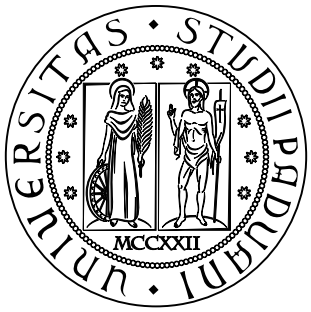

Università degli Studi di Padova

Dipartimento di Matematica "Tullio Levi-Civita"
Corso di Laurea in Matematica

Il Teorema di Riemann-Roch per Curve Algebriche Piane

Relatore:
dott. Adrian Iovita

Laureando:
Emanuele Ronda
Matricola № 1192199

Anno Accademico 2020-2021, Sessione di Laurea

Indice

Capitolo 1

Concetti Introduttivi

1.1 Anelli, Moduli e Campi

Un anello è una terna ordinata $(R, +, \cdot)$, tale che R è un insieme non vuoto, $(R, +)$ è un gruppo abeliano, la moltiplicazione è associativa su R e valgono le seguenti leggi distributive: $a(b + c) = ab + ac, (b + c)a = ba + ca$ per ogni $a, b, c \in R$. Se anche la moltiplicazione è commutativa diremo che l'anello è commutativo. Infine se esiste un elemento $e \in R$ tale che per ogni $a \in R$, vale che $ae = ea = a$, tale elemento è detto identità, è unico e l'anello è detto con identità.

Definizione 1.1. Un anello R in cui ogni ideale è finitamente generato è detto *noetheriano*.

D'ora in poi verranno considearti solo anelli commutativi con identità e, con abuso di nomenclatura, mi riferirò a questi come anelli.

Esercizio 1.2. *Sia R un anello noetheriano, e sia $\{r_i\}_{i\in\mathbb{N}} \subseteq R$ una successione di elementi di R tali che $(r_i) \subseteq (r_{i+1})$ per ogni i. Allora esiste $n \in \mathbb{N}$ tale che $(r_n) = (r_j)$ per ogni $j \geq n$.*

Dimostrazione. Considero l'ideale $I = (r_i : i \in \mathbb{N})$; siccome R è noetheriano, esiste $n \in \mathbb{N}$ tale che $I = (r_0, \ldots, r_n)$. Affermo che $(r_n) = (r_j)$ per ogni $j \geq n$. Sia dunque $j \geq n$ fissato. L'inclusione $(r_n) \subseteq (r_j)$ è data per ipotesi. Viceversa siccome $r_j \in I = (r_0, \ldots, r_n)$, esistono $a_0, \ldots, a_n \in R$ tali che $r_j = \sum_{i=0}^{n} a_i r_i$, ma siccome $r_i \in (r_n) \, \forall i \leq n$, si ha che $r_j = \sum_{i=0}^{n} a_i r_i \in (r_n)$. □

Lemma 1.3. *Sia R un anello. Le seguenti affermazioni sono equivalenti:*

a L'insieme degli elementi non invertibili in R ha la struttura di ideale

b R ha un unico ideale massimale che contiene tutti gli altri ideali propri di R.

Dimostrazione. Una dimostrazione di questo fatto si può trovare in [1] Capitolo 2, Paragrafo 4. □

Un anello che rispetta una (e quindi entrambe) delle condizioni del Lemma 1.3 è detto *anello locale.*

Lemma 1.4. *Sia R un dominio che non è un campo. Allora sono equivalenti le seguenti affermazioni:*

a R è noetheriano, locale e tale che l'ideale massimale sia principale.

b R è tale che esiste un elemento irriducibile $t \in R$ tale che per ogni altro elemento non nullo di $r \in R$, esistono unici un invertibile $u \in R$ e $n \in \mathbb{N}$ tali che $r = ut^n$.

Dimostrazione. Sia R noetheriano, locale e con ideale massimale principale. Sia M tale ideale e sia $t \in R$ un suo generatore.
Dimostro che, per ogni $r \in R, r \neq 0$, esistono u, n come nella seconda condizione: sia $r \in R, r \neq 0$ fissato.
Se r è un invertibile, basta scegliere $u = r, n = 0$ e si conclude. Sia quindi r un non invertibile: allora, $r \in M$, ed esiste $r_0 \in R$ tale che $r = r_0 t$; se r_0 è un invertibile ho concluso, altrimenti $r_0 \in M$, ed esiste $r_1 \in R$ tale che $r_0 = r_1 t$. Itero l'argomento.
Affermo che dopo un numero finito di passi trovo un r_i che è un invertibile. Se per assurdo così non fosse, costruisco una successione $\{r_i\}_{i \in \mathbb{N}} \subseteq R$ di elementi non invertibili e non nulli tali che $(r_i) \subseteq (r_{i+1})$ per ogni i. Per l'Esercizio 1.2 esiste un elemento massimale nella catena degli ideali principali, ovvero, esiste $n \in \mathbb{N}$ tale che $(r_n) = (r_j)\, \forall j \geq n$, in particolare $(r_n) = (r_{n+1})$, ma allora, esiste $s \in R$ tale che $r_{n+1} = sr_n$, perciò:

$$r_n = r_{n+1}t = sr_n t = str_n \Longrightarrow st = 1$$

Ma questo è assurdo perché t non è invertibile.
Dimostro l'unicità della scrittura: sia $r \in R$, e siano $u, v \in R$ invertibili ed $m, n \in \mathbb{N}$ tali che $r = ut^m = vt^n$. Ne segue che $ut^{m-n} = v$ dunque $m = n$ e di conseguenza $u = v$.
Viceversa, sia R tale che esiste un elemento irriducibile t, tale che per ogni altro elemento $r \in R, r \neq 0$, esistono unici $u \in R$ invertibile e $n \in \mathbb{N}$ tali che $r = ut^n$.
Chiaramente $M = (t)$ è un ideale massimale, e se $r \in R$ non è invertibile, per ipotesi è in M; viceversa se in M ci fosse un invertibile, allora $M = R$, ma questo è assurdo perché t è irriducibile. Ne segue che M contiene tutti e soli i non invertibili. Questo dimostra che R è locale.
Inoltre, essendo M l'unico ideale massimale, è principale perché generato da t.
Sia ora $I \trianglelefteq R$ non banale e diverso da M. Essendo R locale, $I \subseteq M$. Sia $r \in I$ non nullo, allora esiste $u \in R$ invertibile tale che $r = ut^n$ per un opportuno naturale n. Sia $m = \min\{n \in \mathbb{N} : r = ut^n, r \in I, r \neq 0\}$. Dimostro che $I = (t^m)$.
Sia $r \in I$, allora $r = ut^n$ per opportuni $u \in R$ invertibile, $n \in \mathbb{N}, n \geq m$, dunque $r = ut^{n-m}t^m \in (t^m)$.
Viceversa, esiste $r \in I$ tale che $r = ut^m$, per un opportuno invertibile u, allora $t^m = u^{-1}r \in I$. □

Un anello che rispetta una (e quindi entrambe) delle condizioni del Lemma 1.4 è detto *anello di valutazione discreta* e si scrive che è un DVR. Un elemento $t \in R$ come nella seconda condizione è detto *parametro uniformizzante*. Parametri uniformizzanti distinti sono tra loro associati.
Sia ora K il campo dei quozienti di R e sia t un parametro uniformizzante fissato: si osserva semplicemente che ogni elemento non nullo $z \in K$ ammette un'unica scrittura nella forma $z = ut^n$, dove u è un'invertibile in R e $n \in \mathbb{Z}$. L'esponente n è detto *ordine* di z e si scrive $n = \text{ord}(z)$. Si pone $\text{ord}(0) = \infty$.
L'ordine di un elemento di K è ben definito, ovvero, non dipende dalla scelta del parametro uniformizzante.

Dimostrazione. Siano $t, s \in R$ due parametri uniformizzanti e sia $u \in R$ invertibile tale che $t = us$. Sia ora $z \in K$ (con le stesse notazioni di sopra), e siano n_t, n_s gli ordini di z calcolati a partire da t e da s rispettivamente. Allora, per un opportuno invertibile $v \in R$:

$$z = vt^{n_t} = v(us)^{n_t} = vu^{n_t}s^{n_t}$$

e per l'unicità della scrittura con il parametro uniformizzante, $n_t = n_s$. □

Osservazione 1.5. Vale che $R = \{z \in K : \text{ord}(z) \geq 0\}$ e $M = \{z \in K : \text{ord}(z) > 0\}$.

Definizione 1.6. Sia R un anello ed M un insieme non vuoto, allora M si dice *R-modulo* se M è dotato di una operazione $+$ rispetto alla quale è un gruppo abeliano ed esiste un'azione di R su M, indicata come $\cdot : R \times M \to M$ tale che :

- $(a + b)m = am + bm$, $\forall a, b \in R, m \in M$;
- $a(m + n) = am + an$, $\forall a \in R, m, n \in M$;
- $(ab)m = a(bm)$, $\forall a, b \in R, m \in M$;
- $1_R m = m$, $\forall m \in M$.

