We consider the problem of finding the rational points on a plane curve \( \Gamma \), given by \( F(x_1, x_2, x_3) \in k[x_1, x_2, x_3] \). The most interesting fields are \( k \), the \( \mathbb{Q} \), \( \mathbb{Q}_p \), \( \mathbb{R} \), \( \mathbb{C} \) (and possibly function fields). 

If \( F \) is linear, \( a_1 x_1 + a_2 x_2 + a_3 x_3, a_i \in k \), we get a line, \( \Gamma_k \).

If \( a_1 \neq 0 \), letting \( x = \frac{z_1}{z_3}, y = \frac{z_2}{z_3} \), we obtain \( x = -\frac{a_2}{a_1}, y = \frac{a_3}{a_1} \). \( y \in \mathbb{K} \cup \mathbb{Q}_p \). Here the line is parametrized by \( k \cup \mathbb{Q}_p \).

If \( F \) is quadratic and irreducible, and \( \Gamma : F = 0 \) has one \( k \)-rational point, then \( \Gamma_k \) is our \( k \)-line again (rationally).

For \( z_1^2 + z_2^2 = z_3^2 \), \( x^2 + y^2 = 1 \),

\[ x = \frac{1-t^2}{1+t^2}, \quad y = \frac{2t}{1+t^2}, \quad t = \frac{y}{x+1}. \]

Now take \( F \) an irreducible cubic. Here there is at most one double point.

\[ y^2 = x^2(x-1) \quad \text{(tangents)} \quad y^2 = x^3. \]

The coordinates of a singular point are equal to their conjugates, and using separability, lie in \( k \).
Now take $F$ cubic irreducible, nonsingular.

Does $F$ have a rational point? There is no decision procedure for finding rational points if $k = \mathbb{Q}$.

Example: (Selmer) $3z_1^3 + 4z_2^3 + 5z_3^3 = 0$. There are $\mathbb{Q}_p$-valued points for all $p$, but no $\mathbb{Q}$-valued point.

If there is a rational point, Mordell's Th. says that for $k = \mathbb{Q}$, the rational points are finitely generated, i.e., there is a finite set of them so that by drawing tangents, and taking residual interactions of the curve with lines, all rational points can be obtained from these.

Fix a rational point $O$, a flex.

The group $\Gamma$ of rational points is obtained as follows:

Define $\Gamma \times \Gamma \to \Gamma, \; P, Q \to P + Q$.

We claim there is a unique rational point $R$, s.t. $(P) + (Q) \sim (R) + (O)$. Since $P$ and $Q$ are rational, so is $S$. But then since $O$ is rational, so is $R$. \( \text{Eqs.} \) also the form for $L_i, \; i \in \{1, 2\}$, and $P = P_i$. Then $(P) + (Q) = (R) + (O) + (P) \sim (R) + (O)$, or $(R) \sim (P) + (Q) - (O)$.

Now $F$ has genus 1, and given any divisor of degree 1 there is a unique pos. divisor linearly equivalent to it, i.e., in the words $K = P + Q$ is characterized by $P, Q,$ and $O$.  

Riemann-Roch implies in each divisor class of degree 1, there is just one effective divisor, a point. Thus, \( P \mapsto \text{Class of } (P) - (0) \) gives a 1:1 correspondence between points and divisor classes of degree 1. Thus \( P_k \) is a commutative group, and Mordell's Theorem says that for \( k = \mathbb{Q} \), \( P_k \) is finitely generated. The proof is non-constructive.

There are some theorems obtainable by analytic methods over \( \mathbb{Q} \).

Also, over \( \mathbb{Q} \), there is the rank problem. The highest known rank is 5, and it is unknown whether there is a bound on the ranks.

(If \( 0 \) is a point of reflection, \( P_1 + P_2 + \cdots + P_m = 0 \) if and only if \( (P_1) + (P_2) + \cdots + (P_m) = \Gamma \cdot C_m \).)

Fix a nonsingular curve, \( A \), complete and of genus \( 1 \), defined over \( k \). Then \( A \) has a nonsing. proj. model defined over \( k \). The genus is 1 in the good sense, i.e., \( A \) has genus 1 over \( k \). Evidently, \( \text{Pic} \) gives a projective embedding \( A \hookrightarrow \mathbb{P}^3 \), if \( 0 \) is a fixed rational point of \( A \), so \( A \) is defined by an equation \( F(x, y) = 0 \)

<table>
<thead>
<tr>
<th>( n )</th>
<th>Basis for ( H^0(A, \mathcal{L}(nD)) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1, ( x ) ( x ) must have a pole of order 2</td>
</tr>
<tr>
<td>3</td>
<td>1, ( x ), ( y )</td>
</tr>
<tr>
<td>4</td>
<td>1, ( x ), ( x^*, y )</td>
</tr>
<tr>
<td>5</td>
<td>1, ( x ), ( x^* ), ( xy ), ( y )</td>
</tr>
<tr>
<td>6</td>
<td>1, ( x ), ( x^* ), ( xy ), ( y ), ( x^3 ), ( y^2 ).</td>
</tr>
</tbody>
</table>
Hence in \( H^0(A, \mathcal{L}(6D)) \), we obtain a relation, which we can actually take as

\[
F(x, y) = y^2 + a_1xy + a_0y + x^3 + a_2x^2 + a_4x + a_6 = 0.
\]
\(a_i \in k\).

Now if the characteristic of \( k \neq 2 \), and \( Y = -2y + a_1x + a_3 = F_y(x, y) \).

\(X = -x\), and obtain: \(Y^2 = 4X^5 + \beta_2X^2 + 2\beta_4X + \beta_6 - 4(X - x)(X - x_2)(X - x_3)(X - x_4)(X - x_5)\).

If char \( k \neq 2,5\), and \( \beta_2 = \frac{\beta_3}{12} + X \), \( \beta_4 = 1 + X \), and give the Weierstrass

form \(4\beta_3 - \beta_2\beta_4 - \beta_6 = \beta_4^2 = 4(\beta_2 - \beta_4)(\beta_2 - \beta_6)(\beta_2 - \beta_8)\).

Where:

\[
\begin{align*}
\beta_2 &= a_4^2 - 4a_6 \\
\beta_4 &= 2a_4 - a_1a_3 \\
\beta_6 &= a_3^2 - 4a_4 \\
\beta_8 &= a_4^2 - a_1a_3a_4 + a_4^2a_6 + a_5a_6^2 - 4a_4a_6 \\
(4\beta_6 &= \beta_2^2 - \beta_8, \text{ so } \beta_8 \text{ is redundant in } \beta_2a_2 + 2.)
\end{align*}
\]

\[
\begin{align*}
\gamma_4 &= \beta_2^2 - 24\beta_4 = 12\beta_2 \\
\gamma_6 &= \beta_2^3 - 3\beta_2\beta_4 + 216\beta_6 = -216\beta_6 \\
\Delta &= \beta_2^2\beta_4 - 8\beta_4^2 - 27\beta_6^2 + 9\beta_2\beta_4\beta_6 - \beta_4^2 - 27\beta_5^2 \\
&= 16(X_1 - x_2)(X_1 - x_3)(X_1 - x_4)(X_1 - x_5)^2 \\
&= 16(e_1 - e_2)^2(e_1 - e_3)^2(e_2 - e_3)^2 \\
J &= \frac{\gamma_5^3}{\Delta} = \frac{1728\beta_6^3}{\Delta} = 1728J.
\end{align*}
\]

If \( A' : F'(x', y') = y'^2 + a'_1x'y' + a'_0y' + x'^3 + a'_2x'^2 + a'_4x' + a'_6 = 0 \).

is another curve of the same form, then an isom. \( \phi : A' \cong A \), over \( k \).

i. e. \( \phi(0') = 0 \), will be of the form \( x \circ \phi = \rho^2 x' + r \), \( y \circ \phi = \rho^3y' + \rho^3ax' + t \), \( \rho, a, t, \rho \in k \), \( \rho \neq 0 \). Then \( \rho^{-2}F(x, y) = F'(x', y') \), and
\[ \rho a' = a_1 + 2a \]
\[ \rho a' = a_2 + 2a_1 + 5z + S^2. \]
\[ \rho a' = a_3 + 2a_1 + 2t = F_y(z, t) \]
\[ \rho a' = a_4 + 2a_3 + 2a_4 + t\alpha + 2a_4 + 3z^2 + 2zt = aF_y(z, t) + F_z(z, t) \]
\[ \rho a' = a_5 + 2a_4 + 2a_5 + t\alpha + 2a_5 + t^2 = F(z, t). \]
\[ \rho a_2' = \beta_2 - 12z \]
\[ \rho a_4' = \beta_4 + 2\beta_2 + 6z^2 \]
\[ \rho a_6' = \beta_6 - 2\beta_4 + 2\beta_2 - 4z^3 \]
\[ \rho a_8' = \beta_8 + 3\beta_6 - 3\beta_4 + 3\beta_2 - 3z^4 \]

To compute the discriminant, note that \( D \) is the only \( \rho \) at \( \infty \) and
\( x \) at that place \( \rho \) vanishes. In fact \( D \) is an infinite point and
the tangent to the line of \( x \). \( D \) is a simple \( \rho \) of the projective
model. Of \( \rho = 3 \), we have
\( Y^2 = 4f(X) = 4(X-X_1)(X-X_2)(X-X_3) \).
As a singularity, \( Y \) and \( f(X) \) must vanish, i.e., \( Y = f(X) \cdot f'(X) \).
So \( D \) is non-singular \( \iff \Delta \neq 0 \).
Of \( \rho = 2 \), the same condition holds.
\[ F_x = ay + ax + a_2 = a_1 + ax + a_2 \]
\[ F_y = ay + 3ax^2 + 2ax + ay = a_3 + 3ax^2 + ay \]
Case 1: \( a_1 = 0 \): non-sing \( \iff a_3 \neq 0 \)
* 2: \( a_1 \neq 0 \): solve for \( x, y \) in terms of \( a_1, a_2 \).

In the classical case, given such an eqn with \( D \neq 0 \), can find a
lattice in \( C \), such that the doubly periodic functions form a
field generated by \( 
\omega_1 \) and \( \omega_2 \), satisfying the relation given
on last page with given \( g_0 \) and \( g_3 \).
\[ \frac{\omega_1}{\omega_2} = 2, \] and \( \omega_2 \) is the elliptic modulus for. Thus if
2 elliptic function fields are isomorphic, they have the same \( j \) and conversely.....

Of course, given 2 elliptic curves \( A, A' \), suppose \( j = j' \). Is there a transformation carrying one into the other? Yes, if \( k \) is algebraically closed! (any characteristic.)

If \( p \neq 3, 3 \) reduce the curve to the form: \( y^2 = 4x^3 - G_2x - G_3. \) Then the only allowable transformations on \( x \) and \( y \) are \( x = p^2x', \ y = p^3y', \ p \neq 0, \) so \( G_2 = p^4G_2', \ G_3 = p^6G_3'. \) and

\[
j = \frac{1728 G_2^3}{G_2^3 - 27 G_3^2}
\]

Case 1: \( j \neq 0, 1728. \) Then \( j^{-1} - 1728 = \frac{G_2^3}{G_2^3 - 27 G_3^2}. \) Taking the transformation: \( p = \pm \sqrt[3]{\frac{G_2^3}{G_2^3 - 27 G_3^2}}, \) we can go from one curve to the other. \( j^{-1} = j'. \) [Because we can take the curve:

\[
A: \ y^2 = 4x^3 - 3c^2 \frac{j}{j - 1728} x - c^2 \frac{j}{j - 1728} \quad c \in k^*, \ \mod k^2,
\]

given any \( j \in k, \) there is an elliptic curve over \( k \) having \( j \) as its invariant.]

Case 2: \( j = 1728. \) \( G_2 = 0, \) gives

\[
y^2 = 4x^3 - cx \quad c \in k^*
\]

Case 3: \( j = 0, \) \( G_3 = 0, \) \( y^2 = 4x^3 - c \)

Case 1: Automorphisms are \( p = \pm 1 \)

Case 2: \( \quad p^4 = 1 \)

Case 3: \( \quad p^6 = 1. \)

Case \( p = 3 \) is an exercise!
\[ p = 2, \quad y^2 + a_1 xy + a_2 y + x^3 + a_3 x^2 + a_4 x + a_6 = 0. \]

\[ \rho a_1' = a_1; \quad (a_1 \neq 0 \text{ is intrinsic}) \]

**Case 1:** \( a_1 \neq 0 \). Can get \( a_1 = 1 \) and thus \( f \) is even \( f = 0 \).

\[ \rho^3 a_2' = a_3 + \rho a_1. \quad a_3 = 0 \text{ for } x = 0, \quad \text{and } a_4 = 0 \text{ for } t = 0 \text{ from here on. Thus we have the form:} \]

\[ y^2 + xy = x^3 + a_2 x^2 + a_6. \]

The only possible transformations are with \( s \) : \( X = X', \quad y = y' + s x \).

What is \( \Delta \) and what is \( j \)?

\[ \beta_2 = 1; \quad \beta_4 = \beta_6 = 0; \quad \beta_3 = a_6; \quad y_4 = 1; \quad \Delta = a_2, \quad \text{and } j = \frac{1}{a_2}. \]

\[ a_6 \neq 0 \quad (a_1 \neq 0 \iff j \neq 0), \text{ so we get} \]

\[ y^2 + xy = x^3 + a_2 x^2 + j. \]

\[ a_6' = a_2 + s^2. \quad f(s) = s^2 + s. \quad f(a_2 + s) = f(s) + f(a_2). \]

(a even, \( a_2 \mod f(k^+) \)).

Automorphism are given by \( s = 0, 1 \). Cycle of order 2.

**Case 2:** \( a_1 = 0 \), i.e., \( j = 0 \).

Using \( r \), make \( a_2 = 0 \), which fixes \( r = a_2 \).

The remaining cases are:

\[ \rho^3 a_6' = a_6 \]

\[ \rho^3 a_4' = a_4 + a_2 a_3 + a_6 \]

\[ \rho^3 a_6' = a_6 + a_2^2 a_4 + t a_2 + s^2 + t^2 \]

Thus we get:

\[ y^2 + a_2 y + x^3 + a_4 x + a_6 = 0, \]

\[ \Delta = a_2^3, \quad j = 0, \quad (a_3 \neq 0). \]

In fact one gets \( y^2 + y = x^3 \) over a separable extension of degree \( \leq 24 \).

\[ \rho^3 = 1, \quad \text{3 possibilities for } \rho \]

\[ 0 = a + s^2 \quad 4 \text{ for } a, \quad (24 \text{ is the order of the group}). \]

\[ 0 = t + t^2 + s^6, \quad 2 \text{ for } t. \]

\( \rho, a, t \) generate the group. \( (1, a, t) \) generates a subgroup of index 5.
which must be the quaternion group since it can only have elements of order 2.
Take \((\mathbb{Z}/3\mathbb{Z}) \times G_2\) where,

\[(a \times q)(b \times q') = (ab \times q b') (1 + q_2) = ab \cdot q_1 \cdot q_2.
\]

Now \(y^2 + xy = x^5 - \frac{36}{j-1728} x - \frac{4}{j-1728}, \quad \Delta = \frac{j^2}{j-1728}\)
makes sense for all \(p\) if \(j \neq 1728\), and \(\Delta \neq 0\) if \(j \neq 0\),
so has invariant \(j\) for all \(p\).

Over algebraically closed fields, \(j\) is a modulus for these curves.

**Explicit formulas for addition of points.**

\[A : F(x,y) = y^2 + a_1 xy + a_3 y + x^5 + a_2 x^3 + a_4 x + a_6 = 0.\]

\[\Delta \neq 0, \quad a_i \in k.\]

\[A_k = A_k \cup \{(0,0)\}, \quad 0 = (\pm \infty), \quad A'_k = \{(x,y) : x, y \in k \}^2.\]

\[0 + P = P + 0 = P\]

Suppose \(P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in A'_k.\)

\[P_1 + P_2 + P_3 = 0, \quad \text{since they are collinear}.
\]

\[L\] is the line through \(P_1\) and \(P_2\).

\((y P_1 - P_2, L\) is the tangent to \(A\).

\[\sigma = F(x, y) - F(x, y) = (y_1 - y_2)(y_1 y_2 + a_3 x_1 + a_4) + (x_1 - x_2).
\]

\[
\frac{y_1 - y_2}{x_1 - x_2} = \lambda = \frac{x_1^2 + x_1 x_2 + a_3 (x_1 + x_2) + a_4 y_1 + a_6}{(y_1 + y_2 + a_3 x_1 + a_4)}.
\]

\[(x^2 + x_1 x_2 + a_3 (x_1 + x_2) + a_4 y_1 + a_6) = \frac{y_1 - y_2}{x_1 - x_2}.
\]
If neither denominator vanishes, i.e., \( x_1 - x_2 \) and \( y_1 + y_2 + a_1 x_1 + a_2 = 0 \) then \( y_1 - y_2 \), i.e., \( \overline{p_1} = \overline{p_2} \), and in such cases, \( y_1 + y_2 + a_1 x_1 + a_2 = F_x(x_1, y_1) \), and the numerator is \( F_x(x_1, y_1) \), so \( \lambda = \frac{F_x}{F_y} = \) slope of line.

If \( x_1 = x_2 \), and \( y_1 + y_2 + a_1 x_1 + a_2 = 0 \), then \( \lambda \) is parallel to \( y \)-axis.

i.e., \( \lambda = \frac{0}{x_1 - x_2} \), \( \lambda = \frac{y_1 - y_2}{x_1 - x_2} \).

If \( \overline{p_1} + \overline{p_2} \neq \overline{0} \), i.e., \( y_1 + y_2 + a_1 x_1 + a_2 = 0 \), then \( \lambda \) has eqn \( y = \lambda x + \mu \). Let \( \mu = y_1 - \lambda x_1 = y_2 - \lambda x_2 \). To find the 3rd intersection:

\[
0 = F(x_1 + \lambda y + v) = x_1^2 + (a_1 + a_2 + \lambda + \mu)v + (\cdots) x + (a_1 + a_2 y + \lambda v).
\]

Let \( x_1 + x_2 + x_3 = \lambda x_1 - a_2 - a_1 \lambda - \lambda v \), permitting \( \lambda \) to solve for \( x_3 \), and \( y_3 = \lambda x_3 + v \) giving \( \overline{p_3} = \overline{-(p_1 + p_2)} \).

Now suppose \( D \) is a valuation ring with maximal ideal \( \mathfrak{m} \), and fraction field \( \mathbb{K} \), and \( \mathbb{K} = \mathbb{Q}/\mathfrak{m} \). Suppose \( A \in D \), i.e., \( F(x, y) \in D[x, y] \).

Given \( A \). Reduce mod \( \mathfrak{m} \) to \( \overline{F}(x, y) \in \mathbb{K}[x, y] \). If \( \Delta \neq 0 \), then \( \Delta \neq 0 \) and \( \overline{F} \) gives an elliptic curve, \( \mathbb{A} \) over \( \mathbb{K} \).

Def: \( A \) has nondegenerate reduction mod \( \mathfrak{m} \) iff. \( \Delta \neq 0 \) (\( A \in Cl(D) \)).

The point is: if we have 2 curves, \( A, A' \), each having a model with nondegenerate reduction mod \( \mathfrak{m} \), and if \( A \) is birationally equivalent to \( A' \) over \( \mathbb{K} \), then \( \mathbb{A} \) is birationally equivalent to \( \overline{A'} \) over \( \mathbb{K} \).

If \( A = \mathbb{A} \), then there is a transformation of type \( r, s, t \) in \( \mathbb{K} \) \( \rho \neq 0 \), s.t. the 5 eqns.: \( \rho a_1 = a_1 + 2 \alpha \), etc., holds, where \((\alpha)\) are coeff's for \( A \), \((\alpha')\) coeff's for \( A' \). To show \( \rho, s, t \in \mathbb{Q}, \rho \neq 0 \). But \( \rho^2 \Delta = \Delta \), so \( \rho \in \mathbb{Q}^* \), and \( \rho \) makes sense. But the 5 eqns.

show that \( r, s, t \) are integral over \( \mathbb{Q} \), so \( \mathbb{A} \). Thus, \( \mathbb{A} \neq \mathbb{A} \).
Now assume that \( a \in \mathbb{C} \) but not zero. \( \Delta \neq 0 \). From the equ., \( x \in \mathbb{C} \iff y \in \mathbb{C} \), so if \( x \notin \mathbb{C} \), \( |x|^2 = 1 |y|^2 \). These should be the points near the origin 0.

