Problem 1.1. Let X be a curve and let $P \in X$. Show there is a function in $f \in K(X)$ such that f is regular at every point except P.

Proof. Let g be the genus of X. We know from 1.3.3 that for $n \gg 0$, we have $\ell(nP) = \deg(nP) + 1 - g$. Thus for $n \gg 0$, we have $\ell(nP) = n + 1 - g$ and therefore for $n \gg 0$ we know $\ell(nP) > 1$. Thus there is an $f \in \Gamma(X, \mathcal{L}(nP)) \subseteq \mathcal{K}(X)$ such that $v_P(f) \geq -n$ and $v_Q(f) \geq 0$ for all $Q \neq P$. Specifically, since $\ell(nP) > 1$, there is an $f \in K(X)$ such that $v_P(f) < 0$, and therefore f has a pole at (and only at) P. $\square$

Problem 1.5. Let D be an effective divisor. Show that $\dim |D| \leq \deg D$, and equality holds if and only if $D = 0$ or $g = 0$.

Proof. First note that $\dim |D| = \ell(D) - 1$. We claim that for every effective divisor D, $\ell(D) \leq \deg D + 1$. We can see this by choosing $P \in X$ and letting $n = \deg D$ and defining $D' = D - (n+1)P$. Then $\deg D' = -1$ and so $\mathcal{L}(D') = 0$. We know that $\dim(\mathcal{L}(D)/\mathcal{L}(D')) \leq \deg(D - D') = n + 1$, and so $\ell(D) \leq n + 1$.

Since $\ell(D) \leq \deg D + 1$, we can see that $\dim |D| = \ell(D) - 1 \leq \deg D$.

($\Leftarrow$) Now assume that $D = 0$. Then $\deg D = 0$ and $\ell(D) = 1$, and so $\dim |D| = 1 - 1 = 0$, so we have equality.

Now assume $g = 0$. By Riemann-Roch, we know $\ell(D) = \ell(W - D) + \deg D - g + 1 = \ell(W - D) + \deg D + 1$ and so $\dim |D| = \ell(W - D) + \deg D$. Since $\deg W = 2g - 2 = -2$, we know that $\deg(W - D) \leq -2$, since D is effective. Thus $\ell(W - D) = 0$ and so we have $\dim |D| = \deg D$.

($\Rightarrow$) Now assume that $\dim |D| = \deg D$. Then $\ell(D) = \deg D + 1$, but Riemann-Roch tells us $\ell(D) = \ell(W - D) + \deg D - g + 1$. Therefore $\ell(W - D) = g$. Suppose $D \neq 0$. But $W - D < W$ since D is effective. We also know $\mathcal{L}(W - D) = \mathcal{L}(W)$. Note that $\deg(W - D) = 2g - 2 - \deg D < 2g - 2 = \deg W$.

We have the containment $H^0(X, \mathcal{L}(W - D)) \subseteq H^0(X, \mathcal{L}(W))$, with equality iff $D = 0$ or $g = 0$. (Given in Hartshorne?)

If $g \neq 0$ but $\ell(W - D) = g = \ell(W)$, and $\mathcal{L}(W - D) = \mathcal{L}(W)$, then

We will show that X is rational if and only if there is a $P \in X$ such that $\ell(P) \geq 2$.

($\Rightarrow$) If X is rational, then $g = 0$, and so for any $P \in X$, $\ell(P) = \ell(W - P) + 2$, but $\deg W = -2$, so $\deg(W - P) = -3$ thus $\ell(W - P) = 0$. Thus $\ell(P) = 2$.

($\Leftarrow$) Suppose there is a $P \in X$ such that $\ell(P) \geq 2$. Then $1 = \ell(0) \neq \ell(P) \geq 2$, so by Fulton 8.29, $\ell(W - 0) = \ell(W - 0 - P)$. Thus $g = \ell(W - P)$. By Riemann-Roch, $\ell(P) = \ell(W - P) + 2 - g$, so $\ell(P) = 2$. Recall $\deg(W) = 2g - 2$, and $\deg(W - P) = 2g - 3$.

Since $\ell(P) = 2$, there is an $f \in \Gamma(X, \mathcal{L}(P)) \subseteq K(X)$ such that $v_P(f) = -1$ and $v_Q(f) \geq 0$ for all $Q \neq P$. This induces a degree 1 map $X \to \mathbb{P}^1$, so X is rational. Specifically, $\widetilde{f} : X \setminus \{P\} \to k \subseteq \mathbb{P}^1$.

Now returning, since $\ell(W - D) = \ell(W) = g$, there is a $P \in X$ such that $\ell(W - P) = g$, so by Fulton 8.29, $\ell(P) \neq 1$ so $\ell(P) = 2$ and so X is rational. Thus $g = 0$. $\square$

Problem 2.3. Let X be a curve and let L be a line in $\mathbb{P}^2$ not tangent to X. Let $\varphi : X \to L$ be a morphism defined by $\varphi(P) = T_P(X) \cap L$. Show that φ is ramified only at inflection points and points on L.

Proof. First some lemmas about nonsingular plane curves of degree d.

Lemma. Note the map $X \to (\mathbb{P}^2)^*$ is given by $p \mapsto [Df(p)]$ where $[Df] = [f_x : f_y : f_z]$. That is, it is given by the graded ring map $T : S_X \leftarrow k[x^*, y^*, z^*]$ where $x^* \mapsto f_x$, $y^* \mapsto f_y$, and $z^* \mapsto f_z$. $T((x^*, y^*, z^*))$ carves out the empty scheme in X as X is nonsingular.

Euler's Lemma (here called "formula") says that if f is a homogenous polynomial of degree d, then $\sum x_i(\partial f/\partial x_i) = d \cdot 5f$.

Lemma. Let's generalize Euler's formula. Let $S = k[x_1, \ldots, x_n]$, $f \in S$ homogeneous of degree d, and $T = T^\bullet(S^n) = S\langle t_1, \ldots, t_n\rangle$ the tensor algebra where t_i's don't commute, x_i's commute, and x_i's commute with the t_j's. Consider the k-linear maps $D : T \to T$ and $\vec{x}^* : T \to T$ where D is of degree 1, and $\vec{x}^*$ is of degree -1, defined as $D := (t_1 \cdot \partial x_1 + \cdots + t_n \cdot \partial x_n) \cdot -$ and $\vec{x}^* := (x_1 \cdot t_1^* + \cdots + x_n \cdot t_n^*) \cdot -$ where t_i^* is the dual operator of t_i in the sense that $t_i^* t_j = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$. Then we have (as long as $\ell < d$)

$$\vec{x}^* \circ D = (x_1 \partial x_1 + \cdots + x_n \partial x_n) \cdot - \text{ and hence } \vec{x}^* D^{\ell+1} f = (d - \ell)[Df].$$

In particular, $\ell = 0$ is Euler's formula and $\ell = 1$ gives $\begin{bmatrix} x & y & z \end{bmatrix} \begin{bmatrix} & & \\ & H & \\ & & \end{bmatrix} = (d-1)[Df]$ (where H is the Hessian matrix of f).

Proof: The subtlety is to realize that $(t_i^*(t_j(-))) = (\partial t_i^* t_j)(-)$; this is why ${}^*t_i$ is defined somewhat weirdly. After that, the proof is pretty much the proof of Euler's formula.

Lemma (Inflection Point). Let $X = \mathfrak{V}(f) \subseteq \mathbb{P}^2_k$ (not necessarily smooth), and let $L = \mathfrak{V}(ax + by + cz)$ be a line (denote $\vec{n} = [a : b : c]$). Let m_P be the intersection multiplicity of X and L at a point $P \in \mathbb{P}^2_k$ (0 if not in intersection). Our goal is to give a criterion for $m_P \geq m$ in terms of $D^m f(P)$ and $\vec{n}^m(P)$.

$m = 1$ is easy: check $f(P) = \vec{n} \cdot P = 0$.

$m = 2$ is still easy: check $Df(P) = \lambda \vec{n}$ for some $\lambda \in k$ (can be zero!)

$m = 3$ is where things get tricky.

WLOG suppose $c \neq 0$ (we then homogenize by c later so this isn't a problem). Let $g(s,t) := f(s, t, -\frac{a}{c} - \frac{b}{c}t) = (p_2 s - p_1 t)'$. Then we see that $m_P \geq m$ iff $\frac{\partial g}{\partial s^i \partial t^j}(p_1, p_2) = 0$ for all $i + j \leq m$.

We immediately recover the $m = 1, 2$ cases. For $m = 3$, (after some long computation), we obtain the following:

Define $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \boxtimes \begin{bmatrix} e & f \\ g & h \end{bmatrix} := de + ah - cf - bg$. Let $I, J \subseteq \{1, 2, 3\}$ of size 2, and given a 3×3 matrix M, denote by $M_{I,J}$ the square submatrix given by I, J. Let $[\vec{n}^2]$ be the outer product of $\vec{n}$ with itself (recall the *outer product* of vectors $\vec{v}$ and $\vec{w}$ is $\begin{bmatrix} v_1 w_1 & v_1 w_2 & \cdots & v_1 w_n \\ v_2 w_1 & v_2 w_2 & \cdots & v_2 w_n \\ \vdots & \vdots & \ddots & \vdots \\ v_m w_1 & v_m w_2 & \cdots & v_m w_n \end{bmatrix}$ and $[D^2 f]$ is the Hessian matrix of f. Then $m_P \geq 3$ if $m \geq 2$ already and $([\vec{n}^2]_{I,J} \boxtimes [D^2 f]_{I,J})(P) = 0$ for all I, J.