Se $N \subseteq M$ è non vuoto, chiuso rispetto alla somma ed al prodotto per scalare, allora N è detto *sotto-R-modulo* di M. Il sotto-R-modulo generato da $S \subseteq M$ è l'insieme $M(S) = \{\sum_{i=0}^{k} r_i s_i : r_i \in R, s_i \in S \, \forall i \leq k, k \in \mathbb{N}\}$.
Sia ora X un insieme qualsiasi e considero l'insieme $M_X = \{\varphi : X \to R\}$, con la somma definita puntualmente ed il prodotto per scalare definito anch'esso puntualmente. Allora M_X è un R-modulo, ed è detto *R-modulo libero su X*. Sia ora $x \in X$ e sia $\varphi_x \in M_X$ definita come $\varphi_x(y) = 0$, se $x \neq y$ e $\varphi_x(x) = 1$, allora $X \subseteq M_X$.
Siano $K \leq L$ campi. Indico l'estensione di campi con $\frac{L}{K}$

Definizione 1.7. Un elemento $x \in L$ si dice *algebrico* su K, se esiste un polinomio $F \in K[X]$, tale che $F(x) = 0$, *trascendente* altrimenti. Allora $K[x]$ è il più piccolo anello che contiene sia K che x. Il suo campo dei quozienti è $K(x)$ ed è il più piccolo campo contenete sia K

che x.
L'estensione $\frac{L}{K}$ si dice *algerbica* se ogni $x \in L$ è algebrico su K.

Osservo ora che L ha una struttura di spazio vettoriale su K; allora, si dice che l'estensione $\frac{L}{K}$ è *finita* se $[L : K] = \dim_K L$ è finita.

Esercizio 1.8. *Siano $K \leq L$ campi e sia L un modulo finitamente generato su K. Allora per ogni anello $K \leq R \leq L$, R è un campo.*

Dimostrazione. Sia $r \in R, r \neq 0$ un elemento algebrico su K, allora esiste un polinomio monico $F \in K[X]$ tale che $F(r) = 0$, sia $F(X) = \sum_{i=0}^{n} a_i X^i$. Considero il polinomio $G(X) = \sum_{i=0}^{n} a_i X^{n-i}$; allora $G(r^{-1}) = 0$, moltiplicando per r^{1-n} e riordinando si trova che r^{-1} è combinazione di elementi di R, dunque è in R. Se r non è algerbico su K, il più piccolo modulo su K che contiene $K[r]$ non è finitamente generato, ma L contiene tale modulo ed L è finitamente generato per ipotesi. Dunque un tale elemento non può esistere. Ne segue che R è un campo. □

Teorema 1.9 (Dell'elemento primitivo)**.** *Sia K un campo di caratteristica 0, e sia $\frac{L}{K}$ un'estensione algerbica finita. Allora, esiste $\alpha \in L$, tale che $L = K(\alpha)$.*

Dimostrazione. Una versione più generale di questo risultato è dimostrata in [2] Capitolo 5. □

1.2 Spazi affini e spazi proiettivi

Sia k un campo. Uno *spazio affine di dimensione n su k* è una terna ordinata $\mathbb{A} = (A, V, +)$, dove A è un insieme, detto insieme dei punti, V è uno spazio vettoriale su k di dimensione n, in biiezione insiemistica con A e $+ : A \times V \to A$ è un'azione di V su A tale che, $P + v = P \iff v = 0$, $\forall P \in A$ e $\forall P, Q \in A$ esiste $v \in V$ tale che $P + v = Q$.
Se $A = V = k^n$, allora lo spazio $\mathbb{A}$ è detto *spazio affine standard di dimensione n sul campo k* e si denota con $\mathbb{A}^n(k)$, o anche con $\mathbb{A}^n$. In tal caso, $P \in \mathbb{A}^n$, si indica con $P = (x_1, \ldots, x_n)$ e queste sono dette coordinate di P.
Considero ora lo spazio vettoriale k^{n+1}. Definisco su k^{n+1} la relazione $\sim$, definita per ogni $x, y \in k^{n+1}$ da $x \sim y \iff$ esiste $\lambda \in k, \lambda \neq 0$ tale che $x = \lambda y$.
La relazione definita è un'equivalenza su k^{n+1}. Sia dunque $\mathbb{P}^n(k)$, o semplicemente $\mathbb{P}^n$, l'insieme quoziente $\frac{k^{n+1}}{\sim}$. Questo insieme è detto *spazio proiettivo* standard di dimensione n sul campo k. I suoi elementi sono detti *punti proiettivi*. Inoltre se $x = (x_1, \ldots, x_{n+1}) \in k^{n+1}$ e $P \in \mathbb{P}^n$ è la sua immagine nel quoziente si scrive $P = [x_1, \ldots, x_{n+1}]$ e si dice che $[x_1, \ldots, x_{n+1}]$ sono delle *coordinate omogenee* del punto proiettivo P.
Fissato un sistema di coordinate omogenee su $\mathbb{P}^n$, considero, per ogni $i \leq n$, l'insieme $U_i = \{P = [x_1, \ldots, x_{n+1}] \in \mathbb{P}^n : x_i \neq 0$[1]$\}$, e la mappa $\varphi_i : U_i \to \mathbb{A}^n$, definita da $\varphi_i([x_1, \ldots, x_{n+1}]) = (\frac{x_1}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i})$, ciascuna di queste mappe è una biiezione.

[1] Questa proprietà è indipendente dalla scelta delle coordinate omogenee.

1.3 Insiemi Algebrici

Sia d'ora in poi k un campo algebricamente chiuso di caratteristica 0, e siano $\mathbb{A}^n, \mathbb{P}^n$ lo spazio affine e lo spazio proiettivo standard di dimensione n su k.

1.3.1 Caso Affine

Definizione 1.10. Sia $S \subseteq k[X_1, \ldots, X_n]$, definisco *l'insieme algebrico affine* $V(S) = \{P = (x_1, \ldots, x_n) \in \mathbb{A}^n : F(P) = 0 \forall F \in S\}$. Se $I \trianglelefteq k[X_1, \ldots, X_n]$ è l'ideale generato da S, vale che $V(I) = V(S)$. Un insieme algebrico affine V è detto *irriducibile* se non è unione di insiemi algebrici affini strettamente contenuti in V. Un insieme algebrico affine irriducibile è detto *varietà affine*.

Proposizione 1.11. *Unione finita di insiemi algebrici è un insieme algebrico. Intersezione arbitraria di insiemi algebrici è un insieme algebrico.* $\emptyset, \mathbb{P}^n$ *sono insiemi algebrici.*

Dimostrazione. La dimostrazione di questo fatto nel caso affine è analoga a quella del caso proiettivo nella proposizione 1.21 □

Definizione 1.12. Sia $X \subseteq \mathbb{A}^n$, definisco l'ideale associato ad X come $I(X) = \{F \in k[X_1, \ldots, X_n] : F(P) = 0 \, \forall P \in X\}$.

Osservazione 1.13. La definizione è ben posta, ovvero $I(X)$ è effettivamente un ideale per ogni X.

Proposizione 1.14. *Un insieme algebrico V è irriducibile se e solo se $I(V)$ è un ideale primo.*

Dimostrazione. Sia V irriducibile e siano $F, G \in k[X_1, \ldots, X_n]$ tali che $FG \in I(V)$. Allora, considero gli insiemi $V(F) = \{P \in V : F(P) = 0\}$ e $V(G) = \{P \in V : G(P) = 0\}$. Chiaramente $V(F) \cup V(G) \subseteq V$. Inoltre siccome $FG \in I(V), F(P)G(P) = 0$, quindi per ogni $P \in V, F(P) = 0$ oppure $G(P) = 0$, dunque $V \subseteq V(F) \cup V(G)$.
Ma V è irriducibile, quindi $V = V(F)$ oppure $V = V(G)$, da cui $F \in I(V)$ oppure $G \in I(V)$.
Viceversa sia V tale che $I(V)$ sia primo e siano $V_1, V_2 \subseteq V$ insiemi algebrici tali che $V = V_1 \cup V_2$. Se $V_1 = \emptyset$ oppure $V_2 = \emptyset$, allora l'altro è uguale a V e non c'è nulla da dimostrare. Suppongo quindi $V_1 \neq \emptyset \neq V_2$. Allora $I(V) \subseteq I(V_1), I(V_2) \implies I(V) \subseteq I(V_1) \cap I(V_2)$. Viceversa:

$$F \in I(V_1) \cap I(V_2) \implies F(P) = 0 \forall P \in V_1 \cup V_2 = V \implies F \in I(V)$$

Vale che $I(V) = I(V_1) \cap I(V_2)$. Sia $F \in I(V_1) \setminus I(V)$, allora, per ogni $G \in I(V_2)$, essendo $FG \in I(V)$ ed $F \notin I(V)$, allora, $G \in I(V)$, da cui $V_2 = V$. □

Sia dunque $V \subseteq \mathbb{A}^n$ un insieme algebrico irriducibile e sia $I(V)$ il suo ideale primo associato. Allora considero l'anello $\Gamma(V) = \frac{k[X_1,\ldots,X_n]}{I(V)}$. Siccome $I(V)$ è primo, $\Gamma(V)$ è un dominio ed è detto *anello coordinato associato* a V.
Siccome $\Gamma(V)$ è dominio, allora è ben definito il suo campo dei quozienti. Sia $k(V)$. Tale campo è detto *campo delle funzioni razionali su* V. Siano ora $P \in V, z \in k(V)$ fissati; si dice che z è definita in P, se esistono $f, g \in \Gamma(V)$, tali che $z = \frac{f}{g}$ e $g(P) \neq 0$. Si definisce a questo punto $\mathcal{O}_P(V) = \{z \in k(V) : z \text{ è definita in } P\}$. $\mathcal{O}_P(V)$ è un anello locale, con ideale massimale $M_P(V) = \{z \in \mathcal{O}_P(V) : z(P) = 0\}$.

1.3.2 Caso Proiettivo

Definizione 1.15. Un punto $P \in \mathbb{P}^n$ si dice *zero* del polinomio $F \in k[X_1, \ldots, X_{n+1}]$ se per ogni scelta $[x_1, \ldots, x_{n+1}]$ di coordinate omogenee per P, vale che $F(x_1, \ldots, x_{n+1}) = 0$, e si scrive $F(P) = 0$.

Vale il seguente:

Lemma 1.16. *Sia $F \in k[X_1, \ldots, X_{n+1}]$ un polinomio di grado d, e siano $F_0, \ldots, F_d \in k[X_1, \ldots, X_{n+1}]$ polinomi omogenei tali che $F = \sum_{i=0}^{d} F_i$ e F_i ha grado i. Allora un punto $P \in \mathbb{P}^n$ è zero di F se e solo se è zero di F_i per ogni i.*

Dimostrazione. Suppongo che P è uno zero di F, allora, se $[x_1, \ldots, x_{n+1}]$ sono coordinate omogenee per P, per ogni $\lambda \in k, \lambda \neq 0$, anche $[\lambda x_1, \ldots, \lambda x_{n+1}]$ sono coordinate omogenee per P. Dunque:

$$0 = F(x_1, \ldots, x_{n+1}) = F(\lambda x_1, \ldots, \lambda x_{n+1}) = \\ = \sum_{i=0}^{d} F_i(\lambda x_1, \ldots, \lambda x_{n+1}) = \sum_{i=0}^{d} \lambda^i F_i(x_1, \ldots, x_{n+1}) = G(\lambda)$$

Osservo ora che l'equazione polinomiale $G(t) = 0$ ha un numero infinito di soluzioni, dunque il polinomio G è nullo, ovvero $F_i(x_1, \ldots, x_{n+1}) = 0$ per ogni scelta di coordinate omogenee $[x_1, \ldots, x_{n+1}]$ per P per ogni i, da cui la tesi.
Viceversa, se P è zero di F_i per ogni i, per ogni scelta di coordinate proiettive $[x_1, \ldots, x_{n+1}]$ per P:

$$F(x_1, \ldots, x_{n+1}) = \sum_{i=0}^{d} F_i(x_1, \ldots, x_{n+1}) = 0$$

□

Sia ora $S \subseteq k[X_1, \ldots, X_{n+1}]$, allora definisco $V(S) = \{P \in \mathbb{P}^n : F(P) = 0 \forall F \in S\}$. Chiaramente se I è l'ideale generato da S, vale che: $V(I) = V(S)$. Un tale insieme è detto *insieme algebrico proiettivo.*

Osservo ora che siccome $k[X_1, \ldots, X_{n+1}]$ è noetheriano, I è finitamente generato, ovvero $I = (F^1, \ldots, F^r)$. Ciascuno degli $(F^i)_{i=1}^r$ può essere scritto come somma di polinomi omogenei nella forma $F^i = \sum_{j=0}^{d_i} F^i_j$, con d_i grado di F_i e F^i_j polinomio omogeneo di grado j. Dunque $V(I) = V(F^1, \ldots, F^r) = V(F^i_j : j \in \{0, \ldots, d_i\}, i \in \{1, \ldots, r\})$.

Definizione 1.17. Un ideale $I \trianglelefteq k[X_1, \ldots, X_{n+1}]$ si dice *omogeneo* se per ogni $F \in I, F = \sum_{i=0}^{d} F_i$, dove d è il grado di F e F_i è un polinomio omogeneo di grado i per ogni i, allora $F_i \in I$ per ogni i.

Definizione 1.18. Sia $X \subseteq \mathbb{P}^n$ pongo $I(X) = \{F \in k[X_1, \ldots, X_{n+1}] : F(P) = 0 \forall P \in X\}$ l'ideale associato ad X.

Osservazione 1.19. $I(X)$ è un ideale omogeneo per ogni $X \subseteq \mathbb{P}^n$.

Proposizione 1.20. *Un ideale $I \trianglelefteq k[X_1, \ldots, X_{n+1}]$ è omogeneo se e solo se è generato da un numero finito di polinomi omogenei*

Dimostrazione. Una dimostrazione di questo fatto è in [1] Capitolo 4, Paragrafo 2. □

Proposizione 1.21. *Unione finita di insiemi algebrici è un insieme algebrico. Intersezione arbitraria di insiemi algebrici è un insieme algebrico. $\emptyset, \mathbb{P}^n$ sono insiemi algebrici.*

Dimostrazione. Siano $S_1, S_2 \subseteq k[X_1, \ldots, X_{n+1}]$, dimostro che $V(S_1) \cup V(S_2) = V(S_1 S_2)$:
Sia $P \in V(S_1) \cup V(S_2)$, allora $P \in V(S_1)$ oppure $P \in V(S_2)$, cioè $F(P) = 0 \forall F \in S_1$ oppure $G(P) = 0 \forall G \in S_2$. Ne segue che $\forall F \in S_1 \forall G \in S_2\, FG(P) = F(P)G(P) = 0$, dunque $V(S_1) \cup V(S_2) \subseteq V(S_1 S_2)$.
Viceversa sia $P \in V(S_1 S_2)$ e suppongo per assurdo che $P \notin V(S_1) \cup V(S_2)$, ovvero che esistano $F \in S_1, G \in S_2$ tali che $F(P) \neq 0 \neq G(P)$, allora $0 = FG(P) = F(P)G(P)$, entrambi non nulli. Assurdo.
Per induzione segue il risultato per famiglie finite.
Sia ora $(S_\alpha)_{\alpha \in A}$, con A insieme arbitrario, tali che $S_\alpha \subseteq k[X_1, \ldots, X_{n+1}] \forall \alpha \in A$. Allora, $\cap_{\alpha \in A} V(S_\alpha)$ è un insieme algebrico: chiaramente,

$$\bigcap_{\alpha \in A} V(S_\alpha) = V(\bigcup_{\alpha \in A} S_\alpha)$$

e quest'ultimo è algebrico. Per dimostrare tale uguaglianza:

$$P \in \bigcap_{\alpha \in A} V(S_\alpha) \Longrightarrow \forall \alpha \in A \forall F \in S_\alpha F(P) = 0 \Longrightarrow \forall F \in \bigcup_{\alpha \in A} S_\alpha F(P) = 0$$

. Viceversa:

$$P \in V(\bigcup_{\alpha \in A} S_\alpha) \Longrightarrow \forall F \in \bigcup_{\alpha \in A} S_\alpha F(P) = 0 \Longrightarrow \forall \alpha \in A \forall F \in S_\alpha F(P) = 0$$

.
$\emptyset = \{P \in \mathbb{P}^n : 1 = 0\} = V(1)$ e $\mathbb{P}^n = \{P \in \mathbb{P}^n : 0 = 0\} = V(0)$. □

Osservazione 1.22. Gli insiemi algebrici, sia affini che proiettivi, sono dei chiusi per una topologia.

Osservo ora che se $F \in k[X_1, \ldots, X_{n+1}]$ è un polinomio omogeneo, è ben definito, per ogni $i \leq n+1$ un polinomio in n indeterminate, detto affinizzato di F rispetto alla i-esima coordinata omogenea: $F_i(X_1, \ldots, \hat{X_i}, \ldots, X_{n+1}) = F(X_1, \ldots, X_{i-1}, 1, X_{i+1}, \ldots, X_n)$. $V = V(F), V_i = V(F_i) \forall i \leq n+1$, sono insiemi algebrici proiettivo e affini tali che $\forall i \leq n+1 \, \varphi_i(V \cap U_i) = V_i$. Un insieme algebrico proiettivo $V = V(S) \subseteq \mathbb{P}^n, S \subseteq k[X_1, \ldots, X_{n+1}]$ si dice *irriducibile* se non è unione di insiemi algebrici più piccoli. Un insieme algebrico irriducibile è detto *varietà*. Vale anche in questo caso che V è irriducibile se e solo se $I(V)$ è primo.
Sia dunque V un insieme algebrico irriducibile proiettivo e sia $I(V)$ il suo ideale primo associato. Allora considero l'anello $\Gamma_h(V) = \frac{k[X_1,\ldots,X_{n+1}]}{I(V)}$. Siccome $I(V)$ è primo, $\Gamma_h(V)$ è un dominio ed è detto *anello omogeneo associato* a V.
Un elemento di $\Gamma_h(V)$ è detto omogeneo se è immagine, tramite la proiezione, di un polinomio omogeneo in $k[X_1, \ldots, X_{n+1}]$. Indico la proiezione con π_V. Siccome $\Gamma_h(V)$ è dominio, allora è ben definito il suo campo dei quozienti. Sia $k_h(V)$. Osservo ora che se $f, g \in \Gamma_h(V)$ sono omogenei dello stesso grado, il rapporto $\frac{f}{g}$ induce una funzione sui punti di V sui quali g non si annulla, infatti, fissato un punto $P \in V$ tale che $g(P) \neq 0$, fissate delle coordinate omogenee $\bar{x}$ per P, e detto d il comune grado di f e g, per ogni $\lambda \in k \setminus \{0\}$, quindi per ogni altra scelta di coordinate omogenee per P:

$$\frac{f(\lambda x)}{g(\lambda x)} = \frac{\lambda^d f(x)}{\lambda^d g(x)} = \frac{f(x)}{g(x)}$$

Queste osservazioni portano a dare la seguente:

Definizione 1.23. Il campo delle funzioni su V è $k(V) = \{z \in k_h(V) : z = \frac{f}{g}, f, g \text{ omogenei di stesso grado}\}$. Gli elementi di $k(V)$ sono detti *funzioni razionali su* V.

$k(V)$ è un sottocampo di $k_h(V)$.
Siano ora $P \in V, z \in k(V)$ fissati; si dice che z è definita in P, se esiste una coppia di omogenei dello stesso grado f, g, tali che $z = \frac{f}{g}$ e $g(P) \neq 0$. Si definisce a questo punto $\mathcal{O}_P(V) = \{z \in k(V) : z \text{ è definita in } P\}$. $\mathcal{O}_P(V)$ è un anello locale, con ideale massimale $M_P(V) = \{z \in \mathcal{O}_P(V) : z(P) = 0\}$.

1.4 Curve Algebriche Piane

1.4.1 Caso Affine

Siano $F, G \in k[X,Y]$, tali polinomi si dicono equivalenti se esiste $\lambda \in k, \lambda \neq 0$ tale che $F = \lambda G$. Questa relazione è un'equivalenza su $k[X,Y]$.
Definisco una *curva piana affine* come una classe di equivalenza di polinomi non costanti rispetto alla relazione introdotta. Dunque posso definire il grado di una curva come il grado di un polinomio (e quindi di tutti i polinomi) della classe di equivalenza.
Sia quindi una curva fissata ed F un rappresentante. Se $F = \prod F_i^{e_i}$, con gli F_i non costanti, irriducibili ed a due a due non associati, allora, si dice che F_i è una *componente della curva F di molteplicità e_i*. Se invece, F è irriducibile, allora $V(F)$ è una varietà affine, dunque sono ben definiti $\Gamma(V(F)), k(V(F)), \mathcal{O}_P(V(F))$, e si indicano con $\Gamma(F), k(F), \mathcal{O}_P(F)$.
Sia ora F una curva e P un suo punto. Si dice che P è un *punto semplice per F* se $F_X(P) \neq 0$ o $F_Y(P) \neq 0$, dove F_X, F_Y sono le derivate parziali di F. In tal caso, la retta $F_X(P)(X - x_P) + F_Y(P)(Y - y_P) = 0$, è detta retta tangente ad F in P.
Suppongo ora che, a meno di una traslazione, $P = (0,0)$; allora $F = F_m + \cdots + F_n$, dove $n = \deg(F), F_i$ è polinomio omogeneo di grado i in $k[X,Y]$, per ogni i ed $F_m \neq 0$. Si definisce la *molteplicità della curva F nel punto P* come m e si scrive $m_P(F) = m$. Infine siccome, F_m è omogeneo in due variabili, può essere scritto nella forma $F_m = \prod_{i=1}^{s} L_i^{r_i}$, dove gli L_i sono fattori lineari a due a due non associati. Gli L_i sono le rette tangenti a F in P e ciascuna ha molteplicità r_i.

Osservazione 1.24. $P \in F \iff m_P(F) > 0$. Se P è semplice $m_P(F) = 1$. Se $m_P(F) > 1, P$ è detto punto *multiplo*.

Il linguaggio degli anelli coordinati e degli anelli locali offre una diversa, ma equivalente caratterizzazione dei punti semplici e della molteplicità di una curva in un suo punto. Userò la seguente notazione: per $G \in k[X,Y], g$ è la sua immagine in $\Gamma(F) = \frac{k[X,Y]}{(F)}$.

Proposizione 1.25. *Un punto $P \in F$ è semplice se e solo se $\mathcal{O}_P(F)$ è un DVR. Inoltre se L è una retta per P che non è tangente in P a F, allora $\ell \in \mathcal{O}_P(F)$ è un parametro uniformizzante.*

Dimostrazione. Per la dimostrazione si veda [1] Capitolo 3, Paragrafo 2. □

Proposizione 1.26. *Sia $P \in F, F$ irriducibile. Allora $m_P(F) = \dim_k \frac{M_P(F)^n}{M_P(F)^{n+1}}$ per n sufficientemente grande.*

Dimostrazione. Si veda [1] Capitolo 3, Paragrafo 2. □

In particolare, da questo segue che la molteplicità di un punto dipende solo dal suo anello locale. Inoltre se P è semplice, allora $\mathcal{O}_P(F)$ è un DVR; sia ord_P^F la funzione ordine indotta su $k(F)$.

Siano ora F, G curve piane e $P \in \mathbb{A}^2$. Si definisce la *molteplicità di intersezione* di F e G in P come $I(P, F \cap G) = \dim_k \frac{\mathcal{O}_P(\mathbb{A}^2)}{(F,G)}$. La moltepilicità di intersezione gode delle seguenti proprietà:

- $I(P, F \cap G)$ esiste per ogni coppia di curve e per ogni punto;
- $I(P, F \cap G) \in \mathbb{N}$ se F, G non hanno componenti comuni passanti per P, altrimenti, se F, G hanno componenti comuni passanti per $P, I(P, F \cap G) = \infty$;
- $I(P, F \cap G) = 0 \iff P \notin F \cap G$, e $I(P, F \cap G)$ dipende solo dalle componenti di F e G passanti per P;
- Se T è un cambio di coordinate affini, e $T(Q) = P$, allora $I(Q, F \cap G) = I(P, F^T \cap G^T)$;
- $I(P, F \cap G) = I(P, G \cap F)$;
- $I(P, F \cap G) \geq m_P(F) m_P(G)$ e vale l'uguaglianza se e solo se F, G non hanno tangenti in P in comune;
- Se $F = \prod_{i=1}^{p} F_i^{r_i}, G = \prod_{j=1}^{q} G_j^{s_j}$, allora $I(P, F \cap G) = \sum_{i,j} r_i s_j I(P, F_i \cap G_j)$;
- $I(P, F \cap G) = I(P, F \cap (G + AF))$, $\forall A \in k[X, Y]$;
- Se P è un punto semplice di F, allora, $I(P, F \cap G) = \mathrm{ord}_P^F(G)$;
- Se F, G non hanno componenti comuni $\sum_{P \in \mathbb{A}^2} I(P, F \cap G) = \dim_k \frac{k[X,Y]}{(F,G)}$.

1.4.2 Caso Proiettivo

Siano $F, G \in k[X, Y, Z]$ due polinomi omogenei non-costanti. Allora, F, G si dicono equivalenti se esiste $\lambda \in k, \lambda \neq 0$, tale che $F = \lambda G$. Questa è un'equivalenza tra i polinomi omogenei. Si definisce una *curva piana proiettiva* come una classe di equivalenza. Il grado di una tale curva è il grado di un polinomio che la definisce.
Osservo ora che se F è una curva proiettiva e $P = [x, y, 1]$ è un suo punto, allora, $(x, y) \in \mathbb{A}^2$ è un punto della curva affine F_*, definita come $F_*(X, Y) = F(X, Y, 1)$, ovvero F_* è *l'affinizzato* di F. In particolare $\mathcal{O}_P(F)$ è isomorfo a $\mathcal{O}_{(x,y)}(F_*)$, dunque se $P \in U_3$ (o simmetricamente in U_1 o U_2), risulta ben definita la molteplicità in P di F, grazie alla teoria delle curve affini. In generale, dati dei punti $P_1, \ldots, P_n \in \mathbb{P}^2$, esiste una retta L che non contiene alcuno di questi punti. Allora, a meno di un cambio di coordinate, posso supporre che questa retta sia la retta Z, quindi i P_i hanno coordinate $[x_i, y_i, 1]$.
Siccome c'è questa corrispondenza fra curve proiettive ed affini, risulta definita anche la molteplicità di intersezione di due curve proiettive in un punto. Una retta L è detta *tangente* ad una curva F in un punto P se $I(P, L \cap F) \geq m_P(F)$. Un punto multiplo è detto *ordinario* se ammette $m_P(F)$ tangenti distinte.

Enuncio ora due teoremi che saranno molto importanti nel seguito.

Teorema 1.27 (di Bezout)**.** *Siano F, G curve piane proiettive prive di componenti comuni. Sia $n = \deg(F), m = \deg(G)$. Allora $\sum_{P \in \mathbb{P}^2} I(P, F \cap G) = mn$.*

Dimostrazione. Si veda [1] Capitolo 5, Paragrafo 3. □

Definizione 1.28. Siano F, G due curve passanti per P prive di componenti comuni per P e sia H un'altra curva. Allora, si dice che *le condizioni di Noether sono soddisfate in P rispettivamente a F, G, H* se $H_* \in (F_*, G_*) \subseteq \mathcal{O}_P(\mathbb{A}^2)$.

Teorema 1.29 (Fondamentale di Noether)**.** *Siano F, G, H curve piane proiettive. Suppongo che F, G non abbiano componenti comuni. Allora esistono $A, B \in k[X, Y, Z]$ omogenei tali che $H = AF + BG$ se e solo se le condizioni di Noether sono soddisfatte in P, per ogni $P \in F \cap G$.*

Dimostrazione. Si veda [1] Capitolo 5, Paragrafo 5. □

1.5 Varietà, Morfismi e Mappe Razionali

A questo punto risulta utile definire una topologia su $\mathbb{P}^n$(e su $\mathbb{A}^n$): la *topologia di Zariski*, definita per ogni $U \subseteq \mathbb{P}^n$, come U è un aperto se e solo se $\mathbb{P}^n \setminus U$ è un insieme algebrico. Per l'Osservazione 1.22, quella definita è effettivamente una topologia. Sia ora V un insieme algebrico irriducibile, e considero su V la topologia indotta dalla topologia di Zariski. Siano $U_1, U_2 \subseteq V$ due aperti, allora, $U_1 \cap U_2 \neq \emptyset$ perché altrimenti, $V = (V \setminus U_1) \cup (V \setminus U_2)$, sarebbe riducibile. Ne segue che per ogni coppia di punti distinti $P, Q \in V$ i loro intorni non sono mai disgiunti. Ne segue che $\mathbb{P}^n$ con la topologia di Zariski non è uno spazio Hausdorff.

Definizione 1.30. Sia $V \subseteq \mathbb{P}^n$ un insieme algebrico irriducibile, e sia $X \subseteq V$ un aperto. X è detto varietà. Analogamente risultano definite le varietà per insiemi affini.

Analogamente a quanto visto per gli insiemi algebrici, possiamo definire le funzioni razionali su X varietà, come $k(X) = \{f_{\restriction X} : f \in k(V)\}$, ed analogamente, per $P \in X, \mathcal{O}_P(X) = \{f \in k(X) : f \text{ è definita in } P\}$.
Se $U \subseteq X$ è aperto, allora U è aperto in V, dunque è una varietà ed è detto *sottovarietà aperta* di X.
Sia ora $Y \subseteq X$ un chiuso, allora, Y si dice irriducibile se non è unione di due suoi sottoinsiemi propri e chiusi in X. Se Y è irriducibile, allora, detta $\bar{Y}$ la sua chiusura in V, $Y = \bar{Y} \cap X$ è un aperto di $\bar{Y}$, quindi è una varietà di $\bar{Y}$, ed è detta *sottovarietà chiusa* di X. Analoghe definizioni valgono nel caso affine.
Sia ora $U \subseteq X$ un aperto non vuoto; definisco $\Gamma(U) = \{f \in k(X) : f \text{ è definita in ogni punto } P \in U\} = \cap_{P \in U} \mathcal{O}_P(X)$.
Considero dunque l'anello $\mathcal{I}(U, k)$ delle mappe da U a k.

Lemma 1.31. *Sia X una varietà proiettiva e sia U un suo sottoinsieme aperto. Sia $z \in \Gamma(U)$ tale che $z(P) = 0$ per ogni $P \in U$. Allora $z = 0$.*

Dimostrazione. Sia $z \in \Gamma(U)$, allora $z \in k(X)$ e z è definita in ogni punto di U; cioè $z = \frac{f}{g}, f, g \in \Gamma_h(X)$ omogenei dello stesso grado, con $g(P) \neq 0 \forall P \in U$. Allora $f(P) = 0 \forall P \in U$.
Dimostro ora che $z = \frac{f}{g} : U \to k$ è una funzione continua se considero su U la topologia indotta dalla topologia di Zariski e su k la topologia di Zariski, una volta identificato $k = \mathbb{A}^1(k) = \mathbb{A}^1$. Sia un chiuso $A \subseteq \mathbb{A}^1$ un chiuso, allora, è un insieme finito. Dunque siccome le antiimmagini commutano con le unioni è sufficiente dimostrare che $z^{-1}(a)$ è un chiuso per ogni $a \in \mathbb{A}^1 = k$.

$$z^{-1}(a) = \{P \in U : z(P) = a\} = \{P \in U : f(P) - ag(P) = 0\} = \\ = \{P \in U : F(P) - aG(P) = 0\} = V(F - aG) \cap U$$

dove F, G sono polinomi omogenei che vengono mappati in f, g nel quoziente $\Gamma_h(X)$. In particolare, $z^{-1}(a)$ è algebrico quindi chiuso.

Infine essendo quindi z continua, ed essendo U denso per la topologia di Zariski, $z(X) = z(\bar{U}) \subseteq \bar{0} = 0$. Ne segue $z = 0$. □

Siccome quindi la mappa $\Gamma(U) \to \mathcal{I}(U,k)$ è una mappa iniettiva, posso identificare $\Gamma(U)$ con la sua immagine.
D'ora in poi con varietà intenderò sia insiemi algebrici proiettivi (o affini) irriducibili, sia quelle che ho chiamato sottovarietà (aperte e chiuse) sia affini che proiettive. Siano quindi X, Y varietà e sia $\varphi : X \to Y$ una mappa insiemistica. Allora è ben definito l'omomorfismo d'anelli, $\tilde{\varphi} : \mathcal{I}(Y,k) \to \mathcal{I}(X,k)$ definito per ogni funzione $f \in \mathcal{I}(Y,k)$ da $\tilde{\varphi}(f) = f \circ \varphi$.

Definizione 1.32. Una mappa $\varphi : X \to Y$, con X, Y varietà è detta *morfismo*, se:

1. φ è continua rispetto alle topologie di Zariski su X e Y;
2. per ogni aperto $U \subseteq Y$ e per ogni $f \in \Gamma(U)$, allora $f \circ \varphi \in \Gamma(\varphi^{-1}(U))$.

Un *isomorfismo* è un morfismo φ che è invertibile e φ^{-1} è un morfismo.

Definizione 1.33. Siano $V \subseteq \mathbb{A}^n, W \subseteq \mathbb{A}^m$; una mappa $p : V \to W$ è una *mappa polinomiale* se $p = (p_1, \ldots, p_m)$ e $p_i \in k[X_1, \ldots, X_n]\, \forall i$.

D'ora in poi mi userò la seguente nomenclatura: dirò che una varietà è affine se è isomorfa ad una varietà in uno spazio affine.

Proposizione 1.34. *Siano X,Y varietà affini. Allora esiste una corrispondenza iniettiva fra morfismi $\varphi : X \to Y$ ed omomorfismi $\tilde{\varphi} : \Gamma(Y) \to \Gamma(X)$. In particolare, un morfismo di $X \subseteq \mathbb{A}^n$ in $Y \subseteq \mathbb{A}^m$ è equivalente ad una mappa polinomiale.*

Dimostrazione. Si veda [1] Capitolo 6, Paragrafo 3. □

Esempio 1.35. Fissato $V \subseteq \mathbb{P}^n$, una varietà, $U_i, \varphi_i, i\{1, \ldots, n+1\}$ gli aperti e le mappe definiti in 1.2. Siano inoltre $V_i = V \cap U_i, \tilde{V_i} = \varphi_i(V_i)$, allora $\varphi_i : V_i \to \tilde{V_i}$ è isomorfismo per ogni i, quindi ogni varietà proiettiva è unione di sottovarietà aperte isomorfe a varietà affini.

Definizione 1.36. Sia K un'estensione di k generata aggiungendo a k un numero finito di elementi. Si dice grado di trascendenza di K su k, e si denota con $\mathrm{tr.deg}_k K$, il più piccolo intero n, tale che esistono $x_1, \ldots, x_n \in K$, tali che K è algebrico su $k(x_1, \ldots, x_n)$. In tal caso si dice che K è un campo di funzioni algebriche in n variabili su k.

Proposizione 1.37. *Sia K un campo di funzioni algebriche in una variabile su k, tale che per ogni $t \in K$, tale che K è algebrico su $k(t)$, allora l'estensione $\frac{K}{k(t)}$ è finita e sia $x \in K \setminus k$. Allora:*

1. *K è algebrico su $k(x)$;*
2. *Esiste un elemento $y \in K$ tale che $K = k(x, y)$.*

Dimostrazione. Sia $t \in K$ tale che K è estensione algebrica di $k(t)$; allora esiste un polinomio $F \in k(t)[X]$ tale che $F(t,x) = 0$. In particolare, siccome x non è algebrico su k, perché k è algebricamente chiuso, allora t compare in $F(t,x)$. Allora, moltiplicando gli eventuali denominatori, posso concludere che esiste $G \in k(x)[T]$ tale che $G(x,t) = 0$, da cui t è algebrico su $k(x)$, ma allora $k(x,t)$ è algebrico su $k(x)$ e di conseguenza lo è K.
Siccome K è algebrico su $k(x)$, allora l'estensione è algebrica e finita, quindi ammette elemento primitivo, ovvero esiste $y \in K$ tale che $K = k(x,y)$. □

Se X è una varietà, allora, $k(X)$ è un'estensione di k finitamente generata. Si definisce allora $\dim(X) = \text{tr.deg}_k k(X)$. Una varietà di dimensione 1 è detta curva.

Osservazione 1.38. Una curva secondo questa definizione è irriducibile, mentre una curva piana definita come in 1.4 può essere riducibile.

Proposizione 1.39. *1. Se U è una sottovarietà aperta di X, allora* $\dim(U) = \dim(X)$*;*

2. Se V è la chiusura proiettiva di una varietà affine V', allora $\dim(V) = \dim(V')$*;*

3. Una varietà ha dimensione zero se e solo se è un punto;

Dimostrazione. I primi due punti discendono dal fatto che i campi di funzioni coincidono. Sia ora V una varietà di dimensione zero: per i primi due punti possiamo supporre sia affine; allora siccome $k(V)$ è algebrico su k, ma k è algebricamente chiuso, segue che $k(V) = k$. In particolare $\Gamma(V) = k$, quindi i resti modulo $I(V)$ sono solo costanti, quindi $I(V)$ è generato da n polinomi di primo grado linearmente indipendenti su k, che si annullano in V, ma quindi V è un unico punto in $\mathbb{A}^n$. Il viceversa è ovvio. □

Definizione 1.40. Siano X, Y varietà, due morfismi $f_1 : U_1 \to Y, f_2 : U_2 \to Y$, con $U_1, U_2 \subseteq X$ aperti, si dicono equivalenti se le loro restrizioni a $U_1 \cap U_2$ coincidono.

Siccome $U_1 \cap U_2$ è denso in X, f_1, f_2 sono determinati dalle loro restrizioni su $U_1 \cap U_2$. Questa relazione è effettivamente una relazione di equivalenza fra i morfismi. Una classe di equivalenza di morfismi è una coppia (U, f) dove $U \subseteq X, U = \cup_\alpha U_\alpha, U_\alpha$ dominio di un singolo morfismo, $f : U \to Y$ definita da $P \in U \implies P \in U_\alpha \exists \alpha, f(P) = f_\alpha(P)$, con f_α morfismo di dominio U_α. Siccome morfismi equivalenti coincidono sulle intersezioni dei rispettivi domini, la definizione di f è ben posta. f è detta *mappa razionale* ed U è il suo dominio.

Definizione 1.41. Una mappa razionale $f : U \to Y, U \subseteq X$ è detta *dominante* se $f(U)$ è denso in Y.
Siano A, B anelli locali tali che $A \leq B$; si dice che B *domina* A, se l'ideale massimale di B contiene l'ideale massimale di A.

Proposizione 1.42. *Siano X, Y varietà e sia $F : X \to Y$ una mappa razionale dominante. Siano $U \subseteq X, V \subseteq Y$ aperti tali che $f : U \to V$ è un morfismo che rappresenta F. Allora:*

1. *l'omomorfismo indotto* $\tilde{f} : \Gamma(V) \to \Gamma(U)$ *è iniettivo, quindi si estende unicamente ad un omomorfismo di* $k(V) = k(Y)$ *in* $k(U) = k(X)$*; inoltre è indipendente dalla scelta di* f*, quindi si denota con* $\tilde{F}$*;*

2. *se* P *è nel dominio di* $F, F(P) = Q$*, allora* $\mathcal{O}_P(X)$ *domina* $\tilde{F}(O_Q(Y))$*; viceversa se* $\mathcal{O}_P(X)$ *domina* $\tilde{F}(\mathcal{O}_Q(Y))$ *per oppurtuni* $P \in X, Q \in Y$*, allora* P *è nel dominio di* F *e* $F(P) = Q$*;*

3. *ogni omomorfismo di* $k(Y)$ *in* $k(X)$ *è indotto da un un'unica mappa razionale dominante di* X *in* Y*.*

Dimostrazione. Si veda [1] Capitolo 6, Paragrafo 6. □

Una mappa razionale di X in Y è detta birazionale se esistono degli aperti $U \subseteq X, V \subseteq Y$ ed un isomorfismo $f : U \to V$ che rappresenta F. Due varietà tra cui esiste una mappa birazionale, si dicono birazionalmente equivalenti. Ad esempio ogni varietà è birazionalmente equivalente ad ogni sua sottovarietà aperta.

Proposizione 1.43. *Due varietà sono birazionalmente equivalenti se e solo se i loro campi di funzioni sono isomorfi*

Dimostrazione. Che due varietà birazionalmente equivalenti abbiano campi di funzioni isomorfi è ovvio.
Viceversa, se $\varphi : k(Y) \to k(X)$ è un isomorfismo, allora, per la dimostrazione della Proposizione 1.42 $\varphi(\Gamma(X)) \subseteq \Gamma(Y_b)$ per un opportuno $b \in \Gamma(Y)$ e $\varphi^{-1}(\Gamma(Y)) \subseteq \Gamma(X_d)$ per un opportuno $d \in \Gamma(X)$. Allora φ si restringe ad un isomorfismo tra $\Gamma((Y_b)_{\varphi^{-1}(d)})$ e $\Gamma((X_d)_{\varphi(b)})$, che è generato da un unico morfismo $f : (X_d)_{\varphi(b)} \to (Y_b)_{\varphi^{-1}(d)}$. □

Corollario 1.44. *Ogni curva è birazionalmente equivalente ad una curva piana.*

Dimostrazione. Sia V una curva allora, per la proposizione 1.37, esistono $x, y \in k(V)$ tali che $k(V) = k(x, y)$. Considero perciò il naturale omomorfismo d'anelli da $k[X, Y]$ in $k[x, y]$, e sia I il suo nucleo. In particolare, essendo V irriducibile, I è primo, dunque $V' = V(I) \subseteq \mathbb{A}^2$ è una varietà. Inoltre, $\Gamma(V') = \frac{k[X,Y]}{I}$ è isomorfo a $k[x, y]$, quindi $k(V')$ è isomorfo, a $k(V)$, quindi per la proposizione precedente le due varietà sono birazionalmente equivalenti. Per vedere che V' è una curva è sufficiente osservare che essendo $k(V), k(V')$ isomorfi, $\dim V' = \dim V = 1$. □

Esercizio 1.45. *Siano* C, C' *curve e sia* F *una mappa razionale tra* C *e* C'*. Allora* F *è dominante oppure è costante. Inoltre se* F *è dominante,* $k(C)$ *è un'estensione algebrica finita di* $\tilde{F}(k(C'))$*.*

Dimostrazione. Se F è dominante allora non c'è niente da dimostrare.
Sia quindi F non dominante, e sia $f : U \to V$ morfismo che rappresenta F. Allora, siccome

F non è dominante, $f(U)$ è non vuoto e non è denso in C'. Esiste perciò $\emptyset \neq V \subseteq C'$ aperto tale che $f(U) \cap V = \emptyset \Longrightarrow f(U) \subseteq C' \setminus V$ che è algebrico, quindi è una sottovarietà chiusa di C' e siccome $f(U) \neq \emptyset$ è non banale ovvero è un punto. Ne segue $f(U) = \{P\}$ per un opportuno $P \in C'$. Essendo U denso in C segue la tesi.
Sia ora F dominante allora $\tilde{F}$ è un omomorfismo non banale di campi, dunque $L = \tilde{F}(k(C'))$ è isomorfo a $k(C')$. Sia L che $k(C)$ sono campi di funzione in una variabile su k. Dunque per la proposizione 1.37 esistono $x, y \in k(C), t, s \in L$, nessuno dei quattro in k tali che $k(C) = k(x, y), L = k(t, s)$. Sempre per la Proposizione 1.37 $k(C)$ è estensione algebrica finita di L: basta aggiungere x, y, quando non già presenti. $\square$

1.6 Scoppiamento di punti affini e proiettivi, Trasformazioni quadratiche e Modello non-singolare

Sia C una curva arbitraria e sia P un suo punto. P è detto punto semplice se $\mathcal{O}_P(C)$ è un DVR.
Sia quindi ord_P^C la funzione d'ordine su $k(C)$ associata a $\mathcal{O}_P(C)$. Se ogni punto di C è semplice, la curva è detta *non-singolare*.

Definizione 1.46. Siano $k \leq K$ campi; un sottoanello A di K è detto *anello locale di* K, se A è un anello locale, K è il campo dei quozienti di A e $k \leq A$. Analogamente si dice che A è un *anello di valutazione discreta di* K se A è un anello locale di K ed è un DVR.

Proposizione 1.47. *Sia C una curva proiettiva e sia $K = k(C)$. Sia inoltre L un campo contenente K ed R un DVR di L che non contiene K. Allora esiste un unico punto $P \in C$ tale che R domina $\mathcal{O}_P(C)$.*

Dimostrazione. Si veda [1] Capitolo 7, Paragrafo 1. □

Corollario 1.48. *Sia F una mappa razionale da una curva C ad una curva proiettiva C'; allora i punti semplici di C sono nel dominio di F.*

Dimostrazione. Se F non è domininante allora è costante (Esercizio 1.45), quindi è definita su ogni punto di C.
Sia quindi F dominante e $P \in C$ un punto semplice. Allora, posto $R = \mathcal{O}_P(C), L = \tilde{F}(k(C'))$, per la Proposizione 1.42, se R domina $\tilde{F}(\mathcal{O}_Q(C'))$ per un $Q \in C'$, allora P è nel dominio di F. Ma siccome F è dominante $\tilde{F}$ è isomorfismo tra $k(C')$ ed L, quindi R domina $\tilde{F}(\mathcal{O}_Q(C'))$ per un oppurtuno Q se $L \not\subseteq R$.
Se per assurdo fosse $L \subseteq R \subseteq k(C)$, essendo $\frac{k(C)}{L}$ algebrica finita per l'Esercizio 1.45, segue che R è un campo per l'Esercizio 1.8. Ma questo è assurdo perché un DVR non è un campo. □

Corollario 1.49. *Sia C una curva proiettiva non-singolare, $K = k(C)$. Allora i DVR di K sono tutti e soli gli $\mathcal{O}_P(C)$.*

Dimostrazione. Che gli $\mathcal{O}_P(C)$ siano DVR di K è ovvio. Viceversa se R è un DVR di K, allora per la Proposizione 1.47 R domina un unico $\mathcal{O}_P(C)$. Quindi siamo nella situazione di due DVR con uno che domina l'altro inclusi nello stesso campo, che per entrambi è il campo dei quozienti. Ne segue $R = \mathcal{O}_P(C)$. L'inclusione non banale si dimostra così: $r \in R \subseteq K \implies r = \frac{g_1}{g_2}, g_2 \neq 0, g_1, g_2 \in \mathcal{O}_P(C)$; se g_2 è invertibile in $\mathcal{O}_P(C)$, allora $r \in \mathcal{O}_P(C)$, altrimenti, se g_2 non è ivi invertibile, allora, neanche in R lo è, quindi $r \notin R$, assurdo. □

Con "risolvere le singolarità" di una curva proiettiva C si intende trovare una curva proiettiva non-singolare X ed una mappa birazionale $f : X \to C$. Per fare questo si parte

dalle curve piane, infatti, se si riesce a dimostrare che per ogni curva piana esiste una tale curva non-singolare, allora, siccome tutte le curve proiettive sono birazionalmente equivalenti ad una curva piana, seguirà che ogni curva è birazionalmente equivalente ad una non-singolare.
L'idea fondamentale è quella dello "scoppiamento dei punti singolari di una curva", che ad un livello intuitivo può essere descritto nel seguente modo: sia $C \subseteq \mathbb{P}^2$ una curva e P un suo punto multiplo. Si rimuove il punto P dal piano e lo si sostituisce con una retta proiettiva r. I punti di r corrispondono alle direzioni tangenti a C in P. Tutto questo si può fare in modo che il "piano scoppiato", ovvero $B = \mathbb{P}^2 \setminus \{P\} \cup r$ sia ancora una varietà. In tal modo si può costruire una cuva $C' \subseteq B$ birazionalmente equivalente a C, ma con singolarità "migliori". Studierò prima cosa avviene nel caso affine e poi in quello proiettivo.
Sia $P = (0,0) \in \mathbb{A}^2$ e sia $U = \{(x,y) \in \mathbb{A}^2 : x \neq 0\}$. Considero ora il morfismo $f : U \to \mathbb{A}^1 = k$ definito per ogni $(x,y) \in U$ da $f(x,y) = \frac{y}{x}$. Allora, $G \subseteq \mathbb{A}^1 \times \mathbb{A}^2 = \mathbb{A}^3, G = \{P = (x,y,z) \in \mathbb{A}^3 : y = xz, x \neq 0\}$, è il grafico di f.
Sia ora $B = \{P = (x,y,z) : y = xz\}$; siccome $Y - XZ \in k[X,Y,Z]$ è irriducibile, B è varietà. Sia inoltre $\pi : B \to \mathbb{A}^2$, la restrizione a B della proiezione da $\mathbb{A}^3$ sulle prime due coordinate: π è un morfismo.
Valgono le seguenti:

- $\pi(B) = U \cup \{P\}$;
- $\pi^{-1}(P) = L = \{(0,0,z) : z \in k\}$ e $\pi^{-1}(U) = G$

Ne segue che π è un isomorfismo fra G ed U, da cui G è sottovarietà aperta di B, e B è la chiusura di G in $\mathbb{A}^3$. Infine L è sottovarietà chiusa di B.
Sia $\varphi : \mathbb{A}^2 \to B$ definita per ogni $(x,z) \in \mathbb{A}^2$ da $\varphi(x,z) = (x,xz,z)$: è un isomorfismo con inversa la proiezione sulla prima e terza coordinata. Considero quindi $\psi : \mathbb{A}^2 \to \mathbb{A}^2$, definita come $\psi = \pi \circ \varphi$; è morfismo perché composta di morfismi.
Sia $E = \psi^{-1}(P) = \varphi^{-1}(L) = \{(x,z) \in \mathbb{A}^2 : x = 0\}$. Ne deduco che $\psi : \mathbb{A}^2 \setminus E \to U$ è isomorfismo.
Sia ora C una curva irriducibile del piano affine e sia $C_0 = C \cap U$ una sottovarietà aperta di C. Sia $C_0' = \psi^{-1}(C_0)$ e sia C' la chiusura di C_0' in $\mathbb{A}^2$. Sia infine $f : C' \to C$ la restrizione di ψ a C'. Siccome $C_0 \subseteq U, f$ è un isomorfismo. Dunque tramite $\tilde{f}$ possiamo identificare $k(C) = k(x,y)$ con $k(C') = k(x,z), y = xz$.
Valgono i seguenti fatti:

- Sia $C = V(F), F = F_r + \cdots + F_n, F_i$ polinomio omogeneo di grado i in $k[X,Y]$, e siano $r = m_P(C), n = \deg(C)$. Allora, $C' = V(F'), F'(X,Z) = F_r(1,Z) + XF_{r+1}(1,Z) + \cdots + X^{n-r}F_n(1,Z)$.

Dimostrazione. $F(X,XZ)=\sum_{i=r}^{n}X^iF_i(1,Z)=X^rF'(X,Z)$. Ma siccome $F_r(1,Z)\neq 0$, allora, X non divide F'. Se per assurdo $F'=GH$, tali che

$$F=X^rF'(X,Z)=X^rF'\left(X,\frac{Y}{X}\right)=X^rG\left(X,\frac{Y}{X}\right)H\left(X,\frac{Y}{X}\right)$$

ma allora F è riducibile, che è assurdo. Ne segue che anche F' è irriducibile, ne segue che $V(F')$ è un chiuso che contiene C_0'. Quindi $C'\subseteq V(F')$.
Viceversa

$$F'(P)=0\Longrightarrow F(\psi(P))=0\Longrightarrow\psi(P)\in C\Longrightarrow P\in C'$$

□

- Supposto che la retta X non sia tangente a C in P, posso supporre che $F_r(X,Y)=\prod_{i=1}^{s}(Y-\alpha_iX)^{r_i}$. Allora $f^{-1}(P)=\{P_1,\dots,P_s\}$, con $P_i=(0,\alpha_i)$ e vale che $m_{P_i}(C')\leq I(P,C\cap E)=r_i$. In particolare, se P è un punto multiplo ordinario, P_i è un punto semplice di C' e $\mathrm{ord}_{P_i}^{C'}(x)=1$.

  Dimostrazione. Chiaramente:

  $$f^{-1}(P)=C'\cap E=\{(0,\alpha):F_r(1,\alpha)=0\}.$$

  Inoltre $m_{P_i}(C)\leq I(P_i,F'\cap X)=I(P_i,\prod_{i=1}^{r}(Z-\alpha_i)\cap X)=r_i$. La parte di enunciato riguardo l'ordine in P_i della funzione x è ovvia. □

- Esiste un intorno affine W di P in C tale che $W'=f^{-1}(W)$ sia una sottovarietà aperta affine di C'. Inoltre $\Gamma(W')$ è un modulo finitamente generato su $\Gamma(W)$ e $x^{r-1}\Gamma(W')\subseteq\Gamma(W)$.

  Dimostrazione. Sia $F(X,Y)=\sum_{i+\geq r}a_{ij}X^iY^j$ e sia $H(Y)=\sum_{j\geq r}a_{0j}Y^{j-r}$, ovvero $F(X,Y)=Y^rH(Y)+XG(X,Y)$. Sia infine h l'immagine in $\Gamma(C)$ di H.
  Chiaramente $H(0)\neq 0$, quindi $W=C_h=\{Q\in C:h(Q)\neq 0\}$ è un intorno aperto affine di P in C. Dimostro che $W=(C_h\cap U)\cup\{P\}$; un'inclusione ($\supseteq$) è ovvia.
  Viceversa,

  $$Q\in W\Longrightarrow F(Q)=0,H(Q)\neq 0\Longrightarrow x_Q=0=y_Q\text{ oppure}$$
  $$x_Q\neq 0\Longrightarrow Q\in(C_h\cap U)\cup\{P\}$$

  Infine osservo che

  $$F'(X,Z)=\sum_{i+j\geq r}a_{ij}X^{i+j-r}Z^j=\sum_{i<r}a_{ij}X^{i+j-r}Z^{r-i}+\sum_{i\geq r}a_{ij}X^{i-r}Y^j$$

Ma questo prova, valutando in (x, z), che z^r è una combinazione della forma $\sum_i b_i z^{r-i}$, da cui $\Gamma(W')$ è un modulo finitamente generato su $\Gamma(W)$. Inoltre per $i \leq r-1$:

$$x^{r-1} z^i = x^{r-1} \frac{y^i}{x^i} \in \Gamma(W)$$

□

Siano ora $P_1, \ldots, P_t \in \mathbb{P}^2$, e per semplicità nella trattazione suppongo che $P_i \in U_3$ per ogni i, quindi $P_i = [a_{i1}, a_{i2}, 1]$. Sia $U = \mathbb{P}^2 \setminus \{P_1, \ldots, P_t\}$.
Definisco i morfismi $f_i : U \to \mathbb{P}^1, f_i(X_1, X_2, X_3) = [X_1 - a_{i1}X_3, X_2 - a_{i2}X_3]$ e sia $f = (f_1, \ldots, f_t) : U \to \mathbb{P}^1 \times \cdots \times \mathbb{P}^1$ la mappa prodotto. Sia infine $G \subseteq U \times \mathbb{P}^1 \times \cdots \times \mathbb{P}^1$ il grafico di f.
Fissate quindi le coordinate omogenee X_1, X_2, X_3 per $\mathbb{P}^2$ e Y_{i1}, Y_{i2} per la i-esima copia di $\mathbb{P}^1$, considero $B = V(Y_{i2}(X_1 - a_{i1}X_3) - Y_{i1}(X_2 - a_{i2}X_3) : i \in \{1, \ldots, t\})$.
Chiaramente $G \subseteq B$. Sia $\pi : B \to \mathbb{P}^2$ la restrizione della proiezione e sia, per ogni i, $E_i = \pi^{-1}(P_i)$. Valgono i seguenti fatti:

1. $E_i = \{P_i\} \times \{f_1(P_i)\} \times \cdots \times \mathbb{P}^1 \times \cdots \times \{f_t(P_i)\}$, con $\mathbb{P}^1$ nell'i-esima posizione; quindi E_i è isomorfo a $\mathbb{P}^1$.

2. $B \setminus \cup_{i=1}^t E_i = B \cap (U \times \mathbb{P}^1 \times \cdots \times \mathbb{P}^1) = G$, perciò π si restringe ad un isomorfismo tra $B \setminus \cup_{i=1}^t E_i$ e U.

3. Se T è un cambio di coordinate proiettive di $\mathbb{P}^2$, con $T(P_i) = P_i'$, e le mappe $f_i' : \mathbb{P}^2 \setminus \{P_1', \ldots, P_t'\} \to \mathbb{P}^1$ sono definite come le f_i, ma con i P_i' al posto dei P_i, allora esiste un unico cambio di coordinate proiettive T_i di $\mathbb{P}^1$ tale che $T_i \circ f_i = f_i' \circ T$, dunque $(T_1, \ldots, T_t) \circ f = f' \circ T$. Infine $(T, T_1, \ldots, T_t)$ mappa isomorficamente G, B, E_i nei corrispondenti G', B', E_i' definiti a partire da f'.

4. Se T_i è un cambio di coordinate in $\mathbb{P}^1$ per un i fissato, esiste un cambio di coordinate T di $\mathbb{P}^2$, tale che $T(P_i) = P_i$ e $T_i \circ f_i = f_i \circ T$.

5. Siano $i \in \{1, \ldots, t\}, Q \in E_i$ fissati; per gli ultimi due punti posso supporre che $P_1 = [0, 0, 1], Q = [\lambda, 1], \exists \lambda \in k$. Sia $\varphi_3^{-1} : \mathbb{A}^2 \to U_3$ il morfismo canonico. Siano $V = U_3 \setminus \{P_j : j \neq i\}, W = (\varphi_3^{-1})^{-1}(V), \psi$ la mappa definita nel caso affine e $W' = \psi^{-1}(W)$. A questo punto considero $\varphi : W' \to \mathbb{P}^2 \times \mathbb{P}^1 \times \cdots \times \mathbb{P}^1$ definita da

$$\varphi(x, z) = ((x, xz, 1), f_1(x, xz, 1), \ldots, (z, 1), \ldots, f_t(x, xz, 1))$$

con $(z, 1)$ in i-esima posizione. φ è un morfismo, ed è tale che $\pi \circ \varphi = \varphi_3 \circ \psi$. Posto $V' = \varphi(W') = B \setminus (\cup_{j \neq i} E_j \cup V(X_3) \cup V(Y_{i2}))$, V' è intorno aperto di Q in B.

6. B è la chiusura di G: se S è un chiuso che contiene G, allora $\varphi^{-1}(S)$ è un chiuso di W' che contiene $\varphi^{-1}(G) = W' \setminus V(X)$, che è aperto quindi denso, ne segue che $\varphi^{-1}(S) = W'$, da cui $Q \in S$. Data l'arbitrarietà di Q in $B \setminus G$, segue che B è la chiusura di G.

7. Il morfismo definito su $\mathbb{P}^2 \times \mathbb{P}^1 \times \cdots \times \mathbb{P}^1 \setminus V(X_3 Y_{i2})$ verso $\mathbb{A}^2$ che mappa un elemento del suo dominio in $(\frac{x_1}{x_3}, \frac{y_{i1}}{y_{i2}})$ è, se ristretto a V', l'inversa di φ. Allora abbiamo il seguente diagramma commutativo:

$$\begin{array}{ccccccc} \mathbb{A}^2 & \hookleftarrow & W' & \xrightarrow{\varphi} & V' & \hookrightarrow & B \\ \downarrow{\scriptstyