i prime, then $N(D) = \prod N(P_i)^{a_i}$ and we see that $N(P_i) = q^{[K(P_i):\mathbb{F}_q]}$. We ignore such issues as convergence in this talk for the sake of brevity. For those familiar with number theory, this definition should not seem so unmotivated. In fact, we might think it as a natural analog to the Dedekin ζ-function of a number field. Much like the Dedekind ζ-function, our geometric version admits a product expansion:

Proposition 55. *For* $\operatorname{Re}(s) > 1$*, we have the equality*

$$\zeta(X,s) = \prod_{P \text{ prime}} (1 - \operatorname{Nm}(P)^{-s})^{-1}$$

with the product on the right converging absolutely (and thus independently of ordering).

Proof. Fix some large $N > 0$. Then we have

$$\prod_{\operatorname{Nm}(P) \leq N} (1 - \operatorname{Nm} P^{-s})^{-1} = \prod_{\operatorname{Nm} P \leq N} (\sum_{n=0}^{\infty} \operatorname{Nm} P^{-ns}) = \sum_{\operatorname{Nm} D \leq N} \operatorname{Nm} D^{-s} + \sum_{\operatorname{Nm} D > N}{}' \operatorname{Nm} D^{-s}$$

Where the primed sum means that we are summing over all $D = \sum a_P \cdot P$ such that $a_P = 0$ if $\operatorname{Nm} P > N$. Thus we have

$$|\prod_{P} (1 - \operatorname{Nm} P^{-s})^{-1} - \sum_{\operatorname{Nm} D \leq N} \operatorname{Nm} D^{-s}| \leq \sum_{\operatorname{Nm} D > N}{}' \operatorname{Nm} D^{-\operatorname{Re}(s)}$$

Letting $N \to \infty$ yields the result because the term on the right must vanish by the convergence of $\zeta(X,s)$. Absolute convergence follows from

$$|\sum_{n=0}^{\infty} \operatorname{Nm} D^{-s}| \leq \sum_{n=0}^{\infty} \operatorname{Nm} D^{-n \operatorname{Re}(s)}$$

■

To further develop the analogues between the ζ-functions, a natural next step is to find a a way to extend ζ beyond the positive half plane; as of now, ζ is only defined for $\operatorname{Re} s > 1$. To do this we rely on the following proposition:

Proposition 56. *For* $\operatorname{Re} s > 1$*, there exists a polynomial* f *of degree* $2g$ *with leading coefficient* q^g *and constant coefficient* 1 *such that*

$$\zeta(X,s) = \frac{f(q^{-s})}{(1 - q^{-s})(1 - q^{1-s})}$$

As such, we may extend $\zeta(X,s)$ *to a meromorphic function on* $\mathbb{C}$.

Proof. By doing casework on $g = 0$, $g = 1$ and $g > 1$, and a truly disgusting computation, we may reduce the statement to the following claim. Let d be the minimal degree of an effective, rational (over $\mathbb{F}_q$) divisor. Then we have the following result for $\operatorname{Re} s > 1$. Let $\widetilde{f}$ be a polynomial of degree at most $2g - 2$ and let $\operatorname{Pic}^0 X$ be the subgroup of divisors of degree 0. Then

$$\zeta(X,s) = \widetilde{f}(q^{-s}) + \frac{|\operatorname{Pic}^0 X|}{q - q}(\frac{q^{1-g+(1-s)\max(0,2g-2+d)}}{1 - q^{d(1-s)}} - \frac{1}{1 - q^{-ds}})$$

This claim is a consequence of casework on the possible values $\ell(D)$ for D a divisor using Riemann-Roch. We leave the (also incredibly disgusting) details to the enthusiastic and masochistic reader. ■

We may continue following in the theory of ζ-functions in number theory. The next step in most introductory courses in number theory is to find a functional equation that expresses a symmetry in the complex plane. We have the same thing here:

Theorem 57. *We have the following functional equation for* $s \in \mathbb{C}$*:*

$$q^{(g-1)(2s-1)}\zeta(X,s) = \zeta(X, 1-s)$$

Proof. The functional equation in the case $g \in \{0, 1\}$ is a simple computation using the form of $\zeta(X, s)$ in Proposition 56. Suppose $g \geq 2$ and let $\zeta(X, s) = \zeta_1(X, s) + \zeta_2(X, s)$ where

$$\zeta_1(X, s) = \frac{1}{q-1} \sum_{1 \leq \deg D < 2g-2} q^{\ell(D) - s \deg D}$$

$$\zeta_2(X, s) = 1 + q^{-(g-1)(2s-1)} + \frac{h}{q-1}(1 + q^{-(g-1)(2s-1)} \frac{q^{g-(2g-1)s}}{1 - q^{1-s}} - \frac{1}{q^{1-s}})$$

where $h = |\operatorname{Pic}^0(X)|$. The fact that

$$\zeta_2(X, 1-s) = q^{(g-1)(2s-1)} \zeta_2(X, s)$$

is an easy computation. Thus it suffices to show that ζ_1 satisfies the same. Let $\rho(D) = \ell(D) - \frac{1}{2} \deg D$. Then we have

$$\zeta_1(X, s) = \frac{1}{q-1} \sum_{1 \leq \deg D < 2g-2} q^{\rho(D) - (s - \frac{1}{2}) \deg D}$$

We have

$$\begin{aligned} \rho(K - D) = \ell(K - D) - \frac{1}{2} \deg(K - D) = \ell(K - D) + 1 - g + \frac{1}{2} \deg D \\ = \ell(D) - \frac{1}{2} \deg D = \rho(D) \end{aligned}$$

by Riemann-Roch. Note also that $\deg(K - D) = 2g - 2 - \deg D$ so

$$\{D | 1 \leq \deg D < 2g - 2\} = \{D | 1 \leq \deg(K - D) < 2g - 2\}$$

Thus we have

$$\begin{aligned} \zeta_1(X, s) = \frac{1}{q-1} \sum_{1 \leq \deg(K-D) < 2g-2} q^{\rho(K-D) - (s - \frac{1}{2})(2g - 2 \deg D)} = \frac{1}{q-1} \sum_{1 \leq \deg D < 2g-2} q^{\rho(D) - (s - \frac{1}{2})(2g - 2 - \deg D)} \\ = q^{(g-1)(2s-1)} \frac{1}{q-1} \sum_{1 \leq \deg D < 2g-2} q^{\rho(D) - (s - \frac{1}{2}) \deg D} = q^{(g-1)(2s-1)} \zeta_1(X, s) \end{aligned}$$

Thus the functional equation holds. ■

We have now introduced a geometric ζ-function with clear analogues to the ones in number theory, but it is not at all clear how this relates to our original question about point counting. To do this we will need to recast the ζ-function into a slightly different form. Let $Z(X, t) = \zeta(X, s)$ with $t = q^{-s}$. Then we have from Proposition 56 that

$$Z(X, t) = \frac{f(t)}{(1 - qt)(1 - t)}$$

and so Z is meromorphic on the complex plane. We have from Theorem 57 that

$$Z(X, \frac{1}{qt}) = q^{1-g} t^{2-2g} Z(X, t)$$

The reason for putting the ζ function in this form is that it allows us to bring point counting into the picture:

Theorem 58. *For $|t| < q^{-1}$ we have*

$$Z(X, t) = \exp(\sum_{i=0}^{\infty} \frac{N_i(X)}{i} t^i)$$

Proof. Note first that $|t| < q^{-1}$ is the same thing as saying $\mathrm{Re}(s) > 1$. Thus by Proposition 55 we have

$$Z(X,t) = \zeta(X,s) = \prod_P (1 - \mathrm{Nm}\, P^{-s})^{-1} = \prod_P (1 - q^{-s\deg P})^{-1} = \prod_P (1 - t^{\deg P})^{-1}$$

Now we apply the logarithm and, manipulating as formal power series,

$$\log Z(X,t) = -\sum_P \log(1 - t^{\deg P}) = \sum_P \sum_{m=1}^{\infty} \frac{t^{m \deg P}}{m}$$

$$= \sum_{m=0}^{\infty} (\sum_{m \deg P = i} \frac{1}{m}) t^i = \sum_{i=1}^{\infty} (\sum_{\deg P | i} \deg P) \frac{t^i}{i} = \sum_{i=0}^{\infty} \frac{N_i^*}{i} t^i$$

Where

$$N_i^* = \sum_{\deg P | i} \deg P$$

Thus it suffices to show that $N_i^* = N_i(X)$. Note that points in $X(\mathbb{F}_{q^i})$ can be placed under an equivalence relation with two points equivalent if and only if they lie over points of $X(k)$ and we have $\deg P$ points in each equivalence class. Note that such points correspond to effective k-rational divisors P. Thus we have

$$N_i(X) = \sum_{P \in S} \deg P$$

where S is a set of representatives of the aforementioned equivalence classes. It will suffice to show that such a point corresponds to an effective divisor if and only if $\deg P | i$. Let P be a divisor in $\overline{k}$ and let x be a component of the same. Then P is a $\mathbb{F}_{q^i}$-rational if and only if $k \subset k(P) \subset \mathbb{F}_{q^i}$ which happens if and only if $[k(P) : k] | i$. But this index is just $\deg P$ so we are done. ■

Now we are getting close to finally proving our desired result. We need one more lemma before we can do this, though. Recall from Proposition 56 that f is a polynomial of degree $2g$ over $\mathbb{C}$. We may then factor it as

$$f(t) = \prod_{i=1}^{2g} (1 - \omega_i t)$$

with ω_i^{-1} being the zeros. We have the following result:

Proposition 59. *With the ω_i as above, we have the following relation*

$$N_r(X) = q^r + 1 - \sum_{i=1}^{2g} \omega_i^r$$

Proof. For brevity we introduce the notation $N_r = N_r(X)$. We have from Theorem 58 and Proposition 56 that

$$\exp(\sum_{r=0}^{\infty} \frac{N_r}{r} t^r) = \frac{\prod_{i=1}^{2g} (1 - \omega_i t)}{(1-t)(1-qt)}$$

Taking the logarithm of both sides yields

$$\sum_{r=0}^{\infty} \frac{N_r}{r} t^r = -\log(1-t) - \log(1-qt) + \sum_{i=1}^{2g} \log(1 - \omega_i t)$$

Taking the derivative of both sides yields

$$\sum_{r=1}^{\infty} N_r t^{r-1} = \frac{1}{1-t} + \frac{q}{1-qt} - \sum_{i=0}^{2g} \frac{\omega_i}{1 - \omega_i t}$$

$$= \sum_{r=0}^{\infty} t^r + q^{r+1} t^r - (\sum_{i=1}^{2g} \omega_i^{r+1}) t^r = \sum_{r=1}^{\infty} (q^r + 1 - \sum_{i=1}^{2g} \omega_i) t^{r-1}$$

Comparing coefficients yields the result. ■

Finally, we are ready to prove the main result of this section.

Theorem 60 (Hasse-Weil)**.** *Let X be a smooth projective curve over $\mathbb{F}_q$ of genus g. Then*

$$|N_r(X) - q^r - 1| \leq 2gq^{\frac{r}{2}}$$

Proof. As in Proposition 59, we write N_r for $N_r(X)$. By Proposition 59 we have $|N_r - q^r - 1| = |\sum_{i=1}^{2g} \omega_i^r| \leq \sum_{i=1}^{2g} |\omega_i^r|$. We will show that all of the zeroes of $Z(X,t)$ must lie on the circle $|t| = q^{-\frac{1}{2}}$. Then the right hand side of the above becomes $2gq^{\frac{v}{2}}$ because the zeroes of $Z(X,t)$ are exactly the ω_i^{-1} and so we will be done. Note that Theorem 53 gives us that for $|t| < \frac{1}{2}$ we have

$$\sum_{r=0}^{\infty}(N_r - q^r - 1)t^r < \infty$$

Indeed the coefficients grow like $O(q^{\frac{r}{2}})$ and so for $|t| < q^{-\frac{1}{2}}$, we have that the series is bounded above by a constant times a geometric series with common ratio $|q^{\frac{1}{2}}t| < 1$. Note that Proposition 59 gives

$$\frac{Z'(X,t)}{Z(X,t)} - \frac{q}{1-qt} - \frac{1}{1-t} = \sum_{r=0}^{\infty}(N_r - q^r - 1)t^r$$

by differentiating the logarithm and applying Theorem 58. The right hand side converges for all $|t| < q^{-\frac{1}{2}}$ so $Z(X,t)$ cannot have any zeroes in this region by the left hand side converging. Now we can apply Theorem 57 and note that we can have no zeroes of $Z(X,t)$ for $|t| > q^{-\frac{1}{2}}$ either. Thus all the zeroes appear on the circle $|t| = q^{-\frac{1}{2}}$ as desired and we are done. ∎

One natural way to interpret this result is relative to the line. We know that the number of points in $\mathbb{P}^1_{\mathbb{F}_{q^r}}$ is just $q^r + 1$. We can see this from an elementary counting argument or from Theorem 60 applied to the case $g = 0$. Then Theorem 60 is bounding the deviation from the projective line. This makes some sort of intuitive sense: as the genus gets bigger, the curve looks less and less like $\mathbb{P}^1$. We can use the above calculation to actually compute $Z(\mathbb{P}^1, t)$. We have $N_r(\mathbb{P}^1) = q^r + 1$ and thus

$$Z(\mathbb{P}^1, t) = \exp(\sum_r \frac{q^r+1}{r} t^r) = \frac{1}{(1-t)(1-qt)}$$

Our result leads naturally into a series of conjectures called the Weil conjectures that dominated much of twentieth century algebraic geometry.

References

[EH] David Eisenbud and Joe Harris. *3264 and All That.*

[Fula] William Fulton. *Intersection Theory.* 2nd edition.

[Fulb] William Fulton. *Introduction to Intersection Theory in Algebraic Geometry.* Conference Board of the Mathematical Sciences. American Mathematical Society.

[Fulc] William Fulton. *Young Tableaux with Applications to Representation Theory and Geometry.*

[Har] Robin Hartshorne. *Algebraic Geometry.*

[Was] Lawrence Washington. *Introduction to Cyclotomic Fields.*