Now for the proof. WLOG let $L = \mathfrak{V}(z)$. Identify $L = \operatorname{Proj} k[x, y] = \mathbb{P}^1$. Then the map $\varphi : X \to \mathbb{P}^1$ is given $p \mapsto [Df(p)] \times [0 : 0 : 1] = [f_y(p) : -f_x(p)]$ (the cross product, which is always nonzero for $p \in X$ since L is not tangent to X). In other words, the map is given by $\varphi^\sharp : k[x,y] \to k[x,y,z]/f$ via $x \mapsto f_y$, and $y \mapsto -f_x$ (as $\varphi^\sharp(x,y)$ carves out $\mathfrak{V}(f_x, f_y, f_z)$, and L not being tangent to X implied that this is empty).

Now, let $p \in X$ so that $\varphi(p) = [f_y(p) : -f_x(p)] = \mathfrak{V}(f_x(p)x + f_y(p)y) \subseteq \mathbb{P}^1$. The function pulls back to $\varphi^\sharp(f_x(p)x + f_y(p)y) = f_x(p)f_y - f_y(p)f_x$, so let $h := f_y(p)f_x - f_x(p)f_y$. The map φ is ramified at p if and only if $\mathfrak{V}(h)$ meets $\mathfrak{V}(f)$ at p with multiplicity > 1 (note $p \in \mathfrak{V}(h)$ indeed). This is equivalent to stating that $[Dh(p)] = \lambda[Df(p)]$ for some $\lambda \in k$. Then we have

$$[Dh(p)] = \begin{bmatrix} & & \\ & Hf(p) & \\ & & \end{bmatrix} \begin{bmatrix} f_y(p) \\ -f_x(p) \\ 0 \end{bmatrix}.$$

So if $p \in L$ then $[f_y(p) : -f_x(p) : 0]$ so that the generalized Euler's formula does the job.

Now for $p = [a : b : 1] \notin L$ case. The condition is equivalent to saying that $[Dh(p)] \times [Df(p)] = 0$, which when computed out says

$$f_y^2 f_{xx} - 2f_x f_y f_{xy} + f_x^2 f_{yy} - f_x f_y f_{xz} + f_x^2 f_{yz} - f_y f_z f_{xx} - f_x f_z f_{xy}, f_z f_y f_{xy} - f_x f_z f_{yy} - f_y^2 f_{xz} + f_x f_y f_{yz}$$

(evaluation at P ommitted for convenience). This corresponds to $(I, J) = ([12],[12]), ([12],[13]), ([12],[23])$ in the inflection point lemma above where $\vec{n} = Df(p)$. We could have at the very beginning arranged so that L is $z = 0$ while $p = [0 : 0 : 1]$ (i.e. do the coordinate change $X = x - az$, $Y = y - bz$, $Z = z$) so we can assume that $a = b = 0$. Then $f_z(p) = f_{zz}(p) = 0$ (both repeated Euler's formula), so that the equation for $(I, J) = ([23],[23])$ is also automatically satisfied, and so p is an inflection point. $\square$

Problem 2.4. *Funny Curves.* Let $\operatorname{char} k = 3$ and let $X = \mathfrak{V}(x^3y + y^3z + z^3x)$. Show that X is nonsingular and that every point is an inflection point. Furthermore, show that the dual curve X^* is isomorphic to X, however the natural map $X \to X^*$ is purely inseparable.

Proof. Observe $X_x = 3x^2y + z^3 = z^3$ (since $\operatorname{char} k = 3$), and $X_y = x^3$ and $X_z = y^3$. Then X is singular at the point $P = (a : b : c)$ satisfying $a^3 = b^3 = c^3 = 0$. Since no such P exists in $\mathbb{P}^2_k$, the curve X must be nonsingular.

Now we will show that every point of X is an inflection point. Let $P = (0 : 0 : 1) \in X$. Then consider the affine localization of X, $\mathfrak{D}(z) \cap X = \mathfrak{V}(x^3y + y^3 + x)$. Then $3x^2y\mathsf{d}x + x^3\mathsf{d}y + 3y^2\mathsf{d}y + \mathsf{d}x = x^3\mathsf{d}y + \mathsf{d}x = 0$. So at point $P = (0 : 0 : 1)$, we have $0\mathsf{d}y + \mathsf{d}x = 0$ and so the line tangent to P at X is $T_P(X) = \mathfrak{V}(x)$. Then let us calculate $i(X \cap T_P(X); P)$. It is the length of the $k[x,y,z]_{(x,y)}$-module $(k[x,y,z]/(x^3y + y^3z + z^3x, x))_{(y)} = k[y,z]/(y^3z)_{(y)}$, which is 3 (since z is a unit). This $i(X \cap T_P(X); P) = 3$ and so P is an inflection point.

Now let $Q = (a : b : 1) \in (\mathfrak{D}(z) \cap X) \setminus \{P\}$. Then $T_Q(X) = \mathfrak{V}(a^3y + x)$ (with the calculation from above). Then $i(X \cap T_Q(X); Q)$ is the length of the $k[x,y,z]_{(x-az,y-bz)}$-module $(k[x,y,z]/(x^3y + y^3z + z^3x))_{(x-az,y-bz)} = (k[y,z]/(-a^9y^4 + y^3z - a^3yz^3))_{(y-bz)} \cong (k[y,z]/(-a^9(y+bz)^4 + (y+bz)^3z - a^3(y+bz)z^3))_{(y)}$, which is 4. Thus $i(X \cap T_Q(X); Q) = 4$, so Q is an inflection point of X.

Now let $R = (0 : 1 : 0) \in X$. Then $\mathfrak{D}(y) \cap X = \mathfrak{V}(x^3 + z + z^3x)$ and so $\mathsf{d}z + z^3\mathsf{d}x = 0$. Thus $T_R(X) = \mathfrak{V}(z)$. Then $i(X \cap T_R(X); R)$ is the length of the $k[x,y,z]_{(x,z)}$-module

$(k[x,y,z]/(x^3y+y^3z+z^3x,z))_{(x)} = (k[x,y]/(x^3y))_{(x)}$, which is 3. Thus $i(X \cap T_R(X); R) = 3$, so R is an inflection point of X.

A very similar argument shows that $i(X \cap T_{(1:0:0)}(X); (1:0:0)) = 3$. Thus every point of X is an inflection point.

The dualizing map $\delta : X \to X^*$ is given by the map of rings $\delta^\sharp : k[x^*, y^*, z^*] \to S_X$ given by $\delta^\sharp(x^*) = X_x = z^3$, $\delta^\sharp(y^*) = X_y = x^3$ and $\delta^\sharp(z^*) = X_z = y^3$. We wish to show that $\ker \delta^\sharp = ((x^*)^3(y^*) + (y^*)^3(z^*) + (z^*)^3(x^*))$.

First note that $\delta^\sharp((x^*)^3(y^*) + (y^*)^3(z^*) + (z^*)^3(x^*)) = (z^3)^3(x^3) + (x^3)^3(y^3) + (y^3)^3(z^3) = (z^3x + x^3y + y^3z)^3 = 0^3 = 0$. Therefore $((x^*)^3(y^*) + (y^*)^3(z^*) + (z^*)^3(x^*)) \subseteq \ker \delta^\sharp$.

This map is purely inseparable because for every $f \in S_X^*$, the polynomial $\alpha^3 - \delta^\sharp(f) \in S_X[\alpha]$ has a root. □

Problem 2.5. Let $f : X \to Y$ be a degree n map and let $g(X) \geq 2$.

(a) If $P \in X$ is a ramification point, and $e_P = r$, show that $f^{-1}f(P)$ consists of exactly n/r points, each having index r. Let $P_1, \ldots, P_s$ be a maximal set of ramification points of X lying over distinct points of Y, and let $e_{P_i} = r_i$. Then show that Hurwitz's Theorem implies that

$$(2g-2)/n = 2g(Y) - 2 + \sum_{i=1}^{s} (1 - 1/r_i).$$

(b) Since $g \geq 2$, let left hand side of the equation is > 0. Show that if $g(Y) \geq 0$, $s \geq 0$, and $r_i \geq 2$ for $1 \leq i \leq s$ are integers such that

$$2g(Y) - 2 + \sum_{i=1}^{s} (1 - 1/r_i) > 0,$$

then the minimum value of this expression is $1/42$. Conclude that $n \leq 84(g-1)$.

Proof.