\( \frac{x}{y} \in \mathbb{C} \), \( y \in \mathbb{C} \), and also, in fact \( \frac{x}{y} \in \mathbb{C} \), i.e., \( |x|^2 = \frac{1}{|y|^2} = \frac{1}{y} \), \( (x \notin \mathbb{C}) \), so letting \( u = \frac{x}{y} \), \( v = \frac{y}{x} \), \( (x \notin \mathbb{C}) \), \( |v|^2 = |\frac{1}{y}| \).

We have the birational transformation: \( y = \frac{1}{v} \), \( x = \frac{u}{v} \).

(Dividing \( 0 = F(x, y) \) by \( y^3 \!). which gives:

\[ C(u, v) = v + a_1 u v + a_2 u^2 v + a_3 u^3 v + a_4 u^4 v^2 + a_5 v^3. \]

\( C \) gives an affine variety, \( A^2 \), and

\[ A^2_k = A^2 \cup A^2_x \quad (\text{disjoint union}) \]

\( 0 \in A^2 \), \( u = 0 \), \( v = 0 \), and \( u \) is a uniformizing parameter for 0.

\[ o = C(u_1, v_1) - C(u_2, v_2), \]

\[ \text{if} \quad \frac{v_1 - v_2}{u_1 - u_2} = \frac{a_1 v_1 + (a_2 u_1 v_1 + a_3 u_1^2 v_1 + a_4 u_1^3 v_1 + a_5 u_1^4 v_1)}{1 + a_1 u_1 + a_2 u_1^2 (v_1 + v_2) + a_3 u_1^3 v_2 (v_1 + v_2) + a_4 u_1^4 v_2^2 (v_1 + v_2) + a_5 u_1^5 v_2^3 (v_1 + v_2)}. \]

For each \( x \in \mathbb{C} \), there is at most one \( (y, z) \in \mathbb{C} \) such that \( (x, y, z) \in A^2 \).

This follows easily since \( 1 + yf \) is a set of units.

\((u, v) \rightarrow u \) gives an injection \( A^2_y \rightarrow \mathbb{C} \), (a bijection when \( k \) is complete (and \( \mathbb{C} \) ?)).

Now stand adding points \( u \in A^2_y \).

If \( P_1, P_2 \in A^2_y \); in such a case, the denominator cannot vanish.

and \( P \in \mathbb{C} \). \( V_i = P \in \mathbb{C} \), so \( V \in \mathbb{C} \) and we get:

\[ u_i + u_2 + u_3 = \frac{a_1 u_1 V_i + a_2 V_i + a_3 V_i^2 + a_4 V_i^3 + a_5 V_i^4}{1 + a_1 u_1 + a_2 u_1^2 + a_3 u_1^3 + a_4 u_1^4 + a_5 u_1^5} \in \mathbb{C}. \]

so \( u_3 \in \mathbb{C} \) and hence \( V \in \mathbb{C} \).

This shows that \( A^2_y \) is a subgroup (at least a subgroup and its corresponding subtractable that \( V P \in A^2_y \), \(-P \in A^2_y \), so \( A^2_y \) is really a subgroup.).
Let $\mathfrak{a}$ be a proper ideal in $\mathcal{O}$, and let $A_\mathfrak{a}'' = \{ (u,v) \in A_\mathfrak{a}^2 : u, v \in \mathfrak{a} \}$. 

First note that $v \mathcal{O} = u_0^2 \mathcal{O}$, so $v \in A_\mathfrak{a}^2$. Note if $P_1, P_2 \in A_\mathfrak{a}$, $P_1 \in A_\mathfrak{a}, P_2 \in A_\mathfrak{a}''$ we have $P_1 + P_2 + u_0 \in A_\mathfrak{a}^2$ in all cases, and

- if $a_1 = 0$, " " $0^2$,
- if $a_1 = 0$, " " $0^4$,
- if $a_1 = a_2 = a_3 = 0$, " " $0^5$.

Thus $(u,v) \mapsto (u)$ gives a homomorphism, $A_\mathfrak{a}'' \to A_\mathfrak{a}/A_\mathfrak{a}^2$, and we have an exact sequence: $\mathcal{O} \to A_\mathfrak{a} \to A_\mathfrak{a}'' \to A_\mathfrak{a}/A_\mathfrak{a}^2$, and there only if $k$ is complete. If the valuation is discrete and $k$ has characteristic $p$, then $A_\mathfrak{a}''$ has no prime-to-$p$ torsion, for we have $A_\mathfrak{a}'' \supset A_\mathfrak{a}^2 \supset A_\mathfrak{a}^{g_2} \supset \cdots$, and the successive quotients are isomorphic to subgroups of $k^*$. 

Proposition: Suppose $\Delta \notin k^2$, then $(x,y) \mapsto (\tilde{x}, \tilde{y})$ gives a homomorphism $A_k \to A_\mathfrak{a}''$, with kernel $A_\mathfrak{a}''$ and the injection $A_k/A_\mathfrak{a}'' \to A_\mathfrak{a}''$ is bijective if $k$ is complete.

Proof: We show $\tilde{P}_1 + \tilde{P}_2 = \tilde{0} \iff P_1 + P_2 \in A_\mathfrak{a}''$. 

But $x_1 + x_2 + x_3 = -a_1 - a_3 \lambda - \lambda^2$. If $P_1, P_2 \in A_\mathfrak{a}$, then $P_3 \in A_\mathfrak{a}''$, 

$\iff \lambda \notin k^2$, $\iff \lambda - a_1 a_3 + a_2 - a_3 \in k$. 

Now we consider the case of nondegenerate reduction, $\tilde{A}_a : y^2 + a_1 yx + a_2 y + x^2 + \cdots \in \tilde{A}$. $A_\mathfrak{a}': y^2 + a_1 yx + a_2 y + x^2 + \cdots \in A_\mathfrak{a}''$. 

we get a homomorphism $A_k \to \tilde{A}_\mathfrak{a}''$, $(\tilde{x}, \tilde{y}) \mapsto (x,y)$ of $(x,y) \mapsto (\tilde{x}, \tilde{y})$ if $x, y \in k$, $(x, y) \mapsto \tilde{0}$.
Now consider the case $\Delta = 0$. We start the discussion anew.

Given $F(x, y) = 0$; $a_1, a_2, a_3, a_4, a_6$ are the coefficients and $\Delta = 0$.

For the form $y^2 + l(x)y + C(x)$, $l(x) = a_1 x + a_3$, $C(x) = x^2 + \ldots$

In any case, $F$ must be irreducible, because if it split, we would have $F = (y + g(x))(y + h(x))$, where $g + h$ is a line, gh a curve!

I claim that by Bezout's Theorem the curve has only one singularity, which can only be a double point. Thus, $\Delta = 0 \Rightarrow \exists (x, t)$ s.t. $F(x, t) = F_1(x, t) = F_2(x, t) = 0$. Such a $x$, so rational.

Now transform by $r = 1, s = 0, z = x, t = t$ to obtain $a_1 = a_3 = a_5 = a_6 = 0$, and the eqn:

$$y^2 + axy + x^3 + a_2x^2 = 0$$

with singularity $\Delta(0, 0)$. To find the tangents, solve

$$a_1^2 + a_1 + a_2 = (a_1 - a_2)(a_1 - 2a_2), \quad (a_1 - a_2)^2 = a_1^2 - 4a_2 = \beta_2.$$ 

Thus we have a node if $\beta_2 > 0$ and a cusp if $\beta_2 < 0$.

Now assume $\lambda_i \in k$. Then setting $s = \lambda$ yields $a_2 = 0$, (as $a_2 = 0$)

Thus $a_2 = 0$ gives a cusp, $a_1 = 1$ a node, respectively.

1. $y^2 + x^3 = 0$.
2. $y^2 + xy + x^3 = 0$.

And $w = x$, as before. $x = y w$

In case 1 we get $1 + y^2 w^3 = 0$; $y = -\frac{1}{w^3}, x = -\frac{1}{w^2}$.

In case 2 we get $y = -\frac{(1 + w)}{w^3}, x = -\frac{(1 + w)}{w^2}$.

In case 3 we include the cases $w = 1, \infty$, and in $O$ we include $w = \infty$. Then in case 1, $O: w = 0$, we get the additive group of $k$, and in case 2, $O: 1 + w = 1$, we get the multiplicative group of $k$.

$$(1 + w)(1 + w) = 0$$
Now using the fact that \( a_2 = a_5 = a_7 = a_9 = 0 \), we have:

\[
\frac{a}{a_1} = \frac{a_2}{a_3} + \left( \frac{a_4}{a_5} \right) a + 0.
\]

So if we have an cusp then reduces to:

\[
\Delta = \Delta \frac{a_2}{a_3} + \left( \frac{a_4}{a_5} \right) a + 0.
\]

If we have a node, \( \Delta = -1 \).

Now choose a model for \( A \), i.e., \((a_1, a_2, a_3, a_4, a_5)\), with \( a_i \in \mathbb{Q} \) and \( 1|A| \) maximal, and \( \Delta \) (\( a_1, \ldots, a_5 \)) be another such model. Give:

\[
\rho, \tau, s, t : a_i \mapsto a_i^\prime \quad and \quad \Delta \text{ changes by a factor} \quad \rho^2 \quad \text{so } l \geq 1
\]

and \( x, s, t \in \mathbb{Q} \) so before, \( \Delta, \rho, \tau, s, t \) make sense, and the transformation can be reduced mod \( q \), and \( \tilde{A} \) and \( \tilde{A}^\prime \) are birational. From now on we always take \( A \tilde{A} \) be a "best" model, i.e., \( 1|A| \) maximal, and \( A_{y} = A_{y}^\prime \). \( A_{y} \) is independent of the "best" model chosen. Similarly we get \( A_{x} = \mathcal{E}(x, y) \); \( \frac{x}{y} \in \mathbb{R} \). Call \( A_y = \mathcal{E}(x, y) \); \( (x, y) \) simple on \( A \tilde{A} ^3 \)

By using:

\[
A_{x} = k^*, \quad A_{y} = 0^*, \quad A_{x} = 1 + y, \quad A_{y} = 1 + 6z, \quad \text{so we have:}
\]

\[A_{x} = 0, A_{y} = 0, A_{x} = 0, \quad \ldots\]

If we have nondegenerate reduction, \( 1|A| = 1 \), and \( \tilde{A} = A_{y}^\prime \). In the case of a general abelian variety, \( A_{x}/A_{y} \equiv ? \) (Wron). We get a hom. from \( A_{y} \) to the complex part of \( \tilde{A}^\prime \). and the sequence:

\[0 \rightarrow A_{y} \rightarrow A_{y} \rightarrow A_{y} \rightarrow \tilde{A}_{y} \text{ is exact - at least after a quadratic extension of } \tilde{k} .\]
Now we consider the case where \( k \) is complete under \( | \cdot | \).

Proposition: If \( k \) is complete, then \( \overline{A_0} \to \overline{A_{0,0}} \) is surj.

Proof: Take a point \( \bar{x} \in \overline{A_{0,0}} \). If \( \bar{x} = \bar{0} \), there is no problem, so assume \( x, y_0 \in \bar{0} \), and \( (x, y_0) \) is a point in \( \overline{A} \). \( F(x, y_0) = \bar{0} \). Either \( |F_x(x, y_0)| = 1 \) or \( |F_y(x, y_0)| = 1 \). If \( |F_x(x, y_0)| = 1 \), consider \( F(x, y_0) \) as an

ign for \( \bar{x} \), and \( x \sim x_0 \) is an approximate root, since \( |F(x, y_0)| < 1 \).

Let \( f(x) = F(x, y_0) \). Then \( f'(x) \) is 1, and \( f(x) \) is surj by Newton's theorem, one gets: \( \exists \) a unique \( x \in \bar{0} \) s.t. \( x = x_0 \) (eg) and \( f(x) = F(x, y_0) \). So every \( (x, y_0) \in \overline{A_{0,0}} \) and \( (x, y_0) - (x_0, y_0) \).

Con: The seq: \( 0 \to A_{0} \to \overline{A_{0}} \to \overline{A_{0,0}} \) is exact if \( k \) is complete.

Connection with Formal Groups.

Use the \( u, v \) notation; just forget \( \mathcal{O} \), use \( k \). \( u \) is a

uniforming parameter of \( \mathcal{O} \), \( \mathcal{O}_{x,0} = k \ll u \ll k \), and \( v = u^2 + B_1 u^3 + B_2 u^5 + \cdots \). \( B_3, \ldots \in k \). Call \( v(u) \). We get \( G(u,v(u)) \) as an identity in \( k \ll u \ll k \), \( w_0 = \mathcal{O}(u, v(u), v(u)v(u)) \)

\( u, \ldots \) is a rational field for addition of pts. Define \( \Phi(w_0, v(u)) = \mathcal{O}(u, v(u), v(u)v(u), v(u)u) \) \( = \mathcal{O}(u, v(u)) \). \( \Phi(0) = v(u) \). The group is an

morphism. \( \Psi(u) \) s.t. \( \Phi(u, \Phi(w_0)) = 0 \). From the additive

\( u, v \) group, we get the formal group, \( \Phi(u, v(u)) = u, v(u) \).

From the multi. group: \( \Phi(u, v(u)) = u, v(u) \).
Now we use the existence of the valuation ring, \( \mathcal{O} \), of \( \mathbb{R} \) in \( \mathcal{O} \), so are the \( B_i \), the coefficients of \( V(u) \), and so are \( c_{ij} \), the entries of \( \Phi(w, w) \). Thus we have a way of describing points \( \mathbb{A}^2 \). For all \( u \in \mathbb{A}^2 \), \( V_i = V(u) \) converges to an element of \( \mathbb{Q} \). \( (u, v) \in \mathbb{A} \).

This gives: \( y \mapsto \mathbb{A}^2 \) (not a home) via \( u \mapsto \mathbb{P}(w) \), with \( P(u) + P(w) = P(w, w) \).

Again, \( \mathcal{O} \) is a valuation ring, with fraction field \( k, \tilde{k} = \mathcal{O}/\mathfrak{g} \). If \( A \) is defined over \( k \). If \( j \in \mathcal{O} \), there exists a model for \( A \) having nondegenerate reduction, but the model is defined over a finite extension \( K \) of \( k \).

Case 1: \( 2 \nmid \mathfrak{g} \): \( y^2 + x(x+1)(x+1) = 0 \).

\[ \Delta = 16 \lambda^3 (1-\lambda)^5 \quad \lambda^2 (1-\lambda)^2 j = 2^8 (1-\lambda + \lambda^3)^3 \]

\[ = 2^8 (1-(1-\lambda^2)) = 2^8 (1-(1-\lambda^2)). \]

Solve for \( \lambda \) and adjoin \( \lambda \) to get \( K = k(\lambda) \).

Case 2: \( 3 \nmid \mathfrak{g} \): \( y^2 + axy + y + x^3 = 0 \).

\[ \Delta = - (27 + a^3) \]

\[ = (a^3 + 27) \alpha^3 + j (27 + a^3) = 0. \]

Solve for \( a \) to get \( K = k(a) \).

\[ \pm 27 \]

N.B., \( \mathfrak{g} \) \( j \in \mathcal{O} \), there exists a model with reduction to an ordinary double \( \mathfrak{p} \) (possibly after a quadratic extension).
General discussion of the case \( j \neq 0 \).

Consider \( C^* \), and take \( g \) s.t. \( 0 < |q| < 1 \). Call the subgroup generated by \( g \), \( \langle g \rangle \). Then \( C^*/\langle g \rangle \) is a compact group, isomorphic to a torus. The forms on this group are all \( f \) defined on \( C^* \) s.t. \( f(q^n) = f(n) \), with \( f \) homomorphic on \( C^* \).

If \( A_g = C^*/\langle g \rangle \), we write \( A = A(g) \). Now assume \( k \)

\( k = \mathbb{C} \) or \( \mathbb{R} \)

\( 0 < |q| < 1 \)

\( 0 \neq q \in \mathbb{C} \).

![Image]

To make \( A = A_g \) s.t. \( A_{k^*} = k^*/\langle g \rangle \)!

\[ f(n) = \sum_{n=-\infty}^{\infty} F(q^n w), \] if this is absolutely convergent, \( f(q^n w) = f(w) \).

Since \( |q| < 1 \), \( q^n w \to 0 \) as \( n \to \infty \), \( q^n w \to \infty \) as \( n \to -\infty \), so \( F \) must be small near 0 and \( \infty \). Take \( F(w) = \frac{w}{(1-w)^a} \), which

\[ x(W) = \sum_{n=-\infty}^{\infty} \frac{q^n w}{(1-q^n w)^2} - 2 \sum_{n=1}^{\infty} \frac{q^n}{(1-q^n)^2} \]

\( x(W) \) is defined for \( W \) not a power of \( q \).

\[ \|F(w)\| = O(1/|w|) \text{ as } |w| \to 0. \]

\[ O(1/|w|) \text{ as } |w| \to \infty \]

\( x \) is a form on \( k^* \) - if allowed to have value \( \infty \) on \( q^2 \), and

\( x \) is actually a form on \( k^*/\langle g \rangle \), as \( x(w) = x(q^n w) \).
Since \( \frac{1}{W+W^{-1}-2} = \frac{1}{N+\frac{1}{W}-2} = \frac{1}{W} \left( \frac{1}{W-1} \right)^2 = \frac{W}{(1-W)^2} \). \( x(W) \) is an
even function of \( W \) in the sense that \( x(W) = x(W^{-1}) \).

\[
x(W) = \frac{W}{(1-W)^2} + \sum_{m=1}^{\infty} \left[ \frac{q^{-m} W}{(1-q^{-m})} + \frac{q^{-m} W^{-1}}{(1-q^{-m})} - \frac{2q^{-m}}{(1-q^{-m})^2} \right] =
\]
\[
\frac{W}{(1-W)^2} + \sum_{m=1}^{\infty} \sum_{n=1}^{\infty} \left( nq^{mn} W^n + nq^{mn} W^{-n} - 2nq^{mn} \right) \quad (1q < 1W < 1q^{-1})
\]
\[
\frac{W}{(1-W)^2} + \sum_{m=1}^{\infty} \left( W^n + W^{-n} - 2 \right) \cdot \frac{nq^{mn}}{1-q^{-m}} \quad (1q < 1W < 1q^{-1})
\]

Consider the case \( k = 0 \). \( x(W) \) is even on \( C^0 \) and has period \( q \). Put
\( W = e^{\pi i} \). Let \( \omega_1 = 2\pi i \), \( \omega_2 = \log q \). For \( z = \frac{\omega_2}{\omega_1} \), \( \log(z) > 0 \).
\( C'/Z \omega_1 + 2Z \omega_2 = C'/q \) by the map.

Claim: \( g(u) = x(W) + \frac{1}{12} \)
\[
\begin{align*}
ge_1 &= \frac{1}{12} + 20 \sum_{m=1}^{\infty} \frac{nq^{mn}}{1-q^{-m}} \\
ge_2 &= \frac{1}{276} + \frac{3}{5} \sum_{m=1}^{\infty} \frac{nq^{mn}}{1-q^{-m}}
\end{align*}
\]

[Indication of how one does it: Write \( x(W) \) as a function of \( W \). For \( u \) near \( u_0 \)
\[
x(u) = \frac{e^u + e^{-u} - 2}{e^u + e^{-u}} + \sum_{n=1}^{\infty} \frac{1}{1-q^{-n}} e^{\frac{u}{2}} + \sum_{n=1}^{\infty} \frac{nq^{u}}{1-q^{-n}} e^{\frac{u}{2}} + \sum_{n=1}^{\infty} \frac{nq^{u}}{1-q^{-n}} e^{\frac{u}{2}}
\]
\[
\frac{1}{12} - \frac{1}{12} + \frac{1}{240} \sum_{m=1}^{\infty} \frac{nq^{mn}}{1-q^{-m}} a^2 + (\frac{1}{240} - \frac{1}{240} \sum_{m=1}^{\infty} \frac{nq^{mn}}{1-q^{-m}}) a^4 + \ldots
\]

has a pole of order 2, so \( x(u) + \frac{1}{12} = g_0(u) \).
\[
g_0(u) = a^2 + \frac{1}{240} \sum_{m=1}^{\infty} \frac{nq^{mn}}{1-q^{-m}} a^2 + \frac{1}{240} \sum_{m=1}^{\infty} \frac{nq^{mn}}{1-q^{-m}} a^4 + \ldots
\]
\( g_0(u) \) is used just formally to check
\[
(g_0(u))^2 - 4(g_0(u))^2 + g_2 g_0(u) + g_3 = C a^2 + D a^4 + \ldots \quad \text{and} \quad i = 0.
\]
Will also find \( f_3(w) = \frac{4g_3}{w^3} - \frac{4x}{w^2} + \frac{2g_2}{w} \).

where \( y(w) = \sum_{n=0}^{\infty} \frac{g_n}{n!} w^n \),

Substituting \( x \) and \( y \) into \( (f_3(w))^2 = 4(f_3(w))^3 + g_2 f_3(w) - g_3 \), one gets the identity:

\[ y^2 + xy - x^3 - b_2 x - b_3 = 0 \]

where \( b_2 \) and \( b_3 \) are certain sums of \( g_2, g_3, g_4, \ldots \).

\[
\begin{align*}
b_2 &= \frac{1}{4} g_2 - \frac{1}{12} f_3 - \frac{1}{5} \sum_{n=1}^{\infty} \frac{g_n}{n} \quad \text{(integer coeff when expanded)}. \\
b_3 &= \frac{1}{4} (g_3 + \frac{g_4}{12} - \frac{1}{432}) - \sum_{n=1}^{\infty} \frac{2g_n + 5g_{n+1} - \frac{g_{n+2}}{12}}{1 - \frac{g}{12}} \\
\end{align*}
\]

(Also \( 7n^5 + 5n^3 = 7s^5(n^3 - 1) + 12n^3, \) so \( b_3 \) has integer coeffs. \( \equiv 0 \mod{12} \))

If \( k \) is arbitrary, use these formal series \( (|q| < 1) \). Then \( b_2 = b_2(q) \in k \) \( b_2 \) and \( b_3(q) \in k \). Then \( y^2 + xy - x^3 - b_2 x - b_3 \) defines a curve \( A = A(q) \) over \( k \).

**Proof:** The map \( w \rightarrow (x(w), y(w)) \) is an isomorphism of \( k \) onto \( A_k \), with kernel \( q \cdot \frac{1}{n} \), and \( \Delta(q) \equiv 0 \mod{q} \), so \( A(q) \) is elliptic.

(Thus gives a transcendental parametrization of the group of rational points.)

**in search of**

\( \Delta = q - 24q^2 = 0 \) since \( \equiv q \mod{q^2} \); \( \Delta(q) = \prod (1 - q^m)^2 \).

\( j = \frac{1}{q} (1 + 744q + 196884q^2 + \cdots) \) so \( j \neq 0 \) in new. arch. case.

Inverting formally gives \( q \) as a p.s. in \( j \), integer coeff. and any such \( j \) is obtainable from a (unique) \( q \).
Proof of the theorem!
We have \( q: k^* \to k \times k \). We claim \( q(k^*) \subset A_k \), i.e.,
\( q: k^* \to A_k \), with the understanding that \( q(q^* A_k) = \) infinite points of \( A_k \), i.e., \( x(w), y(w) \) satisfy \( y^2 + xy = x^3 - b_2 x - b_3 \), \( \forall w \in k^*, w \neq q^* \).
Because of the purity of degree, it suffices to work with \( k \)'s 6.8. \( |q| : 1 < |w| \leq 1 \).
\( x(w) \in k = \mathbb{Z}[w, w^{-1}, (1-w)^{-1}] \ll q \rr \), also \( y(w) \in k \). Claim \((*)\)
holds in this ring. We have a canonical homomorphism \( k \to \mathbb{Z}[w, w^{-1}, (1-w)^{-1}] \ll q \rr \).

Thus we need only show that \((*)\) holds formally. Fix \( w \in k \), \( |w| < 1 \).
and let \( X = X_w(q) \), \( 1 < |w| \). Since \((*)\) holds for \( X, y \) (classical case), \((*)\) holds formally, and hence in the general case.
If \( w_1, w_2 \), do we have \( q(w_1 w_2) = q(w_1) \cdot q(w_2) \)? (in the sense of addition on the curve.)
\( \Rightarrow \) \( 1 < |w_1| \leq 1 < |w_2| \), \( |q| : 1 < |w_1| \leq 1 < |w_2| \).

We know \( q(1) = 0 \), so we can assume \( w_1 \neq 1 = w_2 \). Let \( q(w_2) = (x_1, y_1) \). We must have \( \lambda = \frac{y_1 - y_2}{x_1 - x_2} \), \( \forall x_1 \neq x_2 \).
Then \( \Pi = \Pi_1 + \Pi_2 \iff (x_1 - x_2)^2 y_1 = (y_1 - y_2)^2 + (y_1 - y_2)(x_1 - x_2) - (x_1 - x_2)^2 (x_1 + x_2) \)
and a similar equation holds for \( (x_1 - x_2)^3 y_2 \). These equations hold formally, for \( x_1, y_1, y_2 \in \mathbb{Z}[w_1, w_2, w_1^{-1}, w_2^{-1}, (1-w_1)^{-1}, (1-w_2)^{-1}, (1-w_2)^{-1}] \ll q \rr \).

Since they hold in the complex domain.
If \( x_1 = x_2 \), i.e., \( p_1 = \pm p_2 \), then we have the following.

Lemma: Let \( q: A \to B \) be a map of commutative groups s.t \( q \) assumes infinitely many values,
and \( q(w_1 + w_2) = q(w_1) + q(w_2) \) for all \( w_1, w_2 \) s.t. \( q(w_1) \neq \pm q(w_2) \). Then \( q \) is a homomorphism.

Then for \( q_1 \cdot q_2 \) and \( q_1(q_2) = q_1(q_2) \Rightarrow w_1 = q_2(w_2) \), some \( v \).
Lemma: If \( w \) is separably algebraic over \( k \), and \( q(w) \in A_k \), then \( w \in k \).

Proof: If \( w \in K \), write \( K \) finite and algebraic over \( k \). Let \( G = G(K/k) \).
Then \( G \) acts on \( A_k \), \( K^* \rightarrow A_k \) via \( \varphi(w)^o = (\varphi(w))^o \).
\( o \in G \), since \( o \) leaves all coefficients fixed, but \( o \) leaves the valuation fixed: \( a_0 \rightarrow a \Rightarrow a_0^o \rightarrow a^o \). But then \( w^o = q(w) \Rightarrow lq^{1/2} - 1 \Rightarrow v = 0 \Rightarrow w^o = w \Rightarrow w \in k \).

Now, given \( x_0 \in k \), to find \( w \) s.t \( X(w) \cdot x_0 \).

Case 1: \( |x_0| > lq^{1/2} \). (Line 2 undone, \( |x_0| < 1 \)).

Put \( L = w + w^{-1} - 2 \); \( w^x - (x^2 + 2)w + 1 = 0 \) has roots \( L, w^{-1} \) up \( k \).
\( w^x + w^{-x} - 2 = x^x + c_{x^{-1}} x^{x^{-1}} + \ldots + c_{x^{-1}} x^{x^{-1}} + \frac{1}{x} + \frac{1}{x^2} + \ldots \).
\( x \in k \Rightarrow \exists \ z \in k \) s.t. \( x = f(z) \). The crucial thing is \( |x_0| > \frac{1}{lq^{1/2}} \) and \( |x_0| < lq^{1/2} \). Then we can invert and get \( z = \frac{1}{x} + b_1 x + \ldots \) and the formal inverse series converges for \( \frac{1}{x} < lq^{1/2} \).

Classically, \( q = e^{\pi i \lambda} \), \( z = \frac{z}{z^2} \), and \( \Delta \gg 0 \).

\( A_k = k^{1/2} / q^{1/2} \); \( x \in K \) is algebraic over \( k \), \( A_k \cong k^{1/2} / q^{1/2} \).

Take \( m > 0 \) and \( \Delta \gg 0 \).

If \( k \in K^{\ast} \), \( w^m = q^2 \), i.e., \( w^m \in q^{2 \ast} \). If \( K \) is algebraically closed, this group is generated by \( 2 \) elements, \( w^v, v^w \).
\( x \in A_k \Rightarrow (A_k)^m \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}) \). If char \( = m \). This is true quite generally for \( K \) algebraically closed, and \( p + 1 \) even. \( \frac{1}{lq^{1/2}} - 1 \).
If \( m = p^n \), then \((A_K)_p \approx \mathbb{Z}/p^n\mathbb{Z}\), for \(K\) algebraically closed of characteristic \(p\). This is not true in general: it is true under \(j\) is one of a certain number of absolutely algebraic elements in each characteristic \(p > 0\) in which case \((A_K)_p \approx \mathbb{Z}/p^j\mathbb{Z}\). For example, \(p = 2, j = 0\) so this is an exception.

If \(K\) not algebraically closed, not complete, and if \(K = \bar{K}\), adjoining the coordinates of \(A_K\) in \(\bar{K}\), what kinds of rationality does one get? (Problem.)

Now we have \((A(q))_K \cong K^*/q^\mathbb{Z}\)

\[A_K \supseteq A_0 \supseteq A_q \supseteq A_{\bar{q}}\]

For \(q \in (A(q))_K\), \(a: x(w), y(w), y^2 + xy - x^3 + b_2x + b_3, b_2 \in \mathbb{Q}\).

\[A_0 \cong \{w: w < 1\}\]

\[A_q \cong \{w: w < 1 + 1\}\]

\[A_{\bar{q}} \cong \{w: w \in \mathbb{Q}\}\]

Then \(A_K/A_0 \cong \text{value group/1}_{1/\mathbb{Q}}\mathbb{Z}\). In the case of a discrete valuation \(v = 0/\mathbb{Q}\), \(v - \text{ord } q = \text{ord } 1/\mathbb{Q}\).

Problem: if the valuation is discrete and \(A_0\) is optimal, then is \(A_K/A_0\) always finite? What is its structure. It is known in for \(k = \mathbb{Q}(t), k, \text{alg. cl., char. } 0\).

We have now handled the case \(|j| > 1\). If \(B\) is good with such \(j\), let \(A\) be our standard one (arch. valuation), so we can find \(g\) as a power series in \(1/j\), (and let \(A = A(q), q = q(j)\)).
Then \( A \) and \( B \) have the same \( j \)- and so become isomorphic over a separable quadratic extension \( K/k \). Let \( \sigma(\hat{K}/K) = \{1, \sigma^3\} \).

Let \( \varphi: A \rightarrow B \) be an isom. def. /K. \( \varphi: A_k \rightarrow B_k \). \( B_k = \{ b \in B_k : \sigma b = b^3 \} \). We also have \( \varphi^*: A \rightarrow B \), and we may assume \( \varphi^* = \varphi \), otherwise \( A \cong B \) over \( k \). Thus we have the composite \( A \rightarrow B \rightarrow A \), and \( \varphi^* \varphi \) is nontrivial. Since \( \sigma \neq 1 \) for \( \bar{a} \neq 1728 \), \( A \) has just one nontrivial aut., i.e., \( \varphi^*(a) = -\varphi(a) \).

Thus we want to find the \( a \)'s s.t. \( \varphi(a) = \varphi^*(a) \). Put \( \varphi(a)^3 = \varphi^*(a)^3 = \varphi(a^3) \). Thus we want \( a \)'s s.t. \( a + a^5 = 0 \), and the \( b \)'s s.t. \( b^6 = b \) correspond to the \( a \)'s s.t. \( a^6 = -a \).

It is not a \( \mathbb{G}_m \)-homomorphism.

Thus if you know the structure of \( A_k \) and \( A_k \) for \( [K:k] \cdot [K:k] = 2 \), then by looking at all \( a \in A_k \) s.t. \( a + a^5 = 0 \), get structure of \( B_k \).

Divisible points

Let \( m \) be \( > 0 \). Consider \( A \rightarrow A \) by \( a \rightarrow ma \).

Let \( A_m = A^m \). (On the case \( m = 2 \) - all we need in the Mordell theorem.) Every fact used can be checked directly without using sophisticated alg. geometry.

We always have a surjection \( A\hat{\omega} \rightarrow A_m \), and hence an exact sequence

\[ 0 \rightarrow A_m \rightarrow A\hat{\omega} \rightarrow A_m \rightarrow 0 \]

if \( \text{gcd}(k, m) = 1 \), then:

1. \( A\hat{\omega} \) is divisible by \( m \) (true even of \( p \mid m \) but harder!)
2. \( A_m \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}) \).
3. \( A \rightarrow A \) is separable, unramified of degree \( m \), so if \( a \in A\hat{\omega} \), \( ma \in A_k \), then \( k(A)/k \) is separable.
5. If \( k \) is complete, then \( \tilde{A}_g \) is uniquely divisible by any \( m \) s.t. \( \text{char}(k) + m \).

(5) is proved using the filtrations, \( A_{g_0} \supset A_{g_1} \supset A_{g_2} \supset \cdots \). Then \( A_{g_1}/A_{g_2} \cong k^* \), which is uniquely divisible by \( m \), and \( A_g = \text{finite } A_{g_1}/A_{g_2} \).

**Theorem:** Given a valuation on \( k \), and \( A \) defined over \( k \) with non-degenerate reduction mod \( y \). Then division by \( m \) gives ramified extensions of \( k \): \( m \alpha \in \tilde{A}_g \Rightarrow k(\bar{\alpha})/k \) are ramified.

**Proof:** Might as well assume \( k, K \) complete, \( \alpha \in \tilde{A}_g \), \([K:k] < \infty\).

Let \( \bar{\alpha} \in \tilde{A}_g \). We get a unique extension of the valuation \( \bar{k} \).

Let \( \bar{k}(\bar{\alpha})/\bar{k} \) be separable. Then there is a unique \( E \) s.t. \( \tilde{E} = \tilde{k}(\bar{\alpha}) \) and \( E \) is unramified over \( k \). Now take \( A_E \rightarrow \tilde{A}_E \) which is surjective. \( \tilde{E} \in \tilde{A}_E \Rightarrow \exists \tilde{c} \in A_E \) s.t. \( \tilde{c} = \tilde{\alpha} \), so \( \tilde{c} - \tilde{\alpha} = 0 \), and \( \tilde{c} - a \in A_{\tilde{E}} \subset A_k \). \( m \alpha \in \tilde{A}_g \), \( c \in A_E \Rightarrow m c \in A_{\tilde{E}} \Rightarrow m(c - a) \in A_g \) i.e., \( m(c - a) \in A_{\tilde{E}} \). Then using divisibility of \( A_g \) and \( A \), \( \alpha \in \tilde{A}_E \).

By the same methods one proves:

Under the hypotheses of the thm, the homomorphism \( (\tilde{A}_g)_m 
\rightarrow (\tilde{A}_g)_m \)

is an isomorphism.

**Reference:** Lang Tate A.T.M. Principal homog. space over abelian var's.

Consider \( A_g \) and \( mA_g \). - get an extension of \( D \) - for \( p + m \) ram of coher., get non-degenerate reduction. For \( p + m \), can apply thm and use this D show that the extension is finite over \( D \). Thus it will follow that \( A_g/mA_g \) is finite.
To show $A_k/mA_k$ finite, let $K = k(\frac{1}{mA_k})$ i.e. adjoin $\frac{1}{m}$ to the coefficients of the minimal division $\sigma$. (Assume $m/k = ?$)

Claim: $[K:k] < \infty \iff (A_k:mA_k) < \infty$.

Proof: ($\Rightarrow$): If $A_k = \mathcal{U} \sigma_j + mA_k$ take $m \sigma_j = 0, 1 \leq j < m^2$, $a_i = m b_j, 1 \leq i < m$. Then $K = k(b_0 + c_j)$, generated by $m^2$ elements.

($\Leftarrow$): Let $G = G(K/k)$. For each $a \in A_k$ choose $b \in A_k$ s.t. $a = mb$. For $\sigma \in G$, let $\text{f}_a(\sigma) = \sigma b - b * m \sigma f_b(\sigma) = 0$. So $f_a(\sigma) \in A_m$ which is finite (of order $\leq m^2$).

I claim also $G$ is abelian. To see this note $\sigma \beta = \beta + t \sigma, t \in A_m$, and $\sigma \delta \beta = \beta + t \sigma + t \delta, \sigma t \sigma = t \sigma + t \delta$. Then:

$$f_a(\sigma) : A_k \times G \to A_m$$

is abelian. Also, the kernel on the right consists of those $a$ s.t. $f_a(\sigma) = 0$ for all $\sigma$, hence $K$ is generated by the elements $n a, a \in A$, $n$ must be the identity. The kernel on the left is $\{a : f_a(\sigma) = 0, \forall \sigma \in G \}$. But for such $a$, $k(\frac{1}{mA_k})$ is fixed under $G$, so $k$. Thus $d \in mA_k$. Hence we get a bijective map: $A_k/mA_k \times G \to A_m$ whose kernel on both sides is trivial.

Thus $G$ is abelian of exponent $\leq m$.

Now take $k = a$ finite extension of $k(\frac{1}{k_0})$, and let $k_0 = k$.

Almost all primes in $\mathfrak{p}$ are discrete. Assume $k \neq k_0$.

If $A$ is a curve over $k$, $A$ has nondegenerate reduction (n.d.r.) for almost all primes, i.e., for all $y$ and in a finite set
S which contains:

all archimedean primes \( \mathfrak{p} \).

all \( \mathfrak{p} \) s.t. \( A_i \not\subset \mathfrak{p} \) for some \( i \).

all \( \mathfrak{p} \) s.t. \( \mathfrak{p} \mid \Delta \).

If, in the number field case, enlarge \( S \) so that it contains

all \( \mathfrak{p} \) s.t. \( \mathfrak{p} \mid \mathfrak{m} \).

\( S \) is still finite.

Assuming \( A_m \subset A_k \) and the primitive \( m \)th roots of 1 are in \( k \), then

1. \( k\left(\frac{1}{m} A_k\right) \) is abelian over \( k \), with \( \mathcal{C} = \mathcal{G}(k\left(\frac{1}{m} A_k\right)/k) \)

2. of exponent \( m \). (i.e. \( \mathcal{C} \))

3. and unramified outside \( S \) (i.e. \( k\left(\frac{1}{m} A_k\right) \)).

(Th: \( A_k/mA_k \) is finite if \( (k_0^\times/k_0^\times m) < \infty \). [cf. DG ?]

Let \( K \) be the maximal abelian extension of exponent \( m \) unramified
outside \( S \). Then \( [K: k] < \infty \).

Proof: Take \( f \in k^\times \). When is \( k(\sqrt[m]{f}) \) unramified at \( \mathfrak{p} \)?

\( k(\sqrt[m]{f}) \) unramified at \( \mathfrak{p} \) \( \Leftrightarrow \) order \( (f) = 0 \mod m \) (if \( \mathfrak{p} \not\subset \mathfrak{m} \)).

Consider for field case:

\[ \{ f : (f) = m \mathfrak{m} \text{ outside } S \} \setminus \{ f : (f) = m \mathfrak{m} \text{ in } S \} \]

\[ \{ f : (f) = m \mathfrak{m} \} \]

\[ \{ f : (f) = m(g), g \in k^\times \} \]

\[ = \{ f \in k_0^\times k^\times m \} \]

\[ \{ f \in k^\times m \} \]

\[ \{ f \in k^\times \} \]
$k^m$ is of finite index in $\mathfrak{F}$: $(\mathfrak{f}) = ml$ outside $S^3$.

In the number field case, work with ideals rather than division.

\[ \mathfrak{f} : (\mathfrak{f}) = \mathfrak{A}^m \text{ outside } S^3 \]
\[ \mathfrak{f} : (\mathfrak{f}) = \mathfrak{A}^m \text{ if } \mathfrak{f} \in k^*(\text{units})^3 \]

\[
\begin{align*}
\mathfrak{f} & = \mathfrak{A}^m \text{ outside } S^3 \\
\mathfrak{f} & = \mathfrak{A}^m \\
\mathfrak{f} & \in k^*(\text{units})^3
\end{align*}
\]

\[
\begin{align*}
\mathfrak{f} & \in k^*(\text{units})^3 \\
\mathfrak{f} & \in k^m
\end{align*}
\]

Now look at the case $m = 2$, i.e., $A_k/2A_k$.

Assume $y^2 = (x - e_1)(x - e_2)(x - e_3)$, $e_i \in k^m$. ($k = \mathbb{Q}$).

Then

\[
A_k/2A_k \cong \text{Hom}(G, A_k) = \text{Hom}(G, \text{Hom}(A_2, 3^{\pm 13}))
\]

where $A_m \cong \text{Hom}(A_m, \{m\text{th roots of 1}\})$ is canonical. $G \cong (K/k)$, $3^{\pm} = k^* \cong k$. Hence $f \in \Sigma \iff f \in k^*$.

where $\text{Hom}(A_2, 3^{\pm}) \subset \text{Hom}(A_2, k^{*1})$. $A_2 = \{e, e_1, e_2, e_3\}$ so the fours groups.

An element of $\text{Hom}(A_2, k^{*1})$ is described by 2 elements $e_i, c_i, c_3 \in k^{*1}$ so $e_i c_i c_3 = 0$ or $k^{*1}$. (We have $2a_i = 0$, $a_i + a_i + a_3 = 0$), i.e., $(e_i, c_i, c_3) \in (k^{*1})^3 = \Sigma$, so we get a map $A_k/2A_k$.

\[
\begin{align*}
\mathfrak{f} & = \mathfrak{A}^m \text{ if } \mathfrak{f} \in k^*(\text{units})^3 \\
\mathfrak{f} & \in k^m
\end{align*}
\]
If \( P = (x,y) \in A_k \pmod{2A_k} \), map \( P \mapsto (c_1, c_2, c_3) \), where \( c_i = x - c_i \pmod{k^{*2}} \) (if \( c_i = 0 \), replace it by \( c_i = c_i, c_2 \)).

For which such triples \( (c_1, c_2, c_3) \), does \( \exists P \in A_k \) giving the triple? To find \( x \) s.t. \( x - c_3 = c_3 x^2 \pmod{3} \), where \( c_3 \) are given and \( c_2 \) are determined by the curve? (\( ? \))

In the rational field, \( c_3 = \pm 1 \Gamma P^2 \), \( \Gamma = 0 \) or \( 1 \). \( P \Gamma A_k \), d.m.m. of \( c_3 \).

References:

A defined over \( \mathbb{Q} \), \( y^2 = x^3 - Ax^2 - B \). \( A, B \in \mathbb{Z} \).

If \( P = (x,y) \) is not \( O \) and \( x \) and \( y \) are rational, then, what must the denominators look like?

\[
\begin{align*}
x &= \frac{m}{n^2}, \\
y &= \frac{c}{n^2}, \\
n > 0.
\end{align*}
\]

Define the height of \( P = \max \{ |m|, |m|^{1/3} = h(P) \} \) (and of \( P \) also!)

\( h(0) > 1, \ h(P) \geq 1 \) always. Clearly \( V_{h_0}, \ \{ P \in A_k, \ h(P) = h_0 \} \)

is finite.

For all \( P_0 \in A_k \), \( E \) constant \( c_0 \geq 0 \) s.t. \( h(P + P_0) \leq c_0 h(P)^2 \).

And \( E \) universal \( c_0 \geq 0, \ s.t. \ h(P)^2 \leq c_0 h(2P) \). Both results hold for all \( P \in A_k \).

Assuming these, to prove the Mordell Theorem, we know \( A_k / 2A_k \) is finite. Take a finite set of worst representatives, \( \{ Q_1, \ldots, Q_n \} \) for \( 2A_k \) in \( A_k \).
The Mordell-Weil Theorem.

Weil: sur un théorème de Mordell, Bull Soc Math de France 1930
Northcott: points torsion sur une variété algébrique; Ann 1950
Lang-Neron: with points of ab. Var. over fields; Andy Jan 1959

Theorem: Take A defined over \( \mathbb{Q} \):
\[ y^2 = x^3 - Ax - B \]
with \( A, B \in \mathbb{Z} \). Let \( P = (x, y) \), \( P \neq 0 \) and \( x, y \in \mathbb{Q} \).
What must the denominator look like? \( x = \frac{m}{n^2} \) \& \( y = \frac{e}{n^3} \) for \( n > 0 \); in lowest terms \( (m, n) = 1 = (l, n) \) with \( m, n, l \in \mathbb{Z} \).

Define the height of a point \( P = \max \{ |m|, |n| \} \) = \( h(P) \). Note \( h(0) = 1 \), and \( h(P) > 1 \) always.

Clearly \( h_0 \), \( \{ P \in A \mathbb{Q} : h(P) < h_0 \} \) is a finite set.

For every point \( P_0 \in A \mathbb{Q} \), there is a constant \( c > 0 \) \& \( h(P+P_0) \leq c \cdot h(P)^2 \) and there is a universal constant \( c > 0 \) \& \( h(P)^n \leq c \cdot h(2P) \) for all \( P \in A \mathbb{Q} \).

Assuming there are no points of the Mordell-Weil Theorem:

Know \( A \mathbb{Q} / 2A \mathbb{Q} \) is finite, takes finite number of representatives for cosets — say \( \{ a_1, \ldots, a_r \} \) are representatives for the cosets of \( 2A \mathbb{Q} \) in \( A \mathbb{Q} \). Let \( P = P_0 \in A \mathbb{Q} \); then \( P_0 = a_0 + 2P_1, P_1 = a_1 + 2P_2, \ldots, P_n-1 = a_{n-1} + 2P_n \).

Let \( P = a_0 + 2a_1 + 4a_2 + \ldots + 2^{n-1} a_{n-1} + 2^n P_n \).

Let \( P' = 2P \) and note \( h(P') \leq c \cdot h(P') \leq c \cdot h(P)^2 \). Let \( C > C' c \). Then \( h(P') \leq c \cdot h(P) \) and \( h(P_{n+1}) \leq c \cdot h(P_n) \) so \( h(P) \leq C' \) for \( n \geq 0 \), \( h(P) \leq C + e \) for \( P \in \mathbb{Q} \) is a set of generators.

Proof of first statement:
\[ a^2 = m^3 - An^2 - Bn^2 \]
so \( 1 + \frac{1}{1} + \frac{1}{1} \). Let \( P_0 = (\frac{m_0}{n_0}, \frac{l_0}{n_0}) \) and \( P + P_0 = (\frac{m_0}{n_0}, l_0/n_0) \).

Given by \( X = \{ (x, y) : (x-x_0)(x+x_0) - 2B - 2yy_0 \} \). Then \( (x-x_0)^2 \)
\[ = \{(m^2 - An^2 n_0^2)(m_0^2 + m_0 n^2) - 2Bn^2 n_0^2 - 2Bn^2 n_0^2 \}/(m_0^2 - m_0 n_0^2) \]
\[ = h(P) h(P)^2 - A h(P)^2 - h(P)^3 A h(P)^2 \]
\[ / A h(P)^2 \]
providing these formulas work, we're ok. But they break down in only finitely many cases: \( p = \pm p_0 \). This is still ok for \( p = -p_0 \), and we enlarge the constant in case \( p = p_0 \).

Proof of second statement: Let \( 2P = (X, Y) \).
\[
X = \left\{ x^4 + 2A x^2 + 8B x + A^2 \right\} / \left\{ 4x^3 - 4Ax - 4B \right\} \quad \text{works if} \quad 2P \neq 0 \quad \text{(of which there are four points?)} \quad \text{let} \quad x = x_0 / x_1 \quad \text{in lowest terms, and} \quad X = x_0 / x_1. \quad \text{Then} \quad \frac{x_0^4 + 2Ax_0x_1^2 + 8Bx_0x_1^3 + A^2x_1^4}{x_1} = \frac{20}{L_1(x_0, x_1)}.
\]

Claim: \( l_0 \) & \( l_1 \) have no common zeroes in projective line \( TP_1 \):
\[
F_0(x_0, x_1) L_0(x_0, x_1) + F_1(x_0, x_1) L_1(x_0, x_1) = D_0 x_0^2 + F_1 L_1 = D_1 x_1^3
\]

(homogeneous multilinearly applied to \( P: 1 \) is expressible as a sum with homogeneous int. coeff.) \( F_i \) have coefficients in \( Z \); \( D_0, D_1 \in Z \); \( x_i \in Z \).
and \( gcd(x_0, l_1) \) divides lcm \( D_0, D_1 \). The \( D_i \) depend only on \( A \) & \( B \). New \quad \frac{\max(x_0, x_1)}{\min(|x_0| + 1, |x_1|)} \quad \text{is homogeneous and continuous on the real projective line, so takes on a non-zero minimum, so} \quad \max(|x_0| + 1, |x_1|) \geq \text{const} \cdot h(P)^4 \quad \text{and} \quad \max(x_0, x_1) \geq \frac{\text{const} \cdot h(P)^4}{2} \quad \text{etc.} \quad \text{and} \quad \text{a.e.}

\[ A_2 = \mathbb{Z}^r + F, \quad F \text{ a finite group. And} \quad (A_2 / 2A_2) = \mathbb{Z}^s \quad \text{if there are} \ 2^s \text{ points of order 2:} \ (s = 0, 1, 2) \quad \text{depending on whether} \ x^3 - Ax - B \quad \text{splits.}
\]

Northcott's definition of height:
Take \( TP^n \) = projective \( n \)-space, \( P = (x_0, \ldots, x_n) \in \mathbb{P}^n_k \). If \( k \) is a number field define \( h_k(P) = TP \min_{\text{prime} \ p} (1; p) \) where the product is over all prime divisors \( p \) of \( k \), finite and infinite, and where \( 1/\gamma \) is normalized. Since \( 1 \neq 0 \) in \( k \), \( TP \gamma 1; p = 1 \); the above definition doesn't depend on the way the point \( P \) is represented. Thus \( h_k(P) \) depends only on \( P \), and not on its coordinates.

And \( h_k(P) = h_k(P) \quad [k, k] \quad \text{if} \ k \in \mathbb{K} \) one can show \( h_k(P) = h_k(P) \quad [k, k] \).
and thus define $h(P) = h_k(P)^{1/k^2}$, independent of $k$.

The proof works approximately if you take $k = k_0(x)$; $x = m^2$, $m, n \in \mathbb{Z}$, $h(P) = \max \{ 2^{\deg m}, c \deg n^2 \}$ where $c > 1$.

But we must fix up appeal to compactness of real $P^1$.

Fact (he won’t swear to it): $A_k$ is finitely generated unless it comes from an abelian variety defined over $k_0$. Then $A_k/k_0$ is finitely generated.

Let $k$ be either a number field or a function field in one variable over $k_0$. For $y = (y_0, \ldots, y_n) \in P^n_k$ define $h_k(y) = \prod_p \max (1, y_i/p)$, $y_i$ running over the set of primes $\mathcal{M}_k$ of $k/k_0$ or (function field case) field $k$.

For function fields case: let $f \in k$ and $1/f = e^{\text{deg } f}$; as the function formula holds, $h(y) = h_k(fy)$, where $\gamma = (x_0, \ldots, x_n)$.

1. $\{ P \in P^n_k \mid h_k(P) \leq h_0 \}$ is finite in the number field case or if $k_0$ is finite.

Today, $A$ would be any non-singular complete curve defined over $k$, with function field $k(A)$.

If $f_0, f_1, \ldots, f_n \in k(A)$, not all zero, we get a map $f : A \to P^n_k$ over $k$ by $f(P) = (f_0(P), \ldots, f_n(P))$ for $P \in A_k$, after multiplying all the $f_i$ by a high enough power of $f$ (1 up at $P$) to make sure no $t^n f_i$ has a pole at $P$, but one $t^n f_i$ is non-zero at $P$.

So $A_k$ maps into $P^n_k$ where $h_k$ is a height in $A_k$, depending on choice of $f = (f_0, \ldots, f_n)$; $h_k(P) = h_k(f(P))$.

We were using $f = (1, x)$ before. He claims that the height doesn’t depend too much on the choice of the $f$’s.

2. $y = (y_0, \ldots, y_n)$, set $xyi = (\ldots, fi \circ gi, \ldots)$

Then $h_{xyi} = h_f \circ h_g$.

3. If $B$ is another curve in $A$ and $B \to A$

Then $h_{B \circ f \circ w} = h_f \circ h_w$.

Write $h' = h \iff \exists c_1, c_2 \gg A \in \mathbb{A}$, $c_1 h'(P) \leq h(P) \leq c_2 h'(P)$.

Again $f = (f_0, \ldots, f_n)$, $(f)_0$ is the smallest $s$.

$r_j (f_{10} + f_{11}) > 0$. 

-3.16.
4. If \( \langle f \rangle \sim \langle g \rangle \), then \( b_f \sim b_g \). Let \( (tf)_0 = (t_0 - t) \) for all \( t \in k \). We can consider them equal.

a. Let \( f \equiv g \) \( (t_0, \ldots, f_n, g, \ldots, g_n) \); now \( (f, g)_0 = (f, g) \). Show \( b_f \sim b_g \). The triangle is to go from \((t_0, \ldots, f_n)\) to \((t_0, \ldots, f_n, g)\) and \( (t_0, \ldots, f, g)_0 = (t_0, \ldots, f, g) \). Now consider the ring \( k[\frac{t_0}{g}, \frac{t_1}{g}, \ldots, \frac{t_n}{g}] \subset k(\mathcal{K}) \). The \( \frac{t_i}{g} \) have no common zeros on \( A \) — for otherwise \( g \) has less zeros (more poles) than every \( f_i \). And \((t_0, \ldots, f_n, g)_0 = (t_0, \ldots, f_n, g) \Rightarrow \frac{t_0}{g}, \ldots, \frac{t_n}{g} \) have no common zeros on \( A \).

Now \( \frac{t_0}{g}, \ldots, \frac{t_n}{g} \) generate the unit ideal in \( k[\frac{t_0}{g}, \ldots, \frac{t_n}{g}] \) so by using completeness and by extending \( k \) to get a valuation, \( 1 \equiv \sum q_1 (\frac{t_0}{g}, \ldots, \frac{t_n}{g}) q_j = \sum q_j (\frac{t_0}{g}, \ldots, \frac{t_n}{g}) \) \( \forall q \in A \), \( 1 = \phi (\frac{t_0}{g}, \ldots, \frac{t_n}{g}) \).

So \( \frac{t_0}{g} \in M_k \), \( \exists \phi > 0 \) (depending on \( \phi \)) such that \( \text{Max} \{ | t_0 | g | t_k | \} > \phi \).

where \( \phi \) is normal. and doesn't occur in the denominators of the coefficients of \( \phi \).

Thus \( T_0 \text{Max} \{ | t_0 | g | t_k | \} > T_0 \text{Max} \{ | t_0 | g | t_k | \} \) \( \text{Max} \{ | t_0 | g | t_k | \} \) \( \phi = 1 \equiv \sum q_j (\frac{t_0}{g}, \ldots, \frac{t_n}{g}) q_j \).

Thus \( b_f \sim T_0 \text{Max} \{ | t_0 | g | t_k | \} \).

And \( \phi \) is proved. At least the argument is good for all but finitely many points.

If \( \alpha = (t_0) \) and \( \beta = (t_0) \), then we can write \( h_{\alpha} = h_f \) and the divisor associated with \( f \equiv g \), \( (f, g)_0 = \alpha + \beta \). So \( h_{\alpha + \beta} = h_{\alpha} h_{\beta} \). And \( h_{\beta - \alpha} \sim h_{\alpha} \).

5. Given \( \alpha, \beta \) coming from \( (f) \) and \( (g) \), and \( \varepsilon > 0 \)

\( \exists \) constants \( c_1, c_2 \) depending on \( \varepsilon \), \( \delta_t \), \( \text{deg} b - \varepsilon \leq c_1 h_{\alpha} \), \( \text{deg} h_{\beta} + \varepsilon \leq c_2 h_{\beta} \).

Thus \( c_1 \text{deg} b - \varepsilon \leq c_2 \text{deg} h_{\beta} + \varepsilon \), \( c_1 \text{deg} h_{\alpha} (\varepsilon) \leq c_2 \text{deg} h_{\beta} (\varepsilon) \).

and \( \exists \) essentially only one height function.

Proof of 5: Let \( \phi \) be a prime of \( k \). \( \alpha = \text{deg} \phi, \beta = \text{deg} \phi \). Now \( 3g \alpha + \text{deg} h_{\alpha} = \text{deg} h_{\beta} \) and \( \text{deg} h_{\alpha} = 3g \) and \( \alpha = (\beta) \).

For some family \( \phi \). Now \( \frac{3g}{2} \phi \leq h_{\alpha} \). Let \( \phi = h_{\alpha} \). \( \text{deg} h_{\alpha} = h_{\phi} \) and \( \text{deg} h_{\alpha} = h_{\phi} \).
we can get automorphisms of \( k(A) \) by translating by a point. For \( a = (b, c) \in A_k \), \( T_a : \text{autom of } k(A)/k \), \( P \in k^* \),
\[
T_a(P) = P + a \quad \text{(addition on curve)}
\]
defines a rational map of \( A \) into itself, \( T_\infty : T_a \circ T_a' \).

Define for \( f \in k(A) \), \( f \circ T_a(p) = f(p-a) \); \( f \circ T_a(cP) = f(cP) \).

We want \((x', y') = (x, y) \) for \( p + a = (x', y') \). Take \( K \)
galois over \( k \) with group \( G \). Let \( \sigma \)
operate on \( k(A)/k \) and \( G = G_{k(A)/k} \).

For \( T_a \in G_k \); \( \sigma \circ T_a \) an autom of \( k(A)/k \), \( \sigma \circ T_a = T_{\sigma \circ a} \).

Claim: for \( \sigma \in G \), \( \sigma \circ T_a = T_{\sigma \circ a} \).

Indeed, \( f \circ T_a (P) \quad \sigma \circ f \circ T_a (P) = (f \circ T_a (P)) \quad \sigma = (f \circ T_a (p)) \circ \sigma = (f(cP)) \circ \sigma = f(cP - \sigma a) = (f \circ T_a(cP - \sigma a)) \), and \( T_{\sigma \circ a} \).

To make another group \( G^* \), isomorphic to \( G \), of automorphisms of \( k(A) \). For \( \sigma \in G \) define \( \sigma^* = T_{\sigma \circ a} \circ \sigma \).

\( \{a_\sigma \mid \sigma \in G \} \) is a family of elements of \( k(A) \), indexed by \( G \), \( \sigma \rightarrow a_\sigma \) is a map \( G \rightarrow k(A) \).

What conditions on \( \sigma \) will give \( \sigma^* \circ \sigma = (\sigma^* \circ \sigma)^* \) ?

\( \sigma^* \circ \sigma = T_{\sigma \circ a} \circ \sigma = T_{\sigma \circ a} \circ \sigma \circ T_{\sigma \circ a} \circ \sigma = (T_{\sigma \circ a} \circ \sigma)^* \).

will be true iff \( a_\sigma + \sigma a_\sigma = a_\sigma \) all \( \sigma \in G \).

We define a group \( G^* \), isomorphic to \( G \), of automorphisms of \( k(A) \).

Thus we get \( \sigma \mid K \subseteq k(A) \).

\( F = k(A) \), \( F \cap K \) so the degrees are the same. In fact \( F \) regular in \( k \) it is the function field for some curve \( k(C) \).

\( k(C) = \text{fixed field of } G^* \text{ in } k(A) \).

\( G^* \) is isomorphic to \( \{a_\sigma \mid \sigma \in G \} \) is a group of automorphisms of \( k(A) \).

And \( \sigma \mid K \).

Thus we get \( \sigma \mid K \).

In fact, given any curve \( C \) of genus 1, we can get \( \sigma \)
such that \( C \) comes from \( A \) in the way defined by \( \alpha \).

The elements of \( H'(G_{/K}, A_K) \) are in 1-1 correspondence
with \( K \)-isomorphism classes of the \( C \)'s you get (1).
\( C_K \) is identified with \( A_K \) by \( K(A) \cong K(C) \).

If \( a \in A_K \), \( a^* \in C_K \), \( a \mapsto a^* \) a birational map \( A \to C \)
defined \( /K \), produced by the identification of the function
fields: What is \( (\sigma a)^* ? \)
\[
(\sigma^*(a)) = \frac{\sigma a}{a} = \sigma a + \sigma a^*
\]
\( (\sigma^*(a^*)) = \sigma(a^*) \) is \( \sigma(a^*) \)

Start over: want a birational map \( C \to A \), \( \varphi : C \cong A \),
defined \( /K \) by \( K(C) = K(A) \). Let \( c \in C_K \); then
\[
\varphi(c) = \varphi(c) = \varphi(\varphi(c)) + \varphi c
\]
and
\[
\varphi c = \varphi(\varphi c) = \varphi(\varphi c) + \varphi c \quad (\sigma \in \varphi c)
\]

Let's try to investigate whether \( C \) has rational points;
it certainly does over \( K \).
If \( C_L \equiv c \), then \( \forall \sigma \in H \), \( c = \sigma c \)
and \( \alpha c = \varphi(c) = \varphi(\varphi c) \) so
\( c \mapsto H \{ \alpha c \} \) splits (i.e., is zero).

3-23

**General Question:** Descartes des corps de base

F. Châtelet; Weil: Ann. 1936, 509-524

Serves: Arith. & Corps de ...

... and Saavedra

Let \( A \) be any variety \( /K \), and \( K \) an extension of \( k \).
To find varieties \( B/K \) and \( B \cong A \) over \( K \). Better to consider
a pair \((B, \varphi)\), \( B \) defined \( /K \) and \( \varphi : A \cong B \) an isomorphism.
And \((B, \varphi) \cong (B', \varphi') \iff \exists \psi \) defined \( /K \) st
\( A \to B \)
an map \( K/k \) is gadget with group \( G \).
we have \( \varphi^\sigma = \varphi \psi \psi^\sigma = \varphi(p)^\sigma / p \sigma \psi \)
for \( P \in A \), where \( \sigma \) is any extension of \( \sigma \) to the
field in which the coordinates of \( P \) lie. Now \( p \)
is defined \( /K \) \iff \( \forall \sigma \in G \), \( \varphi = \varphi^\sigma \).

Given a pair \((B, \varphi)\) we get an automorphism
of \( A \) (over \( K \)) by taking \( \varphi^{-1} \circ \varphi^\sigma = \alpha \). \( \sigma \in \text{Aut}_K(A) \). Trivial: \( \alpha \cdot \alpha^\sigma = \alpha^\sigma \), so \( \sigma \mapsto \alpha \)
is a cocycle. Question: given a 1-cocycle, does it
come from a \((B, \varphi)\)? Practically yes.
Then: Given a 1-couple $\sigma \to \alpha_\sigma$ of $G$ in $\text{Aut}_K(A)$,
(1) if $\{\alpha_\sigma\}$ comes from $(B, \varphi)$, then $(B, \varphi)$ is unique up to a $K$-isomorphism.
(2) $\{\alpha_\sigma\}$ does come from $(B, \varphi)$ if every finite set of points on $A$ algebraic over $K$ lies on an affine open subset of $A$ which is defined over $K$ (in the same $K$).

Proof for curves, using the function field:
(1) Observe: if we also have $\psi_1, \psi_2: \psi_1^{-1} \psi_2 = \alpha_2 \circ \alpha_1$, so
$\psi_1^\sigma = \psi_2 \circ \psi_1^{-1}$ and $(\psi_1^{-1})^\sigma = \psi_2^{-1} \circ \psi_1^{-1}$ (all $\sigma$) and $\psi_2 \circ \psi_1^{-1}$ is defined over $K$.
(2) For curves: non-singular, complete
$K$ operates on functions by: for $f \in K(A)$,
$f^\alpha(x) = f(x^\alpha)$, for all $x \in K$. $[\alpha^\text{act}$ on $K(A)]$
How do the $x$'s and $x$'s commute? Claim: $x^\sigma = x^\sigma \alpha$, as follows
$x^\sigma = f^\sigma(f^\sigma(x)) = f^\sigma(f^\sigma(x)) = f^\sigma(f^\sigma(x))$.
so $x^\sigma = x^\sigma$.

Let $K = K_0$, $K^\sigma = (K^\sigma_0)$. $x^\sigma \alpha^\sigma = x^\sigma \alpha^\sigma \epsilon$,
$A \to B$ for $f \in K(B)$, $f \circ \varphi \in K(A)$. By construction, $f^\sigma \circ \varphi = (f \circ \varphi)^{\sigma}$
and we claim: $\varphi^\sigma = \varphi^\sigma \alpha$. For all $f \in K(B)$,
$f^\sigma \circ \varphi \circ \alpha = f^\sigma \circ \varphi \circ \alpha$, formally the same
for affine varieties.

Suppose $\varphi^{-1} \varphi = \beta$, $\varphi^{-1} \varphi = \beta_\sigma$
Let $x = \varphi^{-1} x^\varphi$. Now (if $\Gamma$ defined over $K$)
$x^\sigma \alpha = x^\sigma \alpha \epsilon \varphi^\sigma \alpha$ (all $\sigma$), then
$\varphi^{-1} \varphi = \beta$, $\forall \alpha \in \Gamma \Leftrightarrow \{\beta_\sigma\} \sim \{\beta_\sigma\}$ (colored)
$H^1(G_k/k, \text{Aut}_K(A))$ 1-dimensional cohomology set
$H^1$ in 1-1 correspondence with the $K$-isomorphism classes of $B$'s which solve the problem.

Example let $A$ be a subgroup of $\text{Aut}_K(A)$. $\varphi$ is invariant under $A$. Take only $(B, \varphi)$ st $(B, \varphi) \in A$ (all $\sigma$). Correspondingly, take only $K$-isoms $\Gamma: B \to C$ st
$
\alpha = \varphi^{-1} \Gamma \varphi$ lies in $A$.

Example $A/k$, $\alpha \in A_k$. Let $G = \varphi : B \to A$, $\varphi(\alpha) \in A_k$.
$\varphi(\alpha) = \varphi(\alpha) \circ \alpha = \varphi(\alpha) \circ \alpha = \varphi(\alpha)$, so $B$ has a rational point. Now let $A$ be an elliptic curve,
with 0. Suppose \( j \neq 0, 1728 \). \( H'(G, k) \) for quadratic extensions \( k \) in \( K \). \( \text{Aut}_k A \cong \text{Aut}_k (A, 0) \) with some rules for commutations. The translations are the subgroups of \( \text{Aut}_A \), having the divisor classes of degree 0 fixed.

Now \( H'(G, A_k) \) gives certain curves.

Then (ii) Chian curve \( B \) of genus 1, non-singular, \( \bar{k} \) \( \in \bar{K} \) and an ideal over \( A \) of dim 1 (i.e. an elliptic curve with rational point) defined over \( k \), from which \( B \) is gotten via \( H'(G, A_k) \).

2. The \( A \) is unique up to \( k \)-isomorphism. Let \( K, o \in B_k \), \( \alpha = \frac{T_o}{T_0} \) (translation on \( B \) = group with \( o \) as origin).

3-29

\[
A_{\alpha} = A'_{\alpha}, \text{order} A \text{ minimal}. \quad \text{want} \quad A_{\bar{\alpha}} \text{ over} A_{\bar{\alpha}}^{\text{p}}. \quad \text{char} \; k \neq 2, 3, \; j \in \bar{k}.
\]

The case \( j \notin \bar{k} \) can be handled analytically by the previous methods seen before.

\[
y^2 + (a_1 x + a_2) y = x^3 + a_1 x^2 + a_2 x + a_3
\]

\[
y = y + r x + z, \quad x' = x + z \quad \text{or something. At any rate can get in Weierstrass form:} \quad y^2 = x^3 + A x + B.
\]

\[
x = \rho^a x, \quad y = \rho^b y, \quad y' = x^3 + A x + B
\]

\[
a = \rho^a A, \quad b = \rho^b B, \quad \Delta = \rho^{12} \Delta
\]

And for \( p \) a prime, either \( p^y / A \) or \( p^y B \) (equivalent to minimality).

He makes a list of the possible cases. He says (check)

\( j \neq \infty \) means \( \text{ord} \; \Delta = \min \{ 3 \text{ord} a, 2 \text{ord} b \} \)

\( j = 1728 \) \( \text{ord} a = 0 \) non-degenerate already

\[
\begin{array}{cccc}
1 & \pi^{1/4} & \frac{1}{4} \\
2 & \pi^{1/2} & 2 \\
3 & \pi^{3/4} & \frac{2}{3} \\
\end{array}
\]
Case 2  
3rd a > 2 and b
\[ f = 0 \]
\[ \text{ord}\ 0 \]
\[ \text{non\ degenerate} \]
\[ \text{already} \]

Case 3  
3rd a = 2 and b
\[ f = 0 \]
\[ \text{ord}\ a = 0 = \text{ord}\ b, \text{we already have} \]
\[ \text{non-degenerate reduction} \]
\[ \text{Note}\ \delta \in \alpha \Rightarrow a/b^2 \neq 27/4 \]

\[ \text{if } a = 2, \text{and } b = 3. \text{ Take } \rho = \pi \eta, m = 2. \]
\[ K = k(\rho, \eta^2) \]
\[ \text{Let } G = G_{K/k} \]

Now \[ A_k^* = \text{all points not lying to } (0,0) \]
under \( \eta \)-adic reduction. Let \( \sqrt[3]{x/y} \)
Here \( A_k^0 = \text{kernel of reduction map} \): \( A_k \)
\[ A_k/A_k^0 \cong \tilde{A}_k^0 \text{ reduced } \]
\[ y^2 = x^3 + ax + f \]
\[ 2f \geq 4f^2 \]

we have \[ 2f = 3f \]
\[ (\text{impossible or looking closely}) \]
\[ 3f \\let \delta = f^2, x = \delta^2 \]
\[ \text{ie } f < 3, f < 2 \]
\[ \times \eta \]

we have \[ 2\eta = 3f \]
\[ (\text{impossible on looking closely}) \]
\[ 2\delta \geq 4f \]
\[ (\text{impossible, directly}) \]
\[ 2\delta \geq 4f^2 \]
and then \[ 2\delta > 4f^2 > 3f^2, \text{ so } 2f > 2 \eta \text{ (16/3 = 2 + 4/3) so what's wrong? By looking at the equation, } 3f > 2 \eta \text{ not this case!} \]
Thus the claim is proved.

Claim \( G \) takes \( A_k^0 \) to itself, and \( \hat{G} \) have exact
sequence of \( G \)-modules
\[ 0 \rightarrow A_k^0 \rightarrow A_k \rightarrow \tilde{A}_k \rightarrow 0 \]
where \( G \) acts on \( \tilde{A}_k^0 \) as a factor module. What is
\[ 0 \rightarrow A^0_k \rightarrow A_k \rightarrow \tilde{A}_k \rightarrow H^1(G, A_k^0) \rightarrow \]
\[ \text{Now } A_k^0 = A_k^* \]
\[ A_k^0 = A_k \]
\[ \text{if } H^1(G, A_k^0) = 0, \text{ get } 0 \rightarrow A_k^0 \rightarrow A_k \rightarrow \tilde{A}_k \rightarrow 0 \]
\[ \text{by } f^t + m, \text{ } A_k \text{ is uniquely divisible } A_k/A_k^* \]
by \( m \); especially \( \frac{f}{m} \) by order \( G = n. \text{ Thus } H^1(G, A_k) = 0 \)
let $\xi = \rho^{-1}$, a unit in $K$. Then $(X, Y)^\sigma = (\xi^2 X^\sigma, \xi^3 Y^\sigma)$. Now $(\tilde{X}, \tilde{Y})^\sigma = (\xi^2 \tilde{X}^\sigma, \xi^3 \tilde{Y}^\sigma)$ operation on $\tilde{K}$.

We now need the fixed points: assume $V_0$

$(X, Y)^\sigma = (\tilde{X}, \tilde{Y})$.

Remark: if $\tilde{Y} \neq 0$, then $\xi^3 = \tilde{Y}^{-1}$ so $\xi^3$ splits in $L$ if $X \neq 0$, then $\xi^2 = \tilde{X}^{-1}$ so $\xi^2$ splits in $L$.

Because: look at the exact sequence $0 \to (1 + \rho^2) \to L/K \to \tilde{K}^* \to 
\therefore H_1(L/K) = H_1(\tilde{K}^*)$ 
unniquely divisible so $3$ units $\xi^3 \tilde{Y}^{-1} = \xi^3 = \rho^3(\eta^{-1})$, so $\rho^3$ is invariant under $\sigma$ so $\rho^3/\eta$ is in $K$ so $m = 3$. Similarly $X \neq 0 \Rightarrow m = 2$.

What does $m = 6$ mean? $(\tilde{X}, \tilde{Y}) = (0, 0)$ impossible because $\tilde{X} \neq 0$, $\tilde{Y} \neq 0$.

$m = 4$ means $(\tilde{X}, \tilde{Y}) = (0, 0)$.

ord $a = 1$  \[ \begin{array}{c|c}
 m & A_k / A_k \\
 \hline
 4 & \mathbb{Z}/2\mathbb{Z} \\
 2 & \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2 \\
 2 & \mathbb{Z}/2\mathbb{Z} \\
 4 & \mathbb{Z}/2\mathbb{Z} \\
 \end{array} \]

$m = 3$ means $\rho \in K$ so $\rho^3 - 1 = 1$, $\therefore \xi = \tilde{Y}^{\tilde{X}}$ and $b = 1$

for case $m = 2, \tilde{Y} = 0$.

so $\rho \in K$, $\tilde{X}$ is arbitrary on curve, $\therefore$ get the points of order 2 on the curve.

(v) as $\tilde{X}$ is a square or not. 
(\*) as $X^3 + A X + B$ has defined over $\tilde{K}$

0, 1, or 3 zeros in $\tilde{K}$.

If $A$ is a group variety in $K$, and $C$ any variety in $K$, and $\phi : A \times C \to C$ is a map $s + (\phi(a, c) = a \cdot c)$

1. $a \cdot (a_2 \cdot c) = (a_1 a_2) \cdot c$
2. $1 \cdot c = c$
3. $a, c, d \in C$ $\therefore a \cdot c = c$

Then $C$ is a homogeneous space for $A$ over $K$.

$C$ is a principal homogeneous space iff the $a$ in 3. is unique (call it $c_2 c_3^{-1}$). Then the map $C \times C \to A$ given by $(c_1, c_2) \to c_2 c_3^{-1}$ is regular & defined over $K$.

We can speak of isomorphisms classes of principal homogeneous spaces for $A / K$.

The trivial class contains $C = A$, $A \times A \to C$ is trivial iff it has a rational point (ie iff $C_+ \neq \phi$)

If $K/k$ is Galois with group $G$, classes of $\phi$'s
for $A/k$ which are split by $K$ (trivial $/K$; have real point over $K$) are in natural 1-1 correspondence with the elements of $H^1(G, A_K)$. If $c_0 \in C_K$, let $a_0 = c_0 \cdot c_0^{-1}$ a cocycle if $c_0' \in C_K$, & $C_K$ is isomorphic to $C_K'$, get a non-degenerate cocycle. Can be read about in Lang-Tate. Only non-trivial thing is: given 1-cocycle, to find $C$ at $\exists c \in C_K$. Given $\{a_0, a\}$ cocycle, $\exists A \mapsto C$, $A, C / k$; $\varphi / K$;
\[
s + \varphi^{-1} \varphi = \text{right translation on } A \text{ by } a_0 = T_{c_0}
\]
and define $a \cdot c = \varphi(a \cdot \varphi^{-1}(c))$; now need only check $(a \cdot c)^\varphi = a_0 \cdot c_0$. Suppose $C$ is a psh for $A$ & $A'/k$. Then $A, A'$ are isomorphic, $A \cong A' / k$ canonically. Want $f$ s.t $f(a) \cdot c = a \cdot c$. Well, take $c_0 \in C$ over some large Galois ext $K/k$ & define $f$ so that $f(a) \cdot c_0 = a_0 \cdot c_0$, so $(f(a))^\varphi \cdot c_0 = a_0 \cdot c_0$; note $(f(c_0))^\varphi = f(c_0)$. Then $f(c_0 \cdot c_0) = a_0 \cdot c_0 = a \cdot c$, so $f(a) \cdot c_0 = a_0 \cdot c_0$ since $c_0 = b \cdot c_1$, $b \in A$ then $f(a) \cdot (b \cdot c_1) = f(a) \cdot c_0 = a_0 \cdot c_1 = a \cdot (b \cdot c_1) = f(ab) \cdot c_1 = f(a) \cdot (bc_1)$ so $f = \frac{f}{f}$.

If $C$ is defined / $k$ and $C \times C \to C / k$ is a group law, then $C$ is psh for a group / $k$ which becomes isomorphic to $C$ over $K$, ie $3!$ group $A / k$, and structure of psh for $A/k$ on $C$ such that over $K$, one gets just that group law for $C$. Let $c$ be the neutral element, $c \in C_K$; consider the right translation by $c_0$; let $a_0 = T_{c_0}$ & $\text{Aut}_K(C)$. $(a_0)^\varphi = (T_{c_0})^\varphi = ? = T_{c_0}(x_\varphi) = [T_{c_0}(x)]_{x_\varphi} = (x_\varphi)^\varphi = \text{whoops}$ [it looks as if it may not be true] wants to find some rule like $x_\varphi \cdot c_0 \cdot e^{-\varphi} = (xe)_\varphi$ or wants $T_{c_0} \circ T_{c_0} = T_{c_0}$.

"So study of elliptic curves without rational points reduces to the study of elliptic curves with rational points, and their cohomology."

One example: look at R.R. Thm: Suppose $C$ has no rational points, but it does in a quadratic extension: $C/k$ of genus 1, $[k : k] = 2$, then $k \neq 2$, $c_0 \in C_K$, $C_K = \varphi$. I have $(c_0) + (c_0^{-1}) = \varphi$ is a prime divisor of degree 2 in $k(C)$. Now $\exists$ a function with poles $y_\varphi^{-1}$, and we come out with an equation of type
\[
y^2 = a_0 x^q + a_1 x^{q+1} + a_2 x^{q+2} + a_3 x^{q+3} + a_4 = f_d(x)
\]
$a_0 \neq 0, a_i \in k$
\[d = 3 \text{ non-singular elsewhere}
\]
$y/x^2 \sim \sqrt{x_\varphi}$
Our \( A \) is
\[
Y^2 = X^3 + a_3 X + (a_1 - a_2 - 4a_0 a_4) X + (a_0 a_1 + a_1 a_2 - 4a_0 a_2 a_1)
\]
and \( \overline{\gamma} : C \rightarrow A \) is defined by
\[
X = a \sqrt[3]{\beta}, \quad y = 2a_0 X^2 + a_1 X
\]
where \( K = k(\sqrt[3]{\beta}) \).

Points \( P \) on \( C \) ?
\[
\overline{\gamma}(x, y) = \left( \frac{a_1}{\sqrt[3]{\beta} a_0}, \quad 2\sqrt[3]{\beta} \left( a_1 - \frac{a_1^3}{a_0^2} - 2a_0 a_1 \right) \right)
\]
and \( \overline{\gamma}(P) = \overline{\gamma}(P) = P + a ; \quad \phi^* \phi^{-1} = T_a \) (\( \phi = \overline{\gamma}^{-1} \)) so we have the Jacobian.

\[
\mathcal{G} = \mathbb{I}, \quad \sigma^f \quad \text{if} \quad a_1 = 0, \quad a_0 = a \quad a_0 + a_f = 2a_0 = 0
\]
so we need \( a + a_0 = 0 \) (i.e. an elliptic curve that splits if \( a, b \in A_k \) and \( a = \sigma_0 - b \).

Now \( A K / \sigma \) is a finite group generated by \( \sigma \). The

Jacobian substitution: \( x' = x^a \). Now \( a_{n+1} = a_n + a_0 \)
so \( T_{a_{n+1}} a_0 = 0 \) and \( a_0 = \sigma_0 - b \).

\( H' \) (cyclic, \( A \)) = \{ \text{Tr}_a = 0 \} / \{ a_0 = \sigma_0 - b \} \}

Then \( a = (1 + \sigma + \cdots + \sigma^{n-1}) a_0 \). If \( b = (a_0 - 1) b_0 \) and \( b \in A_k \)
then \( b \in A_k \) since \( \sigma^n b_0 = b \).

Note that \( a \) is a rational function of \( a \) if \( a = (a_1, a_2, \ldots) \)
then \( \sigma(a) = (a_1, a_2, \ldots) = \sum(a) \) and \( x \mapsto (\sigma-1)x \),
\( x \mapsto \Sigma(x) - x \) is onto on \( A_k \).

This completes discussion of \( K \)-homogeneous spaces. Now view elliptic curves without rational points as \( K \)-homogeneous curves with a rational point.

Talks more about cohomology. Let \( A_2 = \text{points of order} \),
\( \overline{k} = \text{algebraic closure of} \ k \), and then \( k = 0 \). Now
\( 0 \rightarrow A_2 \rightarrow A_\sigma \rightarrow A_0 \rightarrow 0 \) is exact. Let \( G = G_{\sigma/k} \);
\[
G = \lim \frac{G_k}{G/k}.
\]
Let \( B \) be a \( G \)-module, \( G = G_k = G_{\sigma/k} \); \( G_k/k = G_k / G_{k/k} \),
\( k/k \) finite (??) Let \( B^G = \{ b \in B | \forall g \in G_k, \sigma b = b \} \).
\( B = U \beta B_{G/k} ; \quad A_{G/k} = A_k \).

Consider \( H^r(G_k, B) = \lim H^r(G_{k/k}, B^G) \), \( \sigma \in k \cdot k \)
\( H^r(G_{k/k}, B^G) \) in the usual way for the \( \lim \). For \( r = 1 \), \( \text{infl} \) is injection, so \( \text{infl} \) becomes a union.

Remark: \( \text{If} \ B \) is an abelian group and \( H^1 \) is the set
of equivalence classes of \( K \)-split by \( k \), and \( \text{if} \ b 

going to $L$ no nonequivalent spaces become equivalent, so that $H'(\ldots L) = H'(\ldots K)$ if $B$ is abelian, things become groups.]

Now $0 \to A_2 \to A_2 \to A_2 \to 0$ is an exact sequence of $G$-modules. We get

$$0 \to H^0(G_2, A_2) \to H^0(G_2, A_3) \to H^0(G_2, A_3) \to H^0(G_2, A_2) \to \cdots$$

and then

$$0 \to A_2 \to A_3 \to A_3 \to A_2 \to A_2 \to \cdots$$

and

$$0 \to A_2/k_{\mathbb{A}_2} \to H^1(G_2, A_2) \to H^1(G_2, A_2) \to 0$$

where $A_2/k_{\mathbb{A}_2} = H^1(G_2, A_2)$.

Let $x \in H^1(G_2, A_2)$ correspond to the path $C$; set

index $x = \min \{ k \in \mathbb{N} : x \} \quad$ and order $\alpha = \text{order of } x$.

in the group $H^1$. Now $\text{ord} x | \text{index } x$ for some $n$.

Let $k = C(z^N)$, $A$ defined over $k$. Let $K = C(z_0, z_1)$;
so $K/k$ is cyclic of order $n$, $G_{k_0}$ is cyclic of order $n$

$$z \mapsto e^{2\pi i n z}$$

Now $A_2 \subset A_2 \subset A_2 = A_2$ because

if $A$ is given by $Y^2 = 4X^3 - 2X - 3$ and if $x, y \in C,

C(x, y) \in C(t)$ has genus $1$.

$C(t)$ has genus $0$.

impossible by Luroth.

Note $H^1(G_{k_0}, A_2) = H^1(G_{k_0}, A_2) = \text{Hom}(G_{k_0}, A_2) \cong (A_2)_n$

of type $(n, n)$.

Let $C$ be a curve (complete, nonsingular) defined
over $\Omega$ alg closed. A divisor $\alpha$ on $C$ is $\alpha = \Sigma a_P (P) \in \Omega$.

where $\{P\}$ is the divisor consisting of $P$ alone.

$\deg \alpha = \Sigma a_P \quad \text{Supp } \alpha = \{ P \mid a_P \neq 0 \}$, a finite set

of $f \in \mathcal{O}(C)^*$, $\langle f \rangle = \Sigma a_P (P) \quad \text{deg } \langle f \rangle = 0$ and

$\text{Supp } \langle f \rangle = \{ \text{zeros & poles of } f \}$.

If $P \in \text{Supp } \langle f \rangle$, $f(P) \neq 0$.

Thus $f : C \to \Omega^*$.

or at least $f(C - \text{Supp } \langle f \rangle) \to \Omega^*$.

extends to divisors which are disjoint from $f$; i.e. $f$.

\text{Supp } \langle f \rangle = \emptyset, f(\alpha) = \prod_{P \in \text{Supp } \langle f \rangle} (P)^{a_P}$

Then (if right hand sides defined)

$f(\{P\}) = f(P), f(\alpha + \beta) = f(\alpha)f(\beta), f(g(\alpha)) = f(g(\alpha))$

and $f(c \cdot \alpha) = c f(\alpha)$ and $\alpha f(\alpha) = f(\alpha)$.

If $\alpha$ is of degree $0$, $f(\alpha)$ depends only on the divisor $\langle f \rangle$.

Then $\alpha$ are functions on $C$ and $\text{Supp } f \cap \text{Supp } g = \emptyset$, then

$f((g)) = g((f))$.
Theorem: Let \( A \) be the group of divisor classes of degree \( 0 \) on \( C \). If \( a \in A \) let \( S(a) \) be its class, \( \alpha \).

Define the pairing \( \Delta^* \times \Delta^* \to \mathbb{Z} \) as follows: for \( \alpha, \beta \in \Delta^* \) choose \( a, b \) s.t. \( S(a) = \alpha, S(b) = \beta \) and \( \text{supp } a \cap \text{supp } b = \emptyset \); also \( m_a = (f_a), m_b = (g_b) \). Set \( \text{em}(\alpha, \beta) = f_b / g_a \). This does not depend on our choices (use reciprocity formula): if we also have \( \alpha', \beta' \) we can assume with a short argument that all of \( \alpha, \beta, \alpha', \beta' \) are disjoint. Now \( \alpha' = \alpha + (k), \beta' = (h'^n) = (f'^n) \) (take \( f' = f'^{\Delta^*} \)) and

\[
\frac{f'_b}{g'_a} = (f'^n) = \frac{f_b}{g_a} = \frac{f(a + (h))}{g((a + (h)))} = \frac{f_b}{g_a} \cdot \frac{g(a + (h))}{g((a + (h)))} = \frac{g((a + (h)))}{g(a + (h))} \cdot \frac{f_b}{g_a}.
\]

Also \( \text{em}(\alpha + \beta, \beta') = \text{em}(\alpha, \beta) \cdot \text{em}((\alpha + \beta), \beta') \).

We have \( m_{\alpha + \beta} = (f_f'), m_a = (f), m_{\alpha'} = (f'_f) \).

And \( \text{em}(\alpha, \beta) = \text{em}(\beta, \alpha)^{-1} \) and is always an \( m^m \) root of \( 1 \), i.e. in \( \Delta^* \). Further, \( \text{em}(\alpha, \beta) = 1 \); but this is more difficult to show.

If \( \rho \notin m \), \( A_m \) has order \( m^{2g} \) and \( \Delta^* \) has order \( m \).

Suppose \( C = A \) is an abelian variety of dimension 1. Let \( \alpha = \sum q \alpha p P \), \( S(\alpha) = \sum q \alpha p P \in A \) (addition on curve).
Suppose \( p = m \). For all \( Q \), \( m^2 \) points above \( Q \), so we have a separable covering of degree \( m^2 \). In fact it is an abelian Galois covering with Galois group \( A_m \); \( A = A/A_m \).

If \( a \) is a divisor on \( A \) of degree zero, then 
\[
S(m^*a) = S(m^*a) = S(ma) = mS(a).
\]
Proof: it suffices to consider \( a = [P] - [Q] \). Now (ab use addition)
\[
[S(P) - S(Q)] = mS(a) \quad S(a) = P - Q \quad S(m^*a) = mP - mQ.
\]
Write \( mP = P \), \( mQ = Q \); now \( m^*P = \Sigma_{\alpha = 0}^{[P_0]} [P_0 + \lambda] \),
\[
m^*Q = \Sigma_{\alpha = 0}^{[Q_0 + \lambda]} [Q_0 + \lambda], \quad \text{so} \quad S(m^*a) = m^2P - m^2Q_0 = mP - mQ \quad \text{qed}
\]

Take \( P, Q \in A_m \); how can we interpret \( \mathbb{E}_m(P, Q) \)? Let
\[
P = S(a) \quad m^2a = (f). \quad \text{Now} \quad (m^*f) = m^2(f) = m^2(G(a)) = m^2a \quad \text{and} \quad S(m^*a) = mS(a) = mP = 0, \quad \text{so} \quad (m^*f) \quad \text{equals} \quad \text{a f divisor of a function}. \quad \text{Using closedness of the field,} \quad (m^*f) = m(f) = (f^m), \quad \text{so} \quad m^*f = f^m \quad \text{and for all} \quad x, \quad f(mx) = F(x)^m. \quad \text{Thus the maximal unramified abelian extension of exponent} \quad m \quad \text{is} \quad A \rightarrow A (\text{speaking of function fields}) \quad f(mx) = F(x)^m = F(x + Q)^m \quad \text{and we claim} \quad \forall x, \quad F(x + Q)/F(x) = \mathbb{E}_m(P, Q).
\]

Look \( [X + Q] - [X] \); \( mB = [X + Q] - [X] + (G) \); choose \( B \) s+ ... and apply \( m^*a \).
\[
m^0a = (g).
\]

So \( mB = (g) \); then \( S(mB) = S(m^0B) = S(mB) = Q \). Now want
\[
f(a) = f(mB) = m^2f(g(a)) = f^m(g(a)) = F(mB) = F(x + Q), \quad \text{q.e.d.}
\]

Let \( P \in A_m \); \( [P] - [Q] \); \( m/[Q] - m/[Q] = (f) \); want \( \mathbb{E}_m(P, P, P) \).

Let \( R \neq Q \), \( P \) and let \( g(X) = f(X + R) \). Can see \( m([P + R] - [R]) = (g) \)
\[
S([P] - [Q]) = P = S([P + R] - [R]), \quad \mathbb{E}_m(P, P, P) = (f(R))/(f(R)); (g(0))/(g(P)) = 1.
\]

If \( P_1, P_2 \in A_{m} \), then putting \( P'_1 = n_{11}P_1 + n_{12}P_2 \),
\[
P'_2 = n_{21}P_1 + n_{22}P_2, \quad \text{we have} \quad \mathbb{E}_m(P'_1, P'_2) = \mathbb{E}_m(P_1, P_2)^{n_{22}P_{21} - n_{12}n_{21}}
\]
\[
\text{and:} \quad \text{If} \quad P_1, P_2 \text{is a basis for} \quad A_m \quad \text{then} \quad \mathbb{E}_m(P_1, P_2) \text{is a primitive} \quad m \text{th root of} \quad 1.
\]

If \( A \) is defined \( \mathbb{F}_k \), \( P, Q \in \mathbb{A}_k \Rightarrow \mathbb{E}_m(P, Q) \in \mathbb{F}_k \). If \( A \subset A_k \), then \( k \) contains the \( m \)th roots of 1.
Result: \( H^r(\mathbb{G}_k, A) \) is dual to \( A_k \)

(As noted in the 1957 Bombieri seminar)

First let \( k \) be an arbitrary field, \( A \) an \( A_k \)-

valued \( k \)-algebra, \( G \) a \( k \)-

homogeneous \( G \).

\[ H^r(G, A_k) \times H^s(G, A_k) \to H^{r+s+1}(G, A_k) \]

will become a linear map \( r = 1, s = 0 \).

\[ H^r(G, A_k) \times H^0(G, A_k) \to H^r(G, A_k) \]

(in general, can be very degenerate; in fact, for \( k \) a finite field, by Iwasawa's theorem, \( H^r(G, A_k) = 0 \).

Take \( \alpha \in H^r \), \( \beta \in H^0 = A_k \). Get \( \gamma \in H^r \) by

following: let \( \alpha \) represent \( \alpha \).

Have \( S: \mathcal{S}_0, A_k \to A_k \); can represent \( \forall \sigma \),

\[ a_{\sigma} \in \sigma \in \mathcal{S}_0, \quad \beta \in A_k \to \beta \in \mathcal{S}_0, \quad \text{say} \]

\( f = (\beta) - (\sigma) \), \( \phi f \) could choose \( f \) instead

\[ \phi f \in \varphi f(\sigma) \]

Now, \( (\beta)_{\sigma} = a_{\sigma} - a_{\varphi f} + a_{\sigma} = 0 \)

\[ (\phi f)_{\sigma} = \sigma_{\varphi f} - \sigma_{\sigma} + \sigma_{\sigma} = (\phi f)_{\sigma} \]

for some \( f \) (depending on \( \sigma, \tau \)),

support of \( (\phi f)_{\sigma} \) is disjoint from support of \( \phi f \).

Claim: \( (\phi f)_{\tau} = 0 \).

Thus, \( (\phi f)_{\tau} = \sigma_{\tau} \)

Now, evaluate \( \phi f \)

A degree zero gives zero.

\[ \sigma_{\tau} = \sigma_{\tau} + (\tau - \sigma_{\tau}) \]

\[ c = c(\tau) = c \circ (\sigma_{\tau}) \]

Real problem is to show choice of \( \sigma \) doesn't matter.

\[ \hat{c} = c + (h) \]

\[ c = c(\hat{c}) = c(h) \]

Now, since it doesn't depend on choices, it's clear to a homomorphism \( \hat{c} \).

Let \( \mathbb{A} \) = separable alg closure of \( k \). Let

\[ H^r(A) = H^r(G \times k, A_k) \]

\[ H^r(A) \times H^0(A) \to H^r(A) \]

\[ H^r(A_k) \times H^0(A_k) \to H^r(A_k) \]

(Using \( k \)-splitting)

\[ H^r(A_k) \times H^0(A_k) \to H^r(A_k) \]

\[ H^r(A_k) \times H^0(A_k) \to H^r(A_k) \]

Borel 

\( \mathbb{A} \) of \( k \)
Now look at $\ast \to A_m \to A_n \to A_\ast$ (with $\ast = \text{char } k$).

(1) We can't go to each big square, adding lifts induces the same with $\ast$.

$C \to H^0(A_m) \to H^0(A) \xrightarrow{m} H^0(A) \to H^1(A)$ (by $m$

$\to H^1(A) \to H^1(A) \to H^1(A) \xrightarrow{m} H^1(A)$

Breaking it up,

$\ast \to A_k / mA_k \to H^1(A) \to [H^1(A)]m \to \ast$

(Exact, if $\ast \neq 0$)

Vertical makes by braiding, but middle by

braiding $A_m \times A_m \to \text{Im } \ast \neq 0$ defined

last time. Let $H^1(A_m) \times H^1(A) \to H^1(A) \ast$ explain

with Frobenius, $a \sigma, b \tau \mapsto c m (a \sigma, b \tau) = e \tau$. 

Claim the diagram is commutative or anticommutative. Do it in first square,

let $b \in A_k$, let $a \sigma$ represent $x \in H^1(A_m)$. Take

$\sigma \tau \in G$, $\sigma = (t)$. Take $f(\sigma)$. Take

$b \in B_\ast$, $\sigma \ast m \bar{b} = b + (y)$. Now

$\bar{b} = (\sigma^{-1}) \bar{b}$ use a fun of $\tau \in G$.

call $\bar{S} \bar{e} = \bar{e} \tau \in A_m$

$c_m (a \sigma, b \tau) \mapsto f_{\sigma, \tau}(b \tau)$

Let $m c_{\tau} = h_{\ast}$

$m(\sigma^{-1}) \bar{b} = (\bar{a} \tau \bar{b}) = (h_{\tau}) = m \bar{a} \tau$

$g(\bar{a} \tau \bar{b}) = e_m = g(\bar{a} \tau \bar{b}) h_{\tau} (b \tau)$

$f_{\tau, \tau}(b \tau) = \frac{f_{\tau, \tau}(m \bar{b})}{g(\bar{b} \tau)} = \frac{f_{\tau, \tau}(b \tau)^m}{g(\bar{b} \tau)} h_{\tau} (b \tau) g(\tau \tau)$

$= \frac{[h_{\tau} (b \tau)]^m g(\tau \tau)}{h_{\tau} (b \tau)[g(\tau \tau)]^m g(\tau \tau)} = e_m = \frac{f_{\tau, \tau}(b \tau)}{g(\tau \tau)} h_{\tau} (b \tau)$

$= (\delta m)_{\tau, \tau}$ where $m_{\tau} = h_{\tau} (b \tau) / g(\tau \tau)$

and it commutes!

(1): $k$ a quadratic number field
If a canonical form $H^r(E^*) \cong Q/\mathbb{Z}$, then $E$ is any finite C-alg module (e.g. $E = \mathbb{A}_m^n$), and $F = \text{Hom}(E, E^*) \cong \text{char}(E)$, let $G = \text{graph}$ on $F$. Then $E \times F \rightarrow K^*$ is a C-homming.

Then $H^r(E)$ is of finite order all $r$, $0$ for $r > 2$. Dual homing in all cases.

Let $X(E) = \frac{\text{h}_0(E) \cdot \text{h}_2(E)}{\text{h}_1(E)}$. If $|E|_k = \text{normed abs value (in } k\text{)}$, of the no of elts of $E$.

The order of $E$ exactly.

(3) A subalg $A_k / A_k' \cong \mathcal{O}_k$ (int$_2$) $A_k / A_k'$ is finite diff of first kind, $w = (1 + a_0 + a_1 u + \cdots) du + \cdots$ $a_i \in \mathcal{O}$.

where $a_i, b_i \in \mathcal{O}$

$k$ a $p$-adic ring. $C = C \text{, alg }$, $H^r(C, x) = H^r(C, x)$. Then from

$0 \rightarrow A_m \rightarrow A \rightarrow \mathcal{O} \rightarrow 0$, get

$0 \rightarrow H^r(A_m) \rightarrow H^r(A) \rightarrow H^r(A) \rightarrow H^r(A_m) \rightarrow H^r(A) \rightarrow H^r(A) \rightarrow H^r(A_m) \rightarrow H^r(A) \rightarrow 0$.

$H(A_m)$ is finite.

Let $b_i, c_i$ be order of kernel, cohom of the max $m$ in dim $i$.

$\frac{\text{h}_0(A_m)}{\text{h}_1(A_m)} = b_i \text{, } \frac{\text{h}_2(A_m)}{\text{h}_1(A_m)} = b_i = 1m^2l_k \frac{b_i}{c_i}$

for $\text{h}_i(A_m) = \text{h}_i(A_m)$, since $A_m \in \text{Hom}(A_m, A_m^*)$.

Use the Lie $\mathcal{L}$-module subalg. Let

$\text{ker}(X \rightarrow X) = \text{char}(X \rightarrow X) = (X, m X)$

$0 \rightarrow X' \rightarrow X \rightarrow X'' \rightarrow 0$ is exact.
then \( q_m(X) = q_m(X') q_m(X'') \)
\( q_m(X) = 1 \) if \( X \) is finite.

\[ q_m(H^n(A)) = \frac{c_0}{b_0} = q_m(A_k) = q_m(\varphi_k) = \frac{1}{m k} \]

\[ \frac{c_0}{b_0} = \frac{\times \sqrt{h'(A_m)}}{l} \]

\[ 0 \rightarrow A_k / m A_k \rightarrow H'(A_m) \rightarrow [H'(A)]_m \rightarrow 0 \]

\[ 0 \rightarrow [H'(A)]_m \rightarrow H'(A_m) \rightarrow A_k / m A_k \rightarrow 0 \]

Since \( A_m \) is a finite cyclic group, \( H'(A_m) \rightarrow H'(A_k) \)

\[ A_k / m A_k \rightarrow [H'(A)]_m \]

is injective, but they are finite of the same order \( b_k = c_0 \).

\[ \frac{A_k / m A_k}{H'(A)]_m} \]

Since \( A_k / m A_k \) is rowan.

m was arbitrary, \( e \in \mathbb{N} \) : the pairing

\[ H'(A) \times A_k \rightarrow H^2(A_k) \rightarrow \mathbb{Q}/\mathbb{Z} \]

\[ \frac{H'(A)}{A_k} \]

Have duality, for each \( m \), get duality in the limit:

\[ H'(A) \times A_k \rightarrow H^2(A_k) \]

ie \( H'(A) = \text{Hom}_{\text{cts}}(A_k, \mathbb{Q}/\mathbb{Z}) \) \( (\cong \text{Hom}_{\text{cts}}(A_k, \mathbb{R}/\mathbb{Z})) \]

\[ A_k = \text{Hom}(H'(A), \mathbb{Q}/\mathbb{Z}) \]

\[ A_k = \text{Hom}(H'(A), \mathbb{R}/\mathbb{Z}) \]

\( A_k = \) finite group of order \( p \), home to \( P \times B \)

\( B' / B' \) finite of order \( p' \), \( B' \equiv B_k \).

\[ H'(A) \cong (\text{finite prime to } p) + H'(A; p) \]

\[ H'(A; p) / \text{finite groups} \cong (\mathbb{Q}/\mathbb{Z}_{p})^{[k : Q_p]} \]

\( A_k \) finite \( \mathbb{Q}^1 \) adic no. field.

\[ H'(k, A) \rightarrow H'(k, A) \rightarrow H(k, A) \]

\( H'(k, A) = \) those \( A \) 's split going from \( k \) to \( K \).

\[ A_k \rightarrow A_k, \ 0 \rightarrow H'(K/k, A) \rightarrow H'(k, A) \rightarrow H'(K, A) \]

\[ 0 \rightarrow A_k / m A_k \rightarrow A_k \rightarrow A_k \]
For: \( \bigwedge_{1 \leq i \leq n} \text{Tr}_{k/k} A_k = 0 \)

Cor.: If red. is nondegenerate & \( K/k \) unramified then \( H'(K/k, A) = 0 \).

Proof: By the duality, \( A_k = \text{Tr}_{k/k} A_K \).

Now \( G_{K/k} = G_{\overline{K}/\overline{k}} \), cyclic.

Long: ab over \( \mathbb{F}_q \) finite field: every rational point is the trace of a rational pt (since never have \( \mathbb{F}_q \) points).

\( \text{Tr} \) gets you everywhere mod \( \mathbb{F}_q \). Now claim \( \text{Tr} \) is onto mod \( \mathbb{F}_q^2, \mathbb{F}_q^3 \), etc.

\( A_k \xrightarrow{\text{Tr}} A_{\overline{k}} \quad A_{\overline{k}} \xleftarrow{\text{Tr}} A_{\overline{k}} \)

\( \text{com} \quad \text{com} \quad \text{com} \)

\( \overline{k}^+ \xrightarrow{\text{Tr}} \overline{k}^+ \quad \overline{k}^+ \xleftarrow{\text{Tr}} \overline{k}^+ \)

etc., + onto.

H. S. 3. are given by conts char of \( A_k \),

\( \chi: A_k \rightarrow \mathbb{Q} / \mathbb{Z} \).

Let \( n \) be minimal s.t. \( \chi(A_{\mathbb{F}_q^n}) = 0 \). \( n \) is the conductor of the character.

What does this mean in terms of \( A_k \)'s?

\( n = 1 \) \( \Leftrightarrow \chi \) is char of \( A_k/A_{\overline{k}} \equiv \overline{A}_{\overline{k}} \) if nondeg. reduction.

[If \( \chi \) char of \( A_k/A_{\overline{k}} \) nondeg. reduction, then \( K \)-algebraic \( \chi \in H' \) \( \Leftrightarrow \text{period of } X/\text{ram } K/k \)]

\( A_k \xrightarrow{\text{Tr}} A_{\overline{k}} \quad e = e(K/k) \)

\( \text{com} \quad \text{com} \quad \text{com} \)

\( \overline{A}_{\overline{k}} \xrightarrow{\text{Tr}} \overline{A}_{\overline{k}} \)

\( T_{k/k}(A_{\mathbb{F}_q^n}) \), often in \( A_k \). Take \( N \) mod.

\( e = e(A_{\mathbb{F}_q^n}) \) a function of \( n \) of what kind?
If $k$ an alg. no.fld., $[k:Q] < \infty$, let $A_k$ defined over $k$, form $\prod_x A_{k_x}$. Invert $A_k$ into it.

$$0 \rightarrow A_k \rightarrow \prod_x A_{k_x}$$

$K_k =$ ring of valuation vectors = adic ring

$$0 \rightarrow V_k \rightarrow V(K_k)^\times \subset \prod_x V_{k_x}$$

Weil: $x \in V(K_k)$; eliminate finite number of $x$ affine covering in the original collection thereof s.t. the coordinates therein are integers.

According to Weil's definition, must include all pts in the product $\prod_x A_{k_x}$. [Also Grothendieck's defn.]

Con think of this as the points on $A$ with coordinates in $K_k$. Very fruitful in the theory of affine algebraic groups. In our situation, $A_k$ is usually not finite, $\prod_x A_{k_x}$ is set. $A_k$ is usually not closed in the product.

Look at local theory in the very good case. $k$ a local (i.e. $p$-adic no. fld.), $A_k$ nondeg. redn., $A_m \subset A_k$, $m \neq 0$ (i.e. $x + m$), then get

$$0 \rightarrow A_k/mA_k \rightarrow H'(G_k, A_m) \rightarrow [H'(G_k, A_m)]_m \rightarrow 0$$

since $A_m \subset A_k$, $H'(G, A_m) = \text{Hom}_{cts}(G_k, A_m)$.

$$\begin{cases} \{ \} \\ \cap \end{cases} 0 \rightarrow \text{Hom}_{cts}(G_{Til}, A_m) \rightarrow \text{Hom}_{cts}(G_k, A_m)$$

(for $b$ s.t. $m b = a$), $\sigma \rightarrow (\sigma^{-1}) b = \tau(a)$

This then a map: $G_{Til} \rightarrow A_m$ canonical res of $\text{Hom}(G_{Til}, A_m)$ with $A_m$ by using Frob substitution.

When does an elt of $H'(G_k, A_m)$ come from an elt of $A_k/mA_k$, i.e. when does it go to zero in $[H'(G_k, A_m)]_m$?

$A_m$ has $m^2$ elts, is of type $(m, m)$. 

26/14.
\[ \frac{A_k}{mA_k} \cong \frac{\tilde{A}_k}{m \tilde{A}_k} \quad \text{because} \quad 0 \rightarrow A_k \rightarrow \tilde{A}_k \rightarrow 0 \quad \text{is uniquely dir. by } m \]

\[ 0 \rightarrow A_k \rightarrow \tilde{A}_k \rightarrow 0 \]

Think of vertical lines as zero everywhere else, get homology sequence: get \( A_k / mA_k \cong \frac{\tilde{A}_k}{m \tilde{A}_k} \cdot (A_k)_m \cong (\tilde{A}_k)_m \).

\[ \text{now } m \tilde{A}_k \text{ have all } \ell \text{ of order } m, \text{ is of type } (m,m), \text{ kernel has } m \ell \text{ els, cokernel has } m \ell \text{ els, } A_k / mA_k \text{ has } m \ell \text{ els} \] (not necessarily in general case with same structure as \( A_m \), but here it so!)

\[ \frac{\tilde{A}_k}{m \tilde{A}_k} \cong A_k / mA_k \rightarrow \text{Hom}(C_{T/k}, A_m) = A_m \]

k number field, \( A/k \). Let \( S \) be a finite set of primes of \( k \), including all \( \neq 1, m, \infty, A \) for a particular \( m \). (I = divisor of model of \( A \))

\[ H'(G_k, A) \rightarrow H'(G_{kx}, A) \]

\( 2 \in H'(G_k, A) \) splits at \( y \) iff it goes to zero there.

There is kernel of the map: \( H'(G_k, A) \rightarrow \prod H'(G_k, A) \)

is finite.

Let \( H'(G_k, A; S) = \{ x \in H'(G_k, A) : x \text{ splits outside of } S \} \)

Thm: \[ [H'(G_k, A; S)]_m \cong [H'(C_{T/k}; A_{\text{unr}})]_m \]

where \( \Omega_S = \text{ the maximal elt of } k \text{ unramified outside of } S, \text{ this group is finite } \]

\[ \text{Certainly have a map } [H'(C_{T/k}, A_{\text{unr}})]_m \rightarrow [H'(G_k, A)]_m \]

easily seen that the image is contained in stuff splitting outside \( S \), using \( \Omega_S \) facts about unramified finite extensions where there is non-degenerate reduction.

\[ \Omega_S \text{ in } k = \Omega_S \text{ in } k(A_m) \quad \text{for } S, \text{ the set of primes of } k(A_m) \text{ above the primes in } S. \]
So take $\alpha \in \mathbb{H}'(G_k, A; S)_m$

$$0 \to A_k/m A_k \to H'(G_k, A_m) \to \mathbb{H}'(G_k, A)_m \to 0$$

$$\downarrow \quad \alpha \in \mathfrak{g}$$

$$0 \to A_k/m A_k \to H'(G_k, A_m) \to \mathbb{H}'(G_k, A)_m$$

$\mathrm{Hom}(G_k, A_m)$

$X_y = \text{rest}_{G_k} X, \quad X_y \mapsto 0 \to X_y$ is "irrelevant" as it comes from character of unramified

Now to finiteness of the group. As far as $m$ is concerned, $S$ is almost as good as the algebraic closure. $A \cong \mathbb{Z} \oplus \mathbb{Q}$ as direct limit by $m$ (1)

$$0 \to \mathbb{A}_m \to A_{\mathbb{Q}} \to A_{\mathbb{Z}} \to 0$$

$$0 \to A_k/m A_k \to H'(G_{\mathbb{Q}/k}, A_m) \to H'(G_{\mathbb{Z}/k}, A_{\mathbb{Z}})_m \to 0$$

Prove this finite!

By a little abuse can reduce it to case $A_m \subset A_k$

$$0 \to k(A_m)/k \to \mathbb{Z}/k \to \mathfrak{sl}_2/k(A_m)$$

finite coho.

i.e. can assume $A_m \subset A_k$

$\mathrm{Hom}(G_{\mathbb{Q}/k}, A_m)$ finite?

$= \mathrm{Hom}(G_{\mathbb{Z}/k}, A_m)$ where

$K = \text{maxi abelian ext} \ of \ k$ of extension in unramified outside $S$. Such $K$ has $[K:k] < \infty$ (can use Kummer theory = unit theorem, or class field theory)

$\mathrm{Hom}(G_{k/k}, A_m)$ is finite

Let $X = X(k, A) = \{ \alpha \in H'(G_k, A) \ | \ \alpha \text{ split at all } \}$

$X_m$ finite all $m$. $X_m = \text{ker } [H'(G_k, A; S) \to \prod H'(G_{k_m}, A)]$

the corollary is equivalent to the above theorem (Lang - Tate + Faltings)

Is $X$ finite? Let's 99% certain if $X$ could be proved finite (would be enough $U_n X_{m,v}$ finite for each $m$) then would be a finite method
for getting the group of rational pts on $A$.
Pretty sure $J$ is anti-symmetrised pairing.

$s: X \times X \rightarrow \mathbb{Q}/\mathbb{Z}$ (anti-symmetric)
s.t. $\langle x, x \rangle = 0$ or at least $\exists \langle \alpha, \beta \rangle = -\langle \beta, \alpha \rangle$

$\mathbb{Q}/\mathbb{Z} = H^2 (\text{cycle classes group})$

then $X_m$ becomes dual to $X/\text{mX}$, all $m$.

$[k: \mathbb{Q}] < \infty$, $\omega$ prime to $k$, $K_\omega$ completion.

$K/\kappa$ finite galois, group $G$.

$K_\omega = K \otimes \mathbb{Q}_\omega = \prod_{\lambda} K_{\lambda}$

$A/k: \quad A_{K_\omega} = \prod_{\lambda} A_{K_{\lambda}}$

$0 \rightarrow A_k \rightarrow \prod_{\lambda} A_{K_{\lambda}} \cong \prod_{\lambda} A_{K_{\lambda}}$

in cohom.

$H'(G, A_{K_\omega}) \rightarrow H'(G, \prod_{\lambda} A_{K_{\lambda}}) \cong \prod_{\lambda} H'(G, A_{K_{\lambda}})$

by nature of $K_\omega$,

$H'(G, A_{K_\omega}) \cong H'(G_\omega, A_{K_\omega})$

where $G_\omega$ is the decomposition group at $\omega$, but for almost all $\omega$, $H'(G_\omega, A_{K_\omega}) = 0$.

$\prod_{\lambda} H'(G, A_{K_{\lambda}}) = \prod_{\lambda} H'(G_\omega, A_{K_{\lambda}})$

$0 \rightarrow X_{K_{1/\omega}} \rightarrow H'(G, A_k) \rightarrow H'(G, \prod_{\lambda} A_{K_{\lambda}})$

$\kappa$-ho is $\omega$-split at $K$ + at every prime $\lambda$ of $K$.

Describe a pairing

$X_{K/\kappa} \times X_{K/\kappa} \rightarrow H^2 (G_{K/\kappa}, \Sigma) \rightarrow \mathbb{Q}/\mathbb{Z}$.

Letting $K \rightarrow \kappa$, check its consistent with inflation to get $X \times X \rightarrow \mathbb{Q}/\mathbb{Z}$.

$X = \mathbb{Z}$ is represented by $a \in \omega G(A_k)$

$s: \forall \gamma, a = \delta a \gamma, a_\gamma \in \mathbb{Z}^0 (G, A_{K_{\gamma}})$

$a = S(a), \omega a$ a $1$-cochain divisor of degree

zero in $K$.

$a = S(\delta \gamma) \gamma \in K_\gamma$

($S$ the sum from divisors of degree $0$ to $\gamma$ points).

$\gamma = \delta \gamma + (\gamma)$ where $\gamma \in K$ is a $1$-cochain of
tors defined $/K_\gamma$. 
\[ \delta \alpha = (f) = \delta (\psi \psi), \quad \delta \beta = \delta \beta \psi + (\psi \psi) \]

\[ \delta \beta = (g) = \delta (\psi \psi) \]

\[ (\alpha, \beta) \mapsto \langle \alpha, \beta \rangle = \chi \in H^2(G, \Gamma_k) \]

\[ L = \chi + \gamma - \psi \psi \psi \psi \]

\[ \delta \chi = \partial \psi \psi \psi \psi - \gamma - \psi \psi \psi \psi \]

\[ f(x) = \langle x, \chi \rangle \mapsto \chi \text{ (lifted induced by this pairing)} \]

Now write everything additively:

\[ f(x) = \delta \psi \psi \psi \psi + \psi \psi \psi \psi \]

\[ f(y) = \psi \psi \psi \psi \]

\[ c \mapsto \text{a 2-cochain in } K^*_x, \text{ each } c \]

\[ H \text{ can make choices s.t. } c_x \in H^1, \text{ almost all } x, \]

\[ H = \prod_{x} H_x, \text{ then } c = (c_x) \text{ would be a 2-cochain in } \pi \text{ of cocycles}. \]

But using these formulas, state clue of \( c \):

\[ (\delta c)_x = \delta (\partial \psi \psi \psi \psi + \psi \psi \psi \psi) = \delta (\psi \psi \psi \psi + \psi \psi \psi \psi) = 0 \]

\[ \implies \delta f = 0 \text{ in } K^*_x \]

\[ \text{its class is a cocycle}, \quad \delta c = 0 \text{ in } \pi \text{ of cocycles}. \]

Formally, except for questions of when things are defined, independent of choice.

Also, \( \langle \alpha, \beta \rangle = -\langle \beta, \alpha \rangle \), probably \( \langle \alpha, \alpha \rangle = 0 \),

doesn't change under inflation *looks non-trivial*.

Conjectures: 1. This process gives canonical \( X \times X \rightarrow \mathbb{Q}/\mathbb{Z} \) with \( \langle \alpha, \alpha \rangle = 0 \)

2. \( \{ \alpha \in X \mid \forall \beta \in X, \langle \alpha, \beta \rangle = 0 \} = mX \)

or \( \{ \alpha \in X_m \mid \forall \beta \in X, \langle \alpha, \beta \rangle = 0 \} = mX \times X = X_m \times mX_m \)

[Cuscelo: On a conjecture of Selmer, Crelle, Fall 1959]

Considering \( x^3 + y^3 = d z^3 \) (3 = 0)

\( \text{Num} (A, A) \text{ contains } \sqrt{3} = \rho, \text{ so that } \rho^2 : A \rightarrow A \)

\( \rho^2(p) = -3 p \)

Let \( m \in M^{(1)} \); \( m \in M^{(2)} (\implies U(m, m) = 1) \) all \( m \in M^{(1)} \)

\( \text{of form } 0(\bar{m}) \text{ for some something}. \)

Note to self: that this statement is:

\[ \forall \alpha \in X \mid \forall \beta \in X, \langle \alpha, \beta \rangle = 0 \implies X_0 \times \rho X \]

Proof: methods of global class field theory with...
some local theory]

\[ 0 \to A_k / m A_k \to H'(G_k, A_m) \to [H'(G_k, A)]_m \to 0 \]

\[ \to [\Sigma \text{H}'(G_k^m, A)]_m \]

get

\[ 0 \to A_k / m A_k \to H'_X(G_k, A_m) \to X_m \to 0 \]

\[ H'(G_k^m, A_m) \]

\[ H'_X(G_k, A_m) \text{ is constructible finitely.} \]

But shee conjecture is true: shee \( \alpha, \beta \in H'_X(G_k, A) \)

Let \( S_m < H'_X \) s.t. \( H'_X / S_m \equiv X_m / m X_m \cap X_m \)

Take \( m, m^2, m^4, \ldots \)

\[ X_m / m X_m \cap X_m \text{ increases its order (can't do),} \]

Call the order \( \pi(m) \). \( \pi(m^2) \leq \pi(m^4) \leq \pi(m^4) \).

Conjecture #: \( X \) is finite

\[ \pi(m^n) \text{ becomes const at } m^n \iff X_{m^n} = X \]

If \( A/k \) is finite with \( g \) elts, \( (A : o) = N \),

\[ |N - (g + 1)| \leq 2g \sqrt{g} \]

Generally, if \( A \) is of genus \( g \), \( A_k = N \), then

\[ |N - (g + 1)| \leq 2g \sqrt{g} \]

If \( C \) is complete nonsingular of genus \( g \). \( C \times C \)

is a surface, \( \Delta \subset C \times C \). A mesh of \( C \to C \)

has graph, consider the mesh \( x \mapsto (x^{(g)}) \)

Points wth \( 1/k \) are pts of intersection of \( \Delta \) with

the graph. Call graph of mesh \( \phi \), \( N = \Delta \cdot \phi \).

Let \( X \) be a nonsingular surface

defined over an alg. closed \( k \).

If \( A, B \) are two smooth curves on \( X \)

\( p \in A \cap B \)

let \( O = O_p, x \) : ring of fens wth no hole at \( p \)

Take \( a, b \in O_p, x \) s.t. \( a = 0 \) is local equation for \( A \)

\( b = 0 \)

\( (a) = A + \ldots \) other things not going thr' \( p \)

\( (b) = B + \ldots \)

\( (a) = A + D \), \( p \notin D \) with \( D \).
\(a, b\) determined \(ab\) to units (the ideal \(a, 0\) is determined).

Look at \((a, b) = a \mathfrak{o} + b \mathfrak{o} \subset \mathfrak{O}_\mathfrak{p}, x\)

\[ i(\mathfrak{A}, \mathfrak{B} \text{ at } \mathfrak{P} \text{ on } X) = \dim_{\mathfrak{A}} (\mathfrak{O}/a \mathfrak{o} + b \mathfrak{o}) \]

\[ \mathfrak{P} X \mathfrak{o} + b \mathfrak{o} = \mathfrak{m} \subset \mathfrak{O}, \mathfrak{m} \text{ mod ideal} \]

\(kX\) higher.

\[ i(\mathfrak{A}, \mathfrak{B} \text{ at } \mathfrak{P} \text{ on } X) = \sum_{i=0}^{n} (-1)^i \dim_{\mathfrak{A}} (\mathfrak{O}/(0/\mathfrak{m}, 0/\mathfrak{I})) \]

\(2\mathfrak{o} = \mathfrak{O}/\mathfrak{o} \otimes \mathfrak{O}/\mathfrak{l} = \mathfrak{O}/\mathfrak{o} + \mathfrak{l} \)

Can look at it asymmetrically: \(A\) has a desingularization, \(A \xrightarrow{k} A\).

Claim: \(i\) also equals \(i = \sum_{\mathfrak{q}(q) = \mathfrak{p}} \text{ord}_\mathfrak{q}(\mathfrak{a} + \mathfrak{b}) \)

\((\mathfrak{a} + \mathfrak{b} = \mathfrak{b} + \mathfrak{a})\).

\(0/\mathfrak{a} \mathfrak{O} \equiv \text{local ring of } \mathfrak{P} \text{ on } A = \mathfrak{O}_\mathfrak{p}, A\)

\(0/\mathfrak{a} \mathfrak{O} + \mathfrak{b} \mathfrak{O} \equiv \mathfrak{O}_\mathfrak{p}, \mathfrak{A} / b_\mathfrak{A} \mathfrak{O}_\mathfrak{p}, \mathfrak{A} \)

\(b_\mathfrak{A} = b_\mathfrak{A} \mathfrak{A} = b + a \mathfrak{O} \)

\(\mathfrak{O}_\mathfrak{p}, \mathfrak{A} \subset \mathfrak{I}(\mathfrak{A}) \equiv \mathfrak{I}(\mathfrak{A}) \)

\(\mathfrak{O}_\mathfrak{p}, \mathfrak{A} \subset \mathfrak{I}(\mathfrak{A}) \)

What is relation between \(\mathfrak{O}_\mathfrak{p}, \mathfrak{A} + \mathfrak{O}_\mathfrak{q}, \mathfrak{A}\)?

\(\mathfrak{q}(\mathfrak{q}) = \mathfrak{p}, \mathfrak{q}, \mathfrak{A} \supset \mathfrak{O}_\mathfrak{p}, \mathfrak{A}\) (r, of finite codim)

\[ \sum_{\mathfrak{q}(\mathfrak{q}) = \mathfrak{p}} \text{ord}_\mathfrak{q}(\mathfrak{a} + \mathfrak{b}) = \sum \dim_{\mathfrak{q}}(\mathfrak{O}/b_\mathfrak{A} \mathfrak{O}) \]

\[ \dim_{\mathfrak{q}}(\mathfrak{O}/b_\mathfrak{A} \mathfrak{O}) \]

\[ \mathfrak{O}_\mathfrak{p}, \mathfrak{A} \rightarrow \prod_{\mathfrak{q}(\mathfrak{q}) = \mathfrak{p}} \mathfrak{O}/\mathfrak{q}, \mathfrak{A} \supset \prod_{\mathfrak{q}} b_\mathfrak{A} \mathfrak{O}/\mathfrak{q}, \mathfrak{A} \]

\[ \dim_{\mathfrak{q}}(\mathfrak{O}/b_\mathfrak{A} \mathfrak{O}) \]

\[ \mathfrak{O}_\mathfrak{p}, \mathfrak{A} \supset b_\mathfrak{A} \mathfrak{O}_\mathfrak{p}, \mathfrak{A} \rightarrow \prod_{\mathfrak{q}} b_\mathfrak{A} \mathfrak{O}/\mathfrak{q}, \mathfrak{A} \]

\[ \dim_{\mathfrak{q}}(\mathfrak{O}/b_\mathfrak{A} \mathfrak{O}) \]
Theorem: If $f = bA \phi$, $\phi \in \mathcal{O}_A$, and $g \in \mathcal{O}_A$, then $\sum_{\mathfrak{p}|\mathfrak{q}} \operatorname{ord}_\mathfrak{q}(bA) = \sum_{\mathfrak{p}|\mathfrak{q}} \operatorname{ord}_\mathfrak{q}(f)$.

Let $A \cdot B$ be the $\mathfrak{p}$-th degree of $\mathfrak{p} \in \mathcal{A}$, where $\mathcal{A}$ is the linear combination of divisors $A$ and $B$. For any divisor $B$, the degree of $A \cdot B$ only depends on the linear equivalence class of $B$. If $B \sim B'$, then $A \cdot B = A \cdot B'$.

Now, let $A \cdot B$ be the sum of $A_i \cdot B$, where $A_i$ are distinct elements of $A$ and $B$. Additive in each argument. $A \cdot B$ is additive in each argument. $A \cdot B$ depends only on the linear equivalence class of $A$ and $B$.

On any surface $X$, if $A$ is a canonical divisor class, $K_X = \mathfrak{p}$-th divisor of a double diff on $X$.

Let $A$ be a nonsingular curve on $X$. Choose a set of vanishing to order 1 on $A$. $A = (x) + A'$, where $A'$ has no chs in common with $A$. 

\[ A = (x) + A' \]
A 

A : A = A : A₀ , good interaction.

For double diffuse on X, define T⁻¹ w = w', single diffuse on A; for P where t = 0 is a local equation, can choose as uniformizing parameters t, u.

w = f dt du

Def: w' = f du restricted to A, = fdu |ₐ doesn't depend on u.
If f dt du = g dt dv, then fdu - gdv restricts to 0 on A. Set 0.

Thm: \( (w') = ((w) + A₀) : A \) as a divisor on A.

Take degrees: \( 2g - 2 = K_A + A₀ \), \( K \) any divisor on X, define \( p_a(V) \) = "virtual arithmetic genus of \( V \)"

\[ p_a(V) = 1 + \frac{K_A + A₀}{2} \]

If \( V \) is nonsingular irreducible, \( p_a(V) = g_V \) irreducible, singular:

\[ p_a(V) = g + \sum \frac{m_i (m_i - 1)}{2} \]

\[ = g + \sum \dim \left( O_{P_i} / O_{P_i} \right) \]

Beyond: Take \( X \) to be the plane, \( X = \mathbb{P}^2 \), \( A \sim B \)

\( \iff \) \( \deg A = \deg B \).

\( A : B = \deg A \deg B \) \( (A₀ : B₀) \) where \( \deg A₀ = \deg B₀ = 1 \).

= \( \deg A \) \( \deg B \)

an \( m \)-deg curve meets an \( n \)-deg curve in \( mn \) pts.

(\( \deg K = 3 \))

A nonsingular plane curve of deg \( m \) \( \Rightarrow \) \( g_A = 1 + \frac{-3m^2 + m}{2} \)

= \( \frac{(m-1)(m-2)}{2} \)

\( X \) surface, \( A, B \) divisors on \( X \); \( A : B = \) tot int

multiplicity: \( A^t = A : A \)

If \( K \) is canonical divisor on \( X \),

\[ 2p_a(X) - 2 = A^t + A : K \]

Thm: If \( A \) linear, then \( p_a(A) = \) genus of \( A \) as a curve with

singularities, \( p_a(A) = g(A) + \sum \left( \frac{1}{\deg O_{P_i}} \right) \)

\( \sum \left( \frac{1}{\deg O_{P_i}} \right) \)
\[ A = \text{normalization of } A. \]

Riemann-Roch for nonsing curve \( C \):
\[
\l(\sigma) = \deg(\sigma) + 1 - g + \l(v - \sigma), \quad \text{if } v \text{ can divisor on } C \]

\[
\l(\sigma) = \dim \{ f \mid f(\sigma) \geq \sigma \} = \dim \l(\sigma) \]

\( \mathcal{O}_C \) = structure sheaf of \( C \), sheaf of germs of regular functions; stalk of \( p \) is local ring at \( p \).
\( \mathcal{O}_C(\sigma) \) = sheaf of germs of rational functions for \( C \), \( (f) \geq -\sigma \)

\[
\l(\sigma) = H^0(C, \mathcal{O}_C(\sigma)) \quad (\text{eg } \mathcal{O}_C(0) = \mathcal{O}_C)
\]

\[
\l(\sigma) = \dim H^0(C, \mathcal{O}_C(\sigma)) = \sum_{i=0}^\infty (-1)^i \dim H^i(C, \mathcal{O}_C(\sigma)) = \deg \sigma + 1 - g
\]

Can do the same thing for surfaces.
\( \mathcal{O}_x(D) \), for a divisor \( D \) on \( X \) : all \( f > 0 \) \( (f) \geq -D \)

\[
X(x, \mathcal{O}_x(D)) = \frac{1}{2} D(D-K) + \text{pa}(x) + 1
\]

(\( R \)-Roch for divisors on a surface)

\[
\l(D) - \dim H^0(X, \mathcal{O}_x(D)) + \dim H^0(X, \mathcal{O}_x(D)) = \frac{1}{2} D(D-K) + \text{pa}(x) + 1
\]

\[
\dim \l(D) = \dim H^0(X, \mathcal{O}_x(D)) + \dim H^0(X, \mathcal{O}_x(D)) = \frac{1}{2} D(D-K) + \text{pa}(x) + 1
\]

get \( R \)-R inequality,

\[
(*) \quad \l(D) + \l(K-D) \geq \frac{1}{2} D(D-K) + \text{pa}(x) + 1
\]

Lemma:
Let \( D \) be a divisor on \( X \), \( D^2 \geq 0 \). Then replacing, if necessary, \( D \) by \( -D \), we will have \( \l(-nD) = 0 \) for all \( n > 0 \). Then for each divisor \( C \), we will have \( \l(C-nD) = 0 \) for large \( n \), \( n \) \( \to \infty \)

(\( \text{Grothendieck, JfRuAM, Note or Mathis, Fall 1957} \))

4.
Let \( m, n > 0 \). Claim: it impossible that

\[
\l(nD) > 0 = \l(-nD) > 0. \quad \text{Hypothesis means } mD \sim E > 0, \quad -mD \sim E' > 0; \quad mD \sim mE \geq 0, \quad -mD \sim mE' \geq 0, \quad 0 \sim mE + mE' \geq 0, \quad nE = -mE' \sim mE = 0. \quad 0 = nE' = \n^2 m^2 D^2 > 0, \text{ impossible.}
\]

Thus, \( \text{claim verified} \).

Apply \( R \)-R inequality (\( *) \), \( \l(-nD) \):

\[
\l(nD) + \l(K+nD) \geq \frac{1}{2} D^2 + \frac{1}{2} D \cdot K + \text{pa}(x) + 1
\]

\[
\to \quad \l(K+nD) \to \infty \approx n \to \infty
\]
Given any divisor $C$, choose $n$ large enough so that $l(K+nD) > l(C+K)$. Claim $l(C+nD) = 0$ for any such $n$. If not, $E \sim C-nD$, $E \geq 0$.

If $E \sim K+nD$, $E \geq 0$.

$E \geq 0 : l(D+E) \geq l(D)$ since $l(D+E) > l(D)$.

$l(C+K) = l(E+K+nD) \geq l(K+nD)$, contradicting above inequality. $l(C+nD) = 0$ for large enough $n$.

Now to finish, apply $R \cdot R$ to $C+nD$:

$l(C+nD) + l(K-C-nD) = \frac{n}{2} D^2 + \text{const} \cdot n + \text{const}$

$\to \infty$ with $n$, qed to lemma.

Then (Hodge, with harmonic integrals, in 1937, in classical case, then by Segre + Petrovsky in abstract case 1938). A, D divisors on complete non-singular $X$. $A^2 > 0$, $AD = 0 \Rightarrow D^2 \leq 0$.

By Grothendieck. First for special kind of $A$: let $H$ be a hyperplane section.

(Rote, all hyperplane sections are linearly equivalent.) (If $A$, $B$ have no common chts, $A > 0$, $B > 0 \Rightarrow A \cdot B > 0$)

If $E \geq 0$, then $HE > 0$ since can move $H$ by linear equivalence so that $H$, $E$ have no common chts.

If $l(D) > 1$, then $H \cdot D = 0$.

$H^2 > 0$, $D \cdot H = 0 \Rightarrow \pm n D \cdot H = 0$ all $n$. $l(\pm n D) \leq 1$ all $n$.

It is impossible that $D^2 > 0$, $D^2 \leq 0$.

If $A^2 > 0$, $DA = 0$, put $u = AH$, $d = DH$ then ($uD - dA$) $H = 0$. $a^2 D^2 + d^2 A^2 = (uD - dA)^2 \leq 0$.

$0 \neq 0 + D^2 \leq 0$.

(inequality of Castelnuovo- Severi). Let $C_1$, $C_2$ be two complete nonsingular curves, let $D$ be a divisor on $X = C_1 \times C_2$.

Let $d = D \cdot C_2 = D \cdot (p_2 \times C_2)$ = degree of $D$ over $C_2$.

$d_2 = D \cdot C_1 = D \cdot (p_1 \times C_1) = \cdots C_1$.

Then $D^2 \leq 2d_1 d_2$.

Consider $C_i$ as embedded in $C_1 \times C_2$. $C_i^2 = 0 = C_i \cdot C_2 = 1$.

Take $A = C_1 + C_2$, $A^2 = 2 > 0$. 
\[ \text{let } D = D^* + d_1 c_1 + d_2 c_2 \quad (\text{def of } D^*) \]
\[ D^* c_1 = 0 = D^* c_2 \]
\[ D^2 + 2 \leq 0 \text{ by Hodge's Index Thm} \]
\[ D^2 = \frac{D^*}{D} \quad \therefore D^2 \leq 2 d_1 d_2 \]

Put \[ Q(D) = 2d_1 d_2 - D^2 \geq 0 \text{ all } D \text{. It behaves in a quadratic way.} \]
(\[ B(D, D') = d_1 d_2 + d_1 d_2 - D D' \text{, the bilinear form associated to } Q \])

Now consider two regular maps
\[ \varphi, \psi : C \rightarrow C_1 \text{ graphs } \Phi, \Psi \subset X = C_1 \times C_2 \]
\[ \Phi, \Psi \equiv C_1 \text{ as curves.} \]
\[ Q(m \Phi + n \Psi) = \alpha m^2 + 2 \beta m n + \gamma n^2 \geq 0 \text{ (all } m,n) \]
\[ \beta^2 - 4 \gamma \leq 0 \]
\[ B(\Phi, \Psi)^2 \leq B(\Phi, \Phi) B(\Psi, \Psi) = Q(\Phi) Q(\Psi) \]
\[ \deg \varphi, \deg \psi \text{ are the degrees of } \Phi, \Psi \text{ rest } / C_2 \]
\[ (\deg \varphi + \deg \psi - N)^2 \leq (2 \deg \varphi - \Phi^2)(2 \deg \psi - \Psi^2) \]

\[ (N = \Phi \cdot \Psi = \text{no. of fixed pts } \varphi = \Psi \text{ with multiplicities counted}) \]
\[ \Phi^2 = 2 g_1 - 2 - \Phi \cdot K \]
\[ K \text{ canonical on } X \]
\[ \Phi \cdot K = 2 g_1 - 2 + \deg \varphi (2 g_s - 2) \]
\[ \Phi^2 = - \deg \varphi (2 g_s - 2) \]
\[ 2 \deg \varphi - \Phi^2 = 2 g_s \deg \varphi \]
\[ (\deg \varphi + \deg \psi - N)^2 \leq 4 g_s \deg \varphi \deg \psi \]
\[ 1 \deg \varphi + \deg \psi - N \leq 2 g_s \sqrt{\deg \varphi \deg \psi} \]

Now let \[ C_1 = C_2 \text{, } \Psi = 1 \]
\[ 1 + \deg \varphi - N \leq 2 g_s \sqrt{\deg \varphi} \]
\[ N \text{ becomes no. of fixed pts of } \varphi : C \rightarrow C \text{. If } C \text{ is defined over a field with } q \text{ elts, define } \]
\[ \varphi(x_1, \ldots x_n) = (x_1^q, \ldots x_n^q) \]
\[ \deg \varphi = q \quad 1 + q - N \leq 2 g_s \sqrt{q} \quad N = \text{no. of its rant / k} \]

What does this result have to do with the Riemann Hypothesis.
Define \( S(s) = \sum_{\mathfrak{n}} \frac{1}{(N\mathfrak{n})^s} = \prod_{\mathfrak{p}} \frac{1}{1 + (N\mathfrak{p})^s} \) for real \( s > 1 \).

For running the nonzero ideals in \( \mathbb{Z} \)

- \( N\mathfrak{n} = \# \text{ elts of } \mathbb{Z}/\mathfrak{n} \). 
- \( N \) is the unique function so \( N\mathfrak{a} N\mathfrak{b} = N(\mathfrak{a} \mathfrak{b}) \) and \( N\mathfrak{p} \) is the number of elts in \( \mathbb{Z}/\mathfrak{p} \).

The formal identity comes from unique factorization.

Consider in domain \( \mathbb{R}(s) > 1 \) is easy to show. Can do it for any no. field \( K \); get \( S_K \); take all \( s \) for \( K \), or all \( s \) for \( K \). Has analytic continuation over all the \( s \)-plane \( C \), except for a simple pole at \( s = 1 \); get

\[
S(1-s) = \left(\frac{\pi}{\sin \pi s}\right) \Gamma(s) S(s) \quad \Gamma(s) S(s) = \Gamma(s) \frac{S(s)}{S(s)}
\]

Except for trivial zeros coming from the \( \Gamma \) factor, \( \mathbb{R} \) zeros outside of \( 0 \leq \Re s \leq 1 \).

If \( K \) is a non-field with non-field \( K_0 \) with \( \mathbb{R} \) elts, define \( S_k \). Define

\[
S_k(s) = \left(\sum_{\mathfrak{p} \in \mathfrak{p}_0} \frac{1}{(N\mathfrak{p})^s} \right)
= \prod_{\text{prime ideal } \mathfrak{p}_0} \frac{1}{1 + (N\mathfrak{p}_0)^s}
\]

where \( N\mathfrak{p}_0 = \deg \mathfrak{p}_0 \)

\[
N\mathfrak{p} = \mathfrak{q} \deg \mathfrak{q}
\]

\[
N\mathfrak{a} = \mathfrak{q} \deg \mathfrak{a}
\]

\[
S_k(s) = \sum_{n=0}^{\infty} D_n q^{-ns} \quad \text{where } D_n = \# \mathfrak{a} \text{ of } \mathfrak{a} \geq 0, \deg \mathfrak{a} = n.
\]

We have a zeta function involving \( Z(u) = Z(\frac{1}{2}u) \).

Let \( \mathcal{A} \) be a linear class. R. R. says that \# of \( \alpha \in \mathcal{A} \) such \( \alpha \geq 0 \) is

\[
\frac{q^{d(A)}}{q - 1}
\]

Let \( d(A) = \text{dim} \mathcal{A} \) for \( \alpha \geq 0 \) for \( \alpha \in \mathcal{A} \).

Claim: \( \forall \mathcal{A}, \ D_n \neq 0 \)

Assume: \( \exists \text{ a divisor of degree } 1 \) for \( n > 2q-2 \).

Then by R. R.,

\[
l(A) = \deg(A) + 1 - q + \ell(\mathfrak{p} - A)
\]

If \( \deg A > 2q-2 \),

Then each class of degree \( n \) has \( \frac{q^{n+2q-3}}{q-1} \) divisors.
No. of classes of degree \( n = \text{no. of classes of degree } 0 = h < \infty \)

\[ D_n = \frac{h^n q^{n+1} - 1}{q^{n+1}} \quad \text{for } n > 2g - 2 \quad \therefore \quad Z(u) \text{ is a rt function of } u. \]

\[ Z(u) = \frac{h}{q-1} \left( \frac{1-u}{1-q u} \right) + \text{polynomial of degree } \leq 2g - 2 \]

for \( 1/4 < \frac{1}{2} \) i.e. \( \text{Re}(u) > 1, \) has poles at \( u = \frac{1}{q}, \) \( u = 1. \) Residues are \( \frac{h}{q-1} \) at \( u = 1 \)

\[ = \frac{h}{q^g} (q-1) \text{ at } U = \frac{1}{q}. \]

One proves the functional equation for \( Z \) by relating \( D_n \) and \( D_{2g-2-n} \) for \( 0 \leq n < 2g-1 \)

One gets \( Z(\frac{1}{q} u) = q^g u^{2g-2} Z(u) \) (by R.R.)

\[ P(u) = q^g u^{2g} P(\frac{1}{q} u), \text{ so that } P \text{ must be of degree } 2g, \] \[ P(0) = 1, \quad P(1) = h. \]

\[ P(u) = \prod_{i=1}^{2g} (1 - \alpha_i u). \]

R.H. Hypothesis says: \( \prod_{i=1}^{2g} \alpha_i = \sqrt{q} \)

\[ Z(u) = \frac{\prod_{i=1}^{2g} (1 - \alpha_i u)}{(1-u)(1-q u)} \]

\[ = Z(u) = 1 + D_1 u + \ldots \]

\[ = 1 + (1+q - \sum_{i=1}^{2g} \alpha_i) u + \ldots \]

\[ D_1 = 1+q - \sum_{i=1}^{2g} \alpha_i = \text{no. of frames of degree } 1 \]

\[ Z(u) = \prod_{x} \left(1 - u^\deg(x)^{-1}\right) \]

\[ \frac{Z'(u)}{Z(u)} = \sum \frac{\deg(x) \cdot u^{\deg(x) - 1}}{1 - u^\deg(x)} = \sum \left( \sum_{n=0}^{\deg(x)} E_n \cdot u^n \right) \]

Coeff of \( u^{m-1} = \text{no. of rt frames over } \mathbb{K}_{m-1} = N_m \]

\[ \left( \frac{z_m}{z(u)} \right) = \sum_{m=1}^{2g} N_m u^m / u; \quad \text{Comparing} \]

\[ \sum_{i=1}^{2g} \alpha_i^m \]

We know that \( \left| \sum_{i=1}^{2g} \alpha_i^m \right| \leq 2g \sqrt{2g} = 2g q^{m/2}. \]

Know that

\[ \prod \alpha_i = q^g. \quad \text{Oh well . . . . . .} \]