(a) Let $P, Q \in f^{-1}f(P)$. Then we will show that $e_P = e_Q$. Let t be a uniformizing parameter of $\mathcal{O}_{Y,f(P)}$, let u be a uniformizing parameter of $\mathcal{O}_{X,P}$ and let w be a uniformizing parameter of $\mathcal{O}_{X,Q}$. Then there is an $a \in \mathcal{O}_{X,P}^\times$ and a $b \in \mathcal{O}_{X,Q}^\times$ such that $f^\sharp(t) = au^{e_P}$ and $f^\sharp(t) = bw^{e_Q}$. Then $au^{e_P} = bw^{e_Q}$ in $K(X)$. Then $e_P = v_P(au^{e_P}) = v_P(bw^{e_Q})$ and $e_Q = v_Q(bw^{e_Q}) = v_Q(au^{e_P})$. Thus $(au^{e_P})/(bw^{e_Q})$ is a unit in both $\mathcal{O}_{X,P}$ and $\mathcal{O}_{X,Q}$. Thus $v_P(au^{e_P}) = v_Q(bw^{e_Q})$ and so $e_P = e_Q$.

Now we know that for all $Q, P \in f^{-1}f(P)$, that $e_P = e_Q$. Now consider the divisor $f(P)$ and its image $f^*f(P) = \sum_{R \to f(P)} e_R \cdot R$. Since $\deg f(P) = 1$, we know $\deg f^*f(P) = n$. Furthermore, we know that e_R is constant by the above proof, so $f^*f(P) = e_R \sum_{R \to f(P)} R$ and so $e_R \deg \left(\sum_{R \to f(P)} R \right) = n$, so there are n/e_R many points in $f^{-1}f(P)$, each having ramification index e_R.

Now let f have s many branch points and let $P_1, \ldots, P_s$ be a maximal set of ramification points over distinct branch points in Y. Hurwitz's Theorem guarantees $2g - 2 = n(2g(Y) - 2) + \deg R$, where R is the ramification divisor of f.

We wish to show that $n\sum_{i=1}^s(1-1/r_i) = \deg R$. Since char$k = 0$, f has only tame ramification points and so $\deg R = \sum_{P\in X}(e_P - 1) = \sum_{P \text{ a ramification point}}(e_P - 1) = sn - n/r_1 - \cdots - n/r_s = n(s - 1/r_1 - \cdots - 1/r_s) = n\sum_{i=1}^s(1-1/r_i)$. This is because there are n/r_i many ramification points for the i^{th} branch point, each having ramification index r_i, and there are s many branch points.

Therefore $\deg R = n\sum_{i=1}^s(1-1/r_i)$ and so Hurwitz's Theorem implies that $2g-2 = n(2g(Y)-2) + n\sum_{i=1}^s(1-1/r_i)$ and so $(2g-2)/n = 2g(Y) - 2 + \sum_{i=1}^s(1-1/r_i)$.

(b) Now we have the equality $(2g-2)/n = 2g(Y) - 2 + \sum_{i=1}^s(1-1/r_i)$, and since the left side of this equality is > 0, so is the right side. Let $g(Y) \geq 0$, $s \geq 0$ and $r_i \geq 2$ for all $1 \leq i \leq s$.

Call the right side of the equation T.

- If $g(Y) \geq 2$, then $T \geq 2$ and $n \leq g - 1$.
- If $g(Y) = 1$, then $s \geq 1$ and $T \geq 0 + 1 - 1/2 = 1/2$ so $n \leq 4(g-1)$.
- If $g(Y) = 0$, then $s \geq 3$ and
  - if $s \geq 5$ then $T \geq -2 + s(1 - 1/2) \geq 1/2$, so that $n \leq 4(g-1)$.
  - if $s = 4$ then $T \geq -2 + 4 - 1/2 - 1/2 - 1/2 - 1/3 = 1/6$, so $n \leq 12(g-1)$
  - if $s = 3$, then we may assume $2 \leq r_1 \leq r_2 \leq r_3$.
    - If $r_1 \geq 3$ then $T \geq -2 + 3 - 1/3 - 1/3 - 1/4 = 1/12$ so $n \leq 24(g-1)$.
    - If $r_1 = 2$ then
      - if $r_2 \geq 4$ then $T \geq -2 + 3 - 1/2 - 1/4 - 1/5 = 1/20$ so $n \leq 40(g-1)$
      - if $r_2 = 3$ then $T \geq -2 + 3 - 1/2 - 1/3 - 1/7 = 1/42$ so $n \leq 84(g-1)$.

In conclusion, $n \leq 84(g-1)$. Note these numbers were obtained from the fact that the resulting number must be positive, and a smaller integer would result in a nonpositive sum.

□

Recall that an invertible sheaf $\mathcal{L}$ on a curve X is *very ample* if it is isomorphic to $\mathcal{O}_X(1)$ for some immersion of X in a projective space. It is *ample* if for any coherent sheaf $\mathcal{F}$ on X, the sheaf $\mathcal{F} \otimes \mathcal{L}^n$ is generated by global sections for $n \gg 0$. We have seen that $\mathcal{L}$ is ample if and only if $\mathcal{L}^n$ is very ample for some $n \gg 0$. We have seen that $\mathcal{L}$ is ample if and only if $\mathcal{L}^n$ is very ample for some $n > 0$. If D is a divisor on X, we will say that D is *ample* or *very ample* if $\mathcal{L}(D)$ is.

Recall that a *linear system* is a set $\mathfrak{d}$ of effective divisors, which forms a linear subspace of a complete linear system $|D|$. A point P is a *base point* of the linear system $\mathfrak{d}$ if $P \in \mathrm{Supp}D$ for all $D \in \mathfrak{d}$. We have seen that a complete linear system $|D|$ is base-point free if and only if $\mathcal{L}(D)$ is generated by global sections.

Proposition 3.1. Let D be a divisor on a curve X. Then:

(a) the complete linear system $|D|$ has no base points if and only if for every point $P \in X$,

$$\dim |D-P| = \dim |D| - 1$$

or $\ell(D-P) = \ell(D) - 1$ (so $\ell(W-D-P) = \ell(W-D)$);

(b) D is very ample if and only if for every two points $P, Q \in X$ (including the case $P = Q$),

$$\dim |D-P-Q| = \dim |D| - 2.$$

Proof. First we consider the exact sequence of sheaves

$$0 \to \mathcal{L}(D-P) \to \mathcal{L}(D) \to k(P) \to 0.$$

Taking global sections, we have

$$0 \to \Gamma(X, \mathcal{L}(D-P)) \to \Gamma(X, \mathcal{L}(D)) \to k,$$

so in any case we see that $\dim |D-P|$ is equal to either $\dim |D|$ or $\dim |D| - 1$. Furthermore, sending a divisor E to $E+P$ defines the linear map

$$\varphi : |D-P| \to |D|$$

which is clearly injective. Therefore, the dimensions of these two linear systems are equal if and only if φ is surjective. On the other hand, φ is surjective if and only if P is a base point of $|D|$, so this proves (a).

To prove (b), we may assume that $|D|$ has no base points. Indeed, this is true if D is very ample. On the other hand, if D satisfies the condition of (b), then we must a fortiori have

$$\dim |D-P| = \dim |D| - 1$$

for every $P \in X$, so $|D|$ has no base points.

This being the case, $|D|$ determines a morphism of X to $\mathbb{P}^n$ (II, 7.1) and (II, 7.8.1), so the question is whether that morphism is a closed immersion. We use the criterion of (II, 7.3) and (II, 7.8.2), so we have to see whether $|D|$ separates points and separates tangent vectors. The first condition says that for any two distinct points $P, Q \in X$, Q is not a base point of $|D-P|$. By (a), this is equivalent to saying

$$\dim |D-P-Q| = \dim |D| - 2.$$

The second condition says that for any point $P \in X$, there is a divisor $D' \in |D|$ such that P occurs with multiplicity 1 in D', because $\dim T_P(X) = 1$, and $\dim T_P(D') = 0$ if P has multiplicity 1 in D', 1 if P has higher multiplicity. But this just says that P is not a base point of $|D-P|$, or, using (a) again,

$$\dim |D-2P| = \dim |D| - 2.$$

Thus our result follows from (II, 7.3). $\square$

Corollary 3.2. Let D be a divisor on a curve X of genus g.

(a) If $\deg D \geq 2g$, then $|D|$ has no base points.

(b) If $\deg D \geq 2g+1$, then D is very ample.

Proof. If case (a), both D and $D-P$ are nonspecial (1.3.4), so by Riemann-Roch, $\dim |D-P| = \dim |D| - 1$. In case (b), D and $D-P-Q$ are both nonspecial, so $\dim |D-P-Q| = \dim |D| - 2$ again by Riemann-Roch. $\square$

Corollary 3.3. A divisor D on a curve X is ample if and only if $\deg D > 0$.

Proof. If D is ample, some multiple is very ample (II, 7.6) so $nD \sim H$ where H is a hyperplane section for a projective embedding, so $\deg H > 0$, hence $\deg D > 0$. Conversely, if $\deg D > 0$, then for $n \gg 0$, $\deg nD \geq 2g(X)+1$ so by (3.2), nD is very ample, and so D is ample (II, 7.6). $\square$

Example 3.3.1. If $g = 0$, then D is ample $\Leftrightarrow$ very ample $\Leftrightarrow$ $\deg D > 0$. Since $X \cong \mathbb{P}^1$ (1.3.5)(the "assumption of the chapter" is that all curves are complete and nonsingular), this is just (II, 7.6.1).

Example 3.3.2. Let X be a curve, and let D be a very ample divisor on X, corresponding to a closed immersion $\varphi : X \to \mathbb{P}^n$. then the degree of $\varphi(X)$, as defined in (I, 7) for a projective variety, is just equal to $\deg D$ (II, Ex. 6.2).

Example 3.3.3. Let X be an elliptic curve, i.e., $g = 1$ (1.3.6). Then any divisor D of degree 3 is very ample. Such a divisor is nonspecial, so by Riemann-Roch, $\dim |D| = 2$. Thus we see that any elliptic curve can be embedded in $\mathbb{P}^2$ as a cubic curve. (Conversely, of course, and nonsingular plane cubic is elliptic, by the genus formula (I, Ex. 7.2).)

In the case $g = 1$ we can actually say D is very ample $\Leftrightarrow$ $\deg D \geq 3$. Because if $\deg D = 2$, then by Riemann-Roch, $\dim |D| = 1$, so $|D|$ defines a morphism of X to $\mathbb{P}^1$, which cannot be a closed immersion.

Example 3.3.4. If $g = 2$, then any divisor D of degree 5 is very ample. By Riemann-Roch, $\dim |D| = 3$, so any curve of genus 2 can be embedded in $\mathbb{P}^3$ as a curve of degree 5.

Example 3.3.5. The result of (3.2) is not the best possible in general. For example, if X is a plane curve of degree 4, then $D = X.H$ is a very ample divisor of degree 4, but $g = 3$ so $2g+1 = 7$.

Next objective: show that any curve can be embedded into $\mathbb{P}^3$. Consider a curve $X \subseteq \mathbb{P}^n$, take a point $O \notin X$, and project X from O into $\mathbb{P}^{n-1}$ (I, Ex. 3.14). This gives a morphism of X into $\mathbb{P}^{n-1}$, and we investigate when it is a closed immersion.

If P, Q are two distinct points of X, we define the *secant line* determined by P and Q to be the line $\mathbb{P}^n$ determined by P and Q to be the line $\mathbb{P}^n$ joining P and Q. If P is a point of X, we define the *tangent line* to X at P to be the unique line $L \subseteq \mathbb{P}^n$ passing through P, whose tangent space $T_P(L)$ is equal to $T_P(X)$ as a subspace of $T_P(\mathbb{P}^n)$.

Proposition 3.4. Let X be a curve in $\mathbb{P}^n$, let O be a point not on X, and let $\varphi : X \to \mathbb{P}^{n-1}$ be the morphism determined by projection from O. Then φ is a closed immersion if and only if

1. O is not on any secant line of X, and
2. O is not on any tangent line of X.

Proof. The morphsim φ corresponds (II, 7.8.1) to the linear system cut out on X be the hyperplanes H of $\mathbb{P}^n$ passing through O. So φ is a closed immersion if and only if this linear system separates points and separates tangent vectors on X (II, 7.8.2). If P, Q are two distinct points on X, then φ separates them if and only if there is an H containing point O and P, but not Q. This is possible if and only if O is not on the line PQ. If $P \in X$, then φ separates tangent vectors at P if and only if there is an H containing O and P, and meeting X at P with multiplicity 1. This is possible if and only if O is not on the tangent line at P. □

Proposition 3.5. If X is a curve in $\mathbb{P}^n$, with $n \geq 4$, then there is a point $O \notin X$ such that the projection from O gives a closed immersion of X into $\mathbb{P}^{n-1}$.

Proof. Let Sec$X$ be the union of all secant lines of X. We call this the *secant variety* of X. It is a locally closed subset of $\mathbb{P}^n$, of dimension ≤ 3, since (at least locally) it is the image of a morphism from $(X \times X \setminus \Delta) \times \mathbb{P}^1$ to $\mathbb{P}^n$ which sends $\langle P, Q, t\rangle$ to the point t on the secant line through P and Q, suitably parametrized.

Let Tan$X$, the *tangent variety* of X, be the union of all tangent lines of X. It is a closed subset of $\mathbb{P}^n$, of dimension ≤ 2, because it is locally an image of $X \times \mathbb{P}^1$.

Since $n \geq 4$, $\mathrm{Sec}X \cup \mathrm{Tan}X \neq \mathbb{P}^n$, so we can find plenty of points O which do not lie on any secant or tangent of X. Then the projection from O gives the required closed immersion, by (3.4). □

Corollary 3.6. Any curve can be embedded in $\mathbb{P}^3$.

Proof. First embed X in any projective space $\mathbb{P}^n$. For example, take a divisor D of degree $d \geq 2g+1$ and use (3.2). Since D is very ample the complete linear system $|D|$ determines an embedding of X in $\mathbb{P}^n$ with $n = \dim |D|$. If $n \leq 3$, we can consider $\mathbb{P}^n$ as a subspace of $\mathbb{P}^3$, so there is nothing to prove. If $n \geq 4$, we use (3.5) repeatedly to project from points until we have X embedded in $\mathbb{P}^3$. □

Next we study the projection of a curve X in $\mathbb{P}^3$ to $\mathbb{P}^2$. In general the secant variety will fill up all of $\mathbb{P}^3$, so we cannot avoid all the secants, and the projected curve will be singular. However, we will see that it is possible to choose the center of projection O so that the resulting morphsim φ from X to $\mathbb{P}^2$ is birational onto its image, and the image $\varphi(X)$ has at most nodes as singularities.

Recall (I, Ex. 5.6) that a *node* is a singular point of a plane curve of multiplicity 2, with distinct tangent directions. We define a *multisecant* of X to be a line in $\mathbb{P}^3$ which meets X in three or more distinct points. A *secant with coplanar tangent lines* is a secant joining two points P, Q of X whose tangent lines L_P, L_Q lie in the same plane, or equivalently, such that L_P meets L_Q.

Proposition 3.7. Let X be a curve in $\mathbb{P}^3$, let O be a point not on X, and let $\varphi : X \to \mathbb{P}^2$ be the morphism determined by projection from O. Then φ is birational onto its image and $\varphi(X)$ has at most nodes as singularities, if and only if

1. O lies on only finitely many secants of X,
2. O is not on any tangent line of X,
3. O is not on any multisecant of X, and
4. O is not on any secant with coplanar tangent lines.

Proof. Going back to the proof of (II, 7.3), condition (1) says that φ is one-to-one almost everywhere, hence birational. When O does lie on a secant line, conditions (2), (3), (4) tell us that line meets X in exactly two points, P, Q, it is not tangent to X at either one, and the tangent lines at P, Q are mapped to distinct lines in $\mathbb{P}^2$ (the tangent lines do not meet in $\mathbb{P}^3$). Hence the image $\varphi(X)$ has a node at that point. □

To show that a point O exists satisfying (1)-(4) of (3.7), we will count the dimensions of the "bad points," as in the proof of (3.5). The hard part is to show that not every secant has coplanar tangent lines. Over $\mathbb{C}$, one could see this from differential geometry. However, we give a different proof, valid in all characteristics, which is achieved by an interesting application of Hurwitz's Theorem.

Proposition 3.8. Let X be a curve in $\mathbb{P}^3$, which is not contained in any plane. Suppose either

(a) every secant line of X is a multisecant, or

(b) for any two points $P, Q \in X$, the tangent lines L_P, L_Q are coplanar.

Then there is a point $A \in \mathbb{P}^3$ which lies on every tangent line of X.

Proof. First we show that (a) implies (b). Fix a point R in X, and consider the morphsim $\psi : X \setminus R \to \mathbb{P}^2$ induced by projection from R. Since every secant is a multisecant, ψ is a many-to-one map. If ψ is inseparable, then for any $P \in X$, the tangent line L_P at X passes through R. This gives (b) and our conclusion immediately, so we may assume that each such ψ is separable. In that case, let T be a nonsingular point of $\psi(X)$ over which ψ is not ramified. If $P, Q \in \psi^{-1}(T)$, then the tangent lines L_P, L_Q to X are projected into the tangent line L_T to $\psi(X)$ at T. So L_P and L_Q are both in the plane spanned by R and L_T, hence coplanar.

Thus we have shown that for any R, and for almost all P, Q such that P, Q, R are collinear, L_P and L_Q are coplanar. Therefore, there is an open set of $\langle P, Q\rangle$ in $X \times X$ for which L_P and L_Q are coplanar. But the property of L_P and L_Q being coplanar is a closed condition, so we conclude that for all $P, Q, \in X$, L_P and L_Q are coplanar. This is (b).

Now assume (b). Take any two points $P, Q \in X$ with distinct tangents, and let $A = L_P \cap L_Q$. By hypothesis, X is not contained in any plane, so in particular, if π is the plane spanned by L_P and L_Q, then $X \cap \pi$ is a finite set of points. For any point $R \in X \setminus X \cap \pi$, the tangent line L_R must meet both L_P and L_Q. But since $L_R \not\subseteq \pi$, it must pass through A. So there is an open set of X consisting of points R such that $A \in L_R$. Since this is a closed condition, we conclude that $A \in L_R$ for all $R \in X$. □

Definition. A curve X in $\mathbb{P}^n$ is *strange* if there is a point A which lies on all the tangent lines of X.

Example 3.8.1.. $\mathbb{P}^1$ is strange.

Example 3.8.2.. A conic in $\mathbb{P}^2$ over a field of characteristic 2 is strange. For example, consider the conic $y = x^2$. Then $\mathsf{d}y/\mathsf{d}x \equiv 0$, so all the tangent lines are horizontal, so they all pass through the point at infinity on the x-axis.

Theorem 3.9. (Samuel [2]). The only strange curves in any $\mathbb{P}^n$ are the line (3.8.1) and the conic in characteristic 2 (3.8.2).

Proof. By projecting down if necessary (3.5) we may assume that X lies in $\mathbb{P}^3$. Choose an $\mathbb{A}^3$ in $\mathbb{P}^3$ with affine coordinates x, y, z in such a way that

1. A is the point at infinity on the x-axis $[1 : 0 : 0 : 0]$
2. if $A \in X$, then its tangent line L_A is not in the xz-plane,
3. the z-axis does not meet X,
4. X does not meet the line at infinity of the xz-plane, except possibly at A.

First we project from A to the yz-plane. Since A lies on every tangent line to X, the corresponding morphism from X to $\mathbb{P}^2$ is ramified everywhere. So either the image is a point (in which case X is a line), or it is inseparable (2.2). We conclude that the functions y and z restricted to X lie in $K(X)^p$, where $\operatorname{char} k = 0 > 0$.

Next, we project from the z-axis to the line M at infinity in the xy-plane. In other words, for each point $P \in X$, we define $\varphi(P)$ to be the intersection of the plane spanned by P and the z-axis with the line M. This gives a morphism $\varphi : X \to M$ of degree $d = \deg X$. Note that φ is ramified exactly at the points of X which lie in the finite part of the xz-plane, but not at A.

We will apply Hurwitz's Theorem (2.4) to the morphism φ. For any point $P \in X \cap xz$-plane, we take $u = x - a$ as a local coordinate, where $a \in k$ and $a \neq 0$. We take $t = y/x$ as a local coordinate at A on M. Then by (2.2) we have to calculate $v_P(\mathsf{d}t/\mathsf{d}u)$. Write $x = u + a$ so $t = y(u + a)^{-1}$. Since $y \in K(X)^p$, we have $\mathsf{d}y/\mathsf{d}u = 0$, so

$$\mathsf{d}t/\mathsf{d}u = -y(u + a)^{-2}.$$

But $u + a$ is a unit in the local ring $\mathcal{O}_P$ (the plane $u + a = x = 0$ does not go through the point P, as $P \in X \cap \mathfrak{V}(y)$ and (3) ($\mathfrak{V}(x, y)$ is the z-axis, which does not meet X)), so

$$v_P(\mathsf{d}t/\mathsf{d}y) = v_P(y).$$

If we let $P_1, \dots, P_r$ be all the finite points of $X \cap xz$-plane, then Hurwitz's Theorem tells us that

$$2g - 2 = -2d + \sum_{i=1}^{r} v_{P_i}(y).$$

Now we consider two cases.

Case 1. If $A \notin X$, the xz-plane meets X only at the points P_i. Since this plane is defined by the equation $y = 0$, we can compute the degree of X as the number of intersections of X with this plane, namely

$$d = \sum_{i=1}^{r} v_{P_i}(y).$$

Substituting in the above, we have

$$2g - 2 = -d$$

which is possible only if $g = 0$ and $d = 2$. Thus $X \cong \mathbb{P}^1$ as an abstract curve (1.3.5), and its embedding is by a divisor D of degree 2. We have $\dim |D| = 2$ by Riemann-Roch, so X is a conic on a plane $\mathbb{P}^2$. For the conic to be strange, we must have $\operatorname{char} k = 2$.

Case 2. If $A \in X$, then by condition (2) the xz-plane meets X transversally at A, so we see similarly

$$d = \sum_{i=1}^{r} v_{P_i}(y) + 1.$$

So

$$2g - 2 = -d - 1$$

which implies $g = 0$, $d = 1$. This is the line. □

Theorem 3.10. Let X be a curve in $\mathbb{P}^3$. Then there is a point $O \notin X$ such that the projection from O determines a birational morphism φ from X to its image in $\mathbb{P}^2$, and that image has at most nodes for singularities.

Proof. If X is contained in a plane already, any O not in that plane will do. So we assume X is not contained in any plane. Then in particular, X is neither a line nor a conic, so by (3.9), X is not strange. Therefore, by (3.8), X has a secant which is not a multisecant, and it has a secant without coplanar tangents. Since the same must be true for nearby secants, we see that there is an open subset of $X \times X$ consisting of pairs $\langle P, Q\rangle$ such that the secant line through P, Q is not a multisecant and does not have coplanar tangents. Hence the subset of $X \times X$ consisting of pairs $\langle P, Q\rangle$ where the secant is a multisecant or has coplanar tangents is a proper subset, has dimension ≤ 1, and so the union in $\mathbb{P}^3$ of the corresponding secant lines has dimension ≤ 2. Combining with the fact that the tangent variety to X has dimension ≤ 2 (see (3.5)), we see that there is an open subset of $\mathbb{P}^3$ consisting of points O which satisfy (2), (3), and (4) of (3.7).

To complete the proof, by (3.7), we must show (1): that O can be chosen to lie on only finitely many secants of X. For this we consider the morphism $(X \times X \setminus \Delta) \times \mathbb{P}^1 \to \mathbb{P}^3$ (defined at least locally) which sends $\langle P, Q, t\rangle$ to the point t on the secant line through P and Q. If the image has dimension < 3, then we can choose O lying on no secant. If the image has dimension = 3, then since it is a morphism between two varieties of the same dimension, we can apply (II, Ex. 3.7) and find there is an open set of points in $\mathbb{P}^3$ over which the fibre is finite. These points lie on only finitely many secants, so we are done. □

Corollary 3.11. Any curve is birationally equivalent to a plane curve with at most nodes as singularities.

Proof. Combine (3.6) with (3.10). □

Remark 3.11.1. In view of (3.11), one way to approach the classification problem for all curves is to study the family of plane curves of degree d with r nodes, for any given d and r. The family of all plane curves of degree d is a linear system of dimension $d(d+3)/2 = \binom{d+2}{d} - 1$, so it is parametrized by a projective space of that dimension. Inside that projective space, the (irreducible) curves with r nodes form a locally closed subset $V_{d,r}$. If X is such a curve, then the genus g of its normalizaiton $\widetilde{X}$ is given by

$$g = \frac{1}{2}(d-1)(d-2) - r$$

because of (Ex. 1.8). So in order for $V_{d,r}$ to be nonempty, we must have

$$0 \leq r \leq \frac{1}{2}(d-1)(d-2).$$

Furthermore, both extremes are possible. We have seen by Bertini's Theorem (II, 8.20.2) that for any d, there are irreducible nonsingular curves of degree d in $\mathbb{P}^2$, so this gives the case $r = 0$. On the other hand, for any d, we can embed $\mathbb{P}^1$ in $\mathbb{P}^d$ as a curve of degree d (Ex. 3.4), and then project it into $\mathbb{P}^2$ by (3.5) and (3.10), to get a curve X of degree d in $\mathbb{P}^2$ having only nodes, and with $g(\widetilde{X}) = 0$. Thus gives $r = \frac{1}{2}(d-1)(d-2)$.

But the general problem of the structure of the $V_{d,r}$ is very difficult. Severi [2, Anhang F] states that for every d, r satisfying $0 \leq r \leq \frac{1}{2}(d-1)(d-2)$, the algebraic set $V_{d,r}$ is irreducible and nonempty of dimension $\frac{1}{2}d(d+3) - r$, but a complete proof was given only recently by Joe Harris.

Section 4: Elliptic Curves.

Our first topic is to define the j-invariant of an elliptic curve, and to show that it classifies elliptic curves up to isomorphism. Since j can be any element of the ground field k, this will show that the affine line $\mathbb{A}^1_k$ is a variety of moduli for elliptic curves over k.

Let X be an elliptic curve over the algebraically closed field k. Let $P_0 \in X$ be a point, and consider the linear system $|2P_0|$ on X. The divisor $2P_0$ is nonspecial, so by Riemann-Roch, this linear system has dimension 1. It has no base points, because otherwise the curve would be rational. Therefore, it defines a morphism $f : X \to \mathbb{P}^1$ of degree 2, and we can specify $f(P_0) = \infty$ by change of coordinates in $\mathbb{P}^1$.

Now if we assume $\operatorname{char} k \neq 2$, it follows from Hurwitz's Theorem that f is ramified at exactly four points, with P_0 being one of them. If $x = a, b, c$ are the three branch points in $\mathbb{P}^1$ besides ∞, then there is a unique automorphism of $\mathbb{P}^1$ leaving ∞ fixed and sending a to

0 and b to 1, namely $x' = (x-a)/(b-a)$. So after this automorphism, we may assume that f is branched over the points $0, 1, \lambda, \infty$ of $\mathbb{P}^1$, where $\lambda \in k$, $\lambda \neq 0, 1$. This defines a quantity λ. We define $j = j(\lambda)$ by the formula

$$j = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}.$$

This is the j-invariant of the curve X. (The coefficient 2^8 is thrown in to make things work in characteristic 2, despite appearances to the contrary!) Our main result then is the following.

Theorem 4.1. Let k be an algebraically closed field of characteristic $\neq 2$. Then:

(a) for any elliptic curve X over k, the quantity j defined above depends only on X;

(b) two elliptic curves X and X' over k are isomorphic if and only if $j(X) = j(X')$;

(c) every element of k occurs as the j-invariant of some elliptic curve over k.

Thus we have a one-to-one correspondence between the set of elliptic curves over k, up to isomorphism, and the elements of k, given by $X \mapsto j(X)$.

We will prove this theorem after some preliminary results.

Lemma 4.2. Given any two points $P, Q \in X$ (including the case $P = Q$), there is an automorphism σ of X such that $\sigma^2 = \mathrm{id}$, $\sigma(P) = Q$, and for any $R \in X$, $R + \sigma(R) \sim P + Q$.

Proof. This linear system $|P + Q|$ has dimension 1 and is base-point free, hence defines a morphism $f : X \to \mathbb{P}^1$ of degree 2. It is separable, since $X \not\cong \mathbb{P}^1$ (2.5), so $K(X)$ is a Galois extension of $K(\mathbb{P}^1)$. Let σ be the nontrivial automorphism of order 2 of $K(X)$ over $K(\mathbb{P}^1)$. Then σ interchanges the two points of each fibre of f. Hence $\sigma(P) = Q$, and for any $R \in X$, $R + \sigma(R)$ is a fibre of f, hence $R + \sigma(R) \in |P + Q|$, i.e., $R + \sigma(R) \sim P + Q$. □

Corollary 4.3. The group $\mathrm{Aut}X$ of automorphisms of X is transitive.

Lemma 4.4. If $f_1 : X \to \mathbb{P}^1$ and $f_2 : X \to \mathbb{P}^1$ are any two morphisms of degree 2 from X to $\mathbb{P}^1$ then there are automorphisms $\sigma \in \mathrm{Aut}X$ and $\tau \in \mathrm{Aut}\mathbb{P}^1$ such that $f_2 \circ \sigma = \tau \circ f_1$.

$$\begin{tikzcd}
X \arrow[r, dashed, "\sigma"] \arrow[d, "f_1"] & X \arrow[d, "f_2"] \\
\mathbb{P}^1 \arrow[r, dashed, "\tau"] & \mathbb{P}^1
\end{tikzcd}$$

Proof. Let $P_1 \in X$ be a ramification point of f_1 and let $P_2 \in X$ be a ramification points of f_2. Then by (4.3) there is a $\sigma \in \mathrm{Aut}X$ such that $\sigma(P_1) = P_2$. On the other hand, f_1 is determined by the linear system $|2P_1|$ and f_2 is determined by the linear system $|2P_2|$. Since σ takes one to the other, f_1 and $f_2 \circ \sigma$ correspond to the same linear system, so they differ only by an automorphism τ of $\mathbb{P}^1$ (II, 7.8.1). □

Lemma 4.5. Let the symmetric group Σ_3 act on $k \setminus \{0,1\}$ as follows: given $\lambda \in k$, $\lambda \neq 0,1$, permute the numbers $0,1,\lambda$ according to $\alpha \in \Sigma_3$, then apply a linear transformation of x to send the first two back to $0,1$ and let $\alpha(\lambda)$ be the image of the third. Then the orbit of λ consists of

$$\lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda}.$$

Proof. Since the linear transformation sending a,b to $0,1$ is $x' = (x-a)/(b-a)$, we have only to evaluate $(c-a)/(b-a)$ where $\{a,b,c\} = \{0,1,\lambda\}$ in any order. □

Proposition 4.6. Let X be an elliptic curve over k, with $\operatorname{char} k \neq 2$, and let $P_0 \in X$ be a given point. Then there is a closed immersion $X \to \mathbb{P}^2$ such that the image is the curve

$$y^2 = x(x-1)(x-\lambda)$$

for some $\lambda \in k$, and the point P_0 goes to the point at infinity $(0:1:0)$ on the y-axis. Furthermore, this λ is the same as the λ defined earlier, up to an element of Σ_3 as in (4.5).

Proof. We embed X in $\mathbb{P}^2$ by the linear system $|3P_0|$, which gives a closed immersion (3.3.3). We choose our coordinates as follows. Think of the vector spaces $H^0(\mathcal{O}(nP_0))$ as contained in each other,

$$k = H^0(\mathcal{O}) \subseteq H^0(\mathcal{O}(P_0)) \subseteq H^0(\mathcal{O}(2P_0)) \subseteq \cdots.$$

By Riemann-Roch, we have

$$\dim H^0(\mathcal{O}(nP_0)) = n$$

for $n > 0$. Choose $x \in H^0(\mathcal{O}(2P_0))$ so that $1, x$ form a basis of that space, and choose $y \in H^0(\mathcal{O}(3P_0))$ so that $1, x, y$ form a basis for that space. Then the seven quantities

$$1, x, y, x^2, xy, x^3, y^2$$

are in $H^0(\mathcal{O}(6P_0))$, which has dimension 6, so there is a linear relation among them. Furthermore, both x^3 and y^2 occur with coefficient not equal to zero, because they are the only functions with a 6-fold pole at P_0. So replacing x and y by suitable scalar multiples, we may assume they have coefficient 1. Then we have the relation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

for suitable $a_i \in k$.

Now we will make linear changes of coordinates to get the equation in the required form. First we complete the square on the left (here we use $\operatorname{char} k \neq 2$), replacing y by

$$y' = y + \frac{1}{2}(a_1x + a_3).$$

The new equation has y^2 equal to a cubic equation in x, so it can be written

$$y^2 = (x-a)(x-b)(x-c)$$

for suitable $a, b, c \in k$. Now we make a linear change of x to send a, b to $0, 1$, so the equation becomes

$$y^2 = x(x-1)(x-\lambda)$$

as required.

Since both x and y have a pole at P_0, that point goes to the unique point at infinity on this curve, which is $(0, 1, 0)$.

If we project from P_0 to the x-axis, we get a finite morphism of degree 2, sending P_0 to ∞, and ramified at $0, 1, \lambda, \infty$. So the λ is the same as the one defined earlier. □

Proof. Proof of (4.1)

(a) To show that j depends only on X, suppose we made two choices of base point $P_1, P_2 \in X$. Let $f_1 : X \to \mathbb{P}^1$ and $f_2 : X \to \mathbb{P}^1$ be the corresponding morphisms. Then by (4.4) we can find automorphisms $\sigma \in \mathrm{Aut} X$ and $\tau \in \mathrm{Aut}\mathbb{P}^1$ such that $f_2 \circ \sigma = \tau \circ f_1$. Furthermore, we could choose σ such that $\sigma(P_1) = P_2$, hence $\tau(\infty) = \infty$. So τ sends the branch points $0, 1, \lambda_1$ of f_1 to the branch points $0, 1, \lambda_2$ of f_2 in some order. Hence by (4.5), λ_1 and λ_2 differ only by an element of Σ_3, via the action of (4.5). So we have only to observe that for any $\alpha \in \Sigma_3$, $j(\lambda) = j(\alpha(\lambda))$. Indeed, since Σ_3 is generated by any two elements of order 2, it is enough to show that

$$j(\lambda) = j\left(\frac{1}{\lambda}\right) \text{ and } j(\lambda) = j(1-\lambda),$$

which is clear by direct computation. Thus j depends only on X.

(b) Now suppose X and X' are two elliptic curves giving rise to λ and λ', such that $j(\lambda) = j(\lambda')$. First we note that j is a rational function of λ of degree 6, i.e., $\lambda \mapsto j$ defines a finite morphism $\mathbb{P}^1 \to \mathbb{P}^1$ of degree 6. Furthermore, this is a Galois covering, with Galois group Σ_3 under the action described above. Therefore, $j(\lambda) = j(\lambda')$ if and only if λ and λ' differ by an element of Σ_3.

Now according to (4.6), X and X' can be embedded in $\mathbb{P}^2$ so as to have the equation $y^2 = x(x-1)(x-\lambda)$, or same with λ'. Since λ and λ' differ by an element of Σ_3 as in (4.5), after a linear change of variable in x, we have $\lambda = \lambda'$. Thus X and X' are both isomorphic to the same curve in $\mathbb{P}^2$.

(c) Given any $j \in k$, we can solve the polynomial equation

$$2^8(\lambda^2 - \lambda + 1)^3 - j\lambda^2(\lambda - 1)^2 = 0$$

for λ, and find a value of λ, necessarily $\neq 0, 1$. Then the equation $y^2 = x(x-1)(x-\lambda)$ defines a nonsingular curve of degree 3 in $\mathbb{P}^2$, which is therefore elliptic, and has the given j as its j-invariant.

□

Example 4.6.1. The curve $y^2 = x^3 - x$ of (I, Ex. 6.2) is nonsingular over any field k with $\mathrm{char} k \neq 2$. It has $\lambda = -1$, hence $j = 2^6 \cdot 3^3 = 1728$.

Example 4.6.2. The "Fermat curve" $x^3 + y^3 = z^3$ is nonsingular over any field k with char$k \neq 3$. Making a change of variables $x = x' + z$, and setting $x' = -\frac{1}{3}$, the equation becomes

$$z^2 - \frac{1}{3}z = y^3 - \frac{1}{27}.$$

From here one can reduce it to a standard form, as in the proof of (4.6), with $\lambda = -\omega$ or $-\omega^2$, where $\omega^3 = 1$. Therefore, $j = 0$.

Corollary 4.7. Let X be an elliptic curve over k with char$k \neq 2$. Let $P_0 \in X$, and let $G = \mathrm{Aut}(X, P_0)$ be the group of automorphisms of X leaving P_0 fixed. Then G is a finite group of order

$$\begin{array}{cc} 2 & \text{if } j \neq 0, 1728 \\ 4 & \text{if } j = 1728 \text{ and } \mathrm{char}k \neq 3 \\ 6 & \text{if } j = 0 \text{ and } \mathrm{char}k \neq 3 \\ 12 & \text{if } j = 0 (= 1728) \text{ and } \mathrm{char}k = 3. \end{array}$$

Proof. Let $f : X \to \mathbb{P}^1$ be a morphism of degree 2, with $f(P_0) = \infty$, branched over $0, 1, \lambda, \infty$ as above. If $\sigma \in G$ then by (4.4) there is an automorphism τ of $\mathbb{P}^1$ sending ∞ to ∞, such that $f \circ \sigma = \tau \circ f$. In particular, τ sends $\{0, 1, \lambda\}$ to $\{0, 1, \lambda\}$ in some order. If $\tau = \mathrm{id}$, then either $\sigma = \mathrm{id}$ or σ is the automorphism interchanging the sheets of f. Thus in any case we have two elements in G.

If $\tau \neq \mathrm{id}$, then τ permutes $\{0, 1, \lambda\}$ so λ must be equal to one of the other expressions of (4.5). This can happen only in the following cases:

(a) if $\lambda = -1$ or $\frac{1}{2}$ or 2, and char$k \neq 3$, then λ coincides with one other element under Σ_3, so G has order 4. This is the case $j = 1728$;

(b) if $\lambda = -\omega$ or $-\omega^2$, and char$k \neq 3$, then λ coincides with two other elements of its orbit under Σ_3, so G has order 6. In this case $j = 0$;

(c) if char$k = 3$ and $\lambda = -1$, then all six elements of the orbit are the same, so G has order 12. In this case $j = 0 = 1728$.

□

Section 5: The Canonical Embedding

Lemma 5.1. If $g \geq 2$, then the canonical linear system $|W|$ has no base points.

Proof. According to (3.1), we must show that for each $P \in X$, $\dim |W - P| = \dim |W| - 1$. Now $\dim |W| = \dim H^0(X, \omega_X) - 1 = g - 1$. On the other hand, since X is not rational, for any point P, $\dim |P| = 0$, so by Riemann-Roch we find $\dim |W - P| = g - 2$, as required. □

Recall that a curve X of genus ≥ 2 is called *hyperelliptic* (Ex. 1.7) if there is a finite morphism $f : X \to \mathbb{P}^1$ of degree 2. Considering the corresponding linear system, we see that X is hyperelliptic if and only if it has a linear system of dimension 1 and degree 2. It is convenient to introduce a classical notation. The *symbol* g^r_d will stand for "a linear system of dimension r and degree d." Thus we say that X is hyperelliptic if it has a g^1_2.

If X is a curve of genus 2, then the canonical linear system $|W|$ is a g^1_2 (Ex. 1.7). So X is necessarily hyperelliptic, and the canonical morphism $f : X \to \mathbb{P}^1$ is the 2-1 map of the definition.

Proposition 5.2. Let X be a curve of genus $g \geq 2$. Then $|W|$ is very ample if and only if X is not hyperelliptic.

Proof. We use the criterion of (3.1). Since $\dim |W| = g - 1$, we see that $|W|$ is very ample if and only if for every $P, Q \in X$, possibly equal, $\dim |W - P - Q| = g - 3$. Applying Riemann-Roch to the divisor $|P + Q|$, we have

$$\dim |P + Q| - \dim |W - P - Q| = 2 + 1 - g.$$

So the question is whether $\dim |P + Q| = 0$. If X is hyperelliptic, then for any divisor $P + Q$ of the g^1_2 we have $\dim |P + Q| = 1$. Conversely, if $\dim |P + Q| > 0$ for some P, Q then the linear system $|P + Q|$ contains a g^1_2 (in fact is a g^1_2), so X is hyperelliptic. This completes the proof. $\square$

Definition: If X is nonhyperelliptic of genus $g \geq 3$, the embedding $X \to \mathbb{P}^{g-1}$ determined by the canonical is the *canonical embedding* of X (determined up to an automorphism of $\mathbb{P}^{g-1}$), and its image, which is a curve of degree $2g - 2$, is a *canonical curve.*

Example 5.2.1. If X is a nonhyperelliptic curve of genus 3, then its canonical embedding is a quartic curve in $\mathbb{P}^2$. Conversely, and nonsingular quartic curve X in $\mathbb{P}^2$ has $\omega_X \cong \mathcal{O}_X(1)$ (II, 8.20.3), so it is a canonical curve. In particular, there exist nonhyperelliptic curves of genus 3 (see also (Ex. 3.2)).

Example 5.2.2. If X is a nonhyperelliptic curve of genus 4, then its canonical embedding is a curve of degree 6 in $\mathbb{P}^3$. We will show that X is contained in a unique irreducible quadric surface Q, and that X is the complete intersection (ideal generated by codim many elements?) of Q with an irreducible cubic surface F. Conversely, if X is a nonsingular curve in $\mathbb{P}^3$ which is a complete intersection of a quadric and a cubic surface, then $\deg X = 6$, and $\omega_X = \mathcal{O}_X(1)$ (II, Ex. 8.4), so X is a canonical curve of genus 4. In particular, there exist such nonsingular complete intersections by Bertini's theorem (II, Ex. 8.4), so there exist nonhyperelliptic curves of genus 4.

To prove the above assertions, let X be a canonical curve of genus 4 in $\mathbb{P}^3$, and let $\mathcal{I}$ be its ideal sheaf. Then we have an exact sequence

$$0 \to \mathcal{I} \to \mathcal{O}_{\mathbb{P}} \to \mathcal{O}_X \to 0.$$

Twisting by 2 and taking cohomology, we have

$$0 \to H^0(\mathbb{P}, \mathcal{I}(2)) \to H^0(\mathbb{P}, \mathcal{O}_{\mathbb{P}}(2)) \to H^0(X, \mathcal{O}_X(2)) \to 0.$$

Now the middle vector space has dimension 10 by (III, 5.1), and the right hand vector space has dimension 9 by Riemann-Roch on X (note that $\mathcal{O}_X(2)$ corresponds to the divisor $2W$, which is nonspecial of degree 12). So we conclude that

$$\dim H^0(\mathbb{P}, \mathcal{I}(2)) \geq 1.$$

An element of that space is a form of degree 2, whose zero-set will be a surface $Q \subseteq \mathbb{P}^3$ of degree 2 containing X. It must be irreducible (and reduced), because X is not contained in any $\mathbb{P}^2$. The curve X could not be contained in two distinct irreducible quadric surfaces Q, Q', because then it would be contained in there intersection $Q \cap Q'$ which is a curve of degree 4, and that is impossible because $\deg X = 6$. So we see that X is contained in a unique irreducible quadric surface Q.

Twisting the same sequence by 3 and taking cohomology, a similar calculation shows that

$$\dim H^0(\mathbb{P}, \mathcal{I}(3)) \geq 5.$$

The cubic forms in here consisting of the quadric form above times a linear form, form a subspace of dimension 4. Hence there is an irreducible cubic form in that space, so X is contained in an irreducible cubic surface F. Then X must be contained in the complete intersection $Q \cap F$, and since both have degree 6, X is equal to that complete intersection.

Proposition 5.3. Let X be a hyperelliptic curve of genus $g \geq 2$. Then X has a unique g^1_2. If $f_0 : X \to \mathbb{P}^1$ is the corresponding morphism of degree 2, then the canonical morphism $f : X \to \mathbb{P}^{g-1}$ consists of f_0 followed by the $(g-1)$-uple embedding of $\mathbb{P}^1$ in $\mathbb{P}^{g-1}$. In particular, the image $X' = f(X)$ is a rational curve of degree $g-1$ (Ex. 3.4), and f is a morphism of degree 2 onto X'. Finally, every effective canonical divisor on X is a sum of $g-1$ divisors in the unique g^1_2, so we write $|W| = \sum_1^{g-1} g^1_2$.

Proof. Proof is long. □

Theorem 5.4 (Clifford). Let D be an effective special divisor on the curve X. Then

$$\dim |D| \leq \frac{1}{2} \deg D.$$

Furthermore, equality occurs if and only if either $D = 0$ or $D = W$ or X is hyperelliptic and D is a multiple of the unique g^1_2 on X.

Lemma 5.5. Let D, E be effective divisors on a curve X. Then $\dim |D| + \dim |E| \leq \dim |D + E|$.

Proof. We define a map of sets

$$\varphi : |D| \times |E| \to |D + E|$$

by sending (D', E') to $D' + E'$ for any $D' \in |D|$ and $E' \in |E|$. The map φ is finite-to-one, because a given effective divisor can be written in only finitely many ways as a sum of two other effective divisors. On the other hand, since φ corresponds to the natural bilinear map of vector spaces

$$H^0(X, \mathcal{L}(D)) \times H^0(X, \mathcal{L}(E)) \to H^0(X, \mathcal{L}(D+E)),$$

we see that φ is a morphism when we endow $|D|, |E|$ and $|D+E|$ with their structure of projective spaces. Therefore, since φ is finite-to-one, the dimension of its image is exactly $\dim |D| + \dim |E|$, and from this the result follows. $\square$

Classification of Curves

To classify curves, we first specify the genus, which as we have seen (1.1.1) can be any nonnegative integer $g \geq 0$. If $g = 0$, X is isomorphic to $\mathbb{P}^1$ (1.3.5), so there is nothing further to say. If $g = 1$, then X is classified up to isomorphism by its j-invariant (4.1), so here again we have a good answer to the classification problem. For $g \geq 2$, the problem becomes much more difficult, and except for a few special cases (e.g., (Ex 2.2)), one cannot give an explicit answer.

For $g \geq 3$ we can subdivide the set $\mathfrak{M}_g$ of all curves of genus g according to whether the curve admits linear systems of certain degrees and dimensions. For example, we have defined X to be hyperelliptic if it has a g_2^1, and we have seen that there are hyperelliptic curves of every genus $g \geq 2$ (Ex. 1.7), and at least for $g = 3$ and 4, that there are nonhyperelliptic curves (5.2.1) and (5.2.2).

More generally, we can subdivide curves according to whether they have a g_d^1 for various d. If X has a g_3^1 it is called *trigonal*.

Remark 5.5.1. The facts here are as follows. For any $d \geq \frac{1}{2}g + 1$, any curve of genus g has a g_d^1; for $d < \frac{1}{2}g + 1$, there exist curves of genus g having no g_d^1. See Kleiman and Laksov [1] for proofs. Note that in particular this implies that there exist nonhyperelliptic curves of every genus $g \geq 3$ (V, Ex. 2.10). We give some examples of this result.

Example 5.5.2. For $g = 3, 4$ this result states that there exist nonhyperelliptic curves (which we have seen) and that every such curve has a g_3^1. Of course if X is hyperelliptic, this is trivial, by adding a point to the g_2^1. If X nonhyperelliptic of genus 3, then its canonical embedding is a plane quartic curve (5.2.1). Projecting form any point of X to $\mathbb{P}^1$, we have a g_3^1. Thus X has infinitely many g_3^1's.

If X is nonhyperelliptic of genus 4, then its canonical embedding in $\mathbb{P}^3$ lies on a unique irreducible quadric surface Q (5.2.2). If Q is nonsingular, then X has type (3,3) on Q (II, 6.6.1), and each of the two families of lines on Q cuts out a g_3^1 on X. So in this case X has two g_3^1's (to see that these are the only ones, copy the argument of (5.5.3) below). If Q is singular, it is a quadric cone, and the one family of lines on Q cuts out a unique g_3^1 on X.

Example 5.5.3. Let $g = 5$. Then (5.5.1) says that every curve of genus 5 has a g_4^1, and that there exist such curves with no g_3^1. Let X be a nonhyperelliptic curve of genus 5, in its canonical embedding as a curve of degree 8 in $\mathbb{P}^4$. First we show that X has a g_3^1 if and only if it has a trisecant in this embedding. Let $P, Q, R \in X$. Then by Riemann-Roch, we have

$$\dim |P + Q + R| = \dim |W - P - Q - R| - 1.$$

On the other hand, since X is in its canonical embedding, $\dim |W-P-Q-R|$ is the dimension of the linear system of hyperplanes in $\mathbb{P}^4$ which contain P, Q, R. Hence $\dim |P+Q+R| = 1$ if and only if P, Q, R are contained in a 2-dimensional family of hyperplanes, which is equivalent to saying that P, Q and R are collinear. Thus X has a g^1_3 if and only if it has a trisecant (and in that case it will have a 1-parameter family of trisecants).

Now let X be a nonsingular complete intersection of three quadric hypersurfaces in $\mathbb{P}^4$. Then $\deg X = 8$, and $\omega_X \cong \mathcal{O}_X(1)$, so X is a canonical curve of genus 5. If X had a trisecant L, then L would meet each of the quadric hypersurfaces, and so $L \subseteq X$ which is impossible. So we see that there exist curves of genus 5 containing no g^1_3.

Now projecting this X from one of its own points P to $\mathbb{P}^3$, we obtain a curve $X' \subseteq \mathbb{P}^3$ of degree 7, which is nonsingular (because X had no trisecants). This new curve X' must have trisecants, because otherwise a projection from one of its points would give a nonsingular curve of degree 6 in $\mathbb{P}^2$, which has the wrong genus. So let Q, R, S lie on a trisecant of X'. Then their inverse images on X, together with P, form four points which lie in a plane of $\mathbb{P}^4$. Then the same argument as above shows these points give a g^1_4.

Coming back to the general classification question, for fixed g one would like to endow the set $\mathfrak{M}_{\mathsf{g}}$ of all curves of genus g up to isomporphism with an algebraic structure, in which case we call $\mathfrak{M}_{\mathsf{g}}$ the *variety of moduli* if curves of genus g. Such is the case for $\mathsf{g} = 1$, where the j-invariants form an affine line.

The best way to specify the algebraic structure on $\mathfrak{M}_g$ would be to require it to be a universal parameter variety for families of curves of genus g, in the following sense: we require that there be a flat family $\mathfrak{X} \to \mathfrak{M}_g$ of curves of genus g such that for any other flat family $X \to T$ of curves of genus g, there is a unique morphism $T \to \mathfrak{M}_g$ such that X is the pullback of $\mathfrak{X}$. In this case we call $\mathfrak{M}_g$ a *fine moduli variety.* Unfortunately, there are several reasons why such a universal family cannot exist. One is that there are nontrivial families of curves, all of whose fibres are isomorphic to each other (III, Ex. 9.10).

However, Mumford has shown that for $g \geq 2$ there is a *coarse moduli variety* $\mathfrak{M}_g$, which has the following properties (Mumford [1, Th. 5.11]):

(1) the set of closed points of $\mathfrak{M}_g$ is in one-to-one correspondence with the set of isomorphism classes of curves of genus g;

(2) if $f : X \to T$ is any flat family of curves of genus g, then there is a morphism $h : X \to T$ such that for each closed point $t \in T$, X_t is in the isomorphism class of curves determined by the point $h(t) \in \mathfrak{M}_g$.

In case $g = 1$, the affine j-line is a coarse variety of moduli for families of elliptic curves with a section. One verifies condition (2) using the fact that j is a rational function of the coefficients of a plane embedding of the curve (Ex. 4.4).

Remark 5.5.4. In fact, Deligne and Mumford [1] have shown that $\mathfrak{M}_g$ for any $g \geq 2$ is an irreducible quasi-projective variety of dimension $3\mathsf{g} - 3$ over any fixed algebraically closed field.

Example 5.5.5. Assuming that $\mathfrak{M}_g$ exists, we can discover some of its properties. For example, using the method of (Ex. 2.2), one can show that hyperelliptic curves of genus g

are determined as two-fold coverings of $\mathbb{P}^1$, ramified at $0, 1, \infty$ and $2g-1$ additional points, up to the action of a certain finite group. Thus we see that the hyperelliptic curves correspond to an irreducible subvariety of dimension $2g-1$ of $\mathfrak{M}_g$. If $g = 2$, this is the whole space, which confirms that $\mathfrak{M}_2$ is irreducible of dimension 3.

Example 5.5.6. Let $g = 3$. Then the hyperelliptic curves form an irreducible subvariety of dimension 5 of $\mathfrak{M}_3$. The nonhyperelliptic curves of genus 3 are the nonsingular plane quartic curves. Since the embedding is canonical, two of them are isomorphic as abstract curves if and only if they differ by an automorphism of $\mathbb{P}^2$. The family of all these curves is parametrized by an open set $U \subseteq \mathbb{P}^N$ with $N = 14$, because a form of degree 4 has 15 coefficients. So there is a morphism $U \to \mathfrak{M}_3$, whose fibres are images of the group PGL(2) which has dimension 8. Since any individual curve has only finitely many automorphsims (Ex. 5.2), the fibres have dimension =8, and so the image of U has dimension $14 - 8 = 6$. So we confirm that $\mathfrak{M}_3$ has dimension 6.

Exercise 5.2. If X is a curve of genus ≥ 2 over a field of characteristic 0, show that the group Aut$X$ of automorphisms of X is finite. [*Hint*: If X is hyperelliptic, use the unique g_2^1 and show that Aut$X$ permutes the ramification points of the 2-fold covering $X \to \mathbb{P}^1$. If X is not hyperelliptic, show that Aut$X$ permutes the hyperosculation points of the canonical embedding. (Ex. 4.6: Let X be a curve of genus g embedded as a curve of degree d in $\mathbb{P}^n$, $n \geq 3$, not contained in any $\mathbb{P}^{n-1}$. For each point $P \in X$, there is a hyperplane H containing P, such that P counts at least n times in the intersection $H \cap X$. This is called an *osculating hyperplane* at P. It generalizes the notion of tangent line of curves in $\mathbb{P}^2$. If P counts at least $n+1$ times in $H \cap X$, we say H is a *hyperosculating hyperplane*, and that P is a *hyperosculation point*. It generalizes the notion of inflection point.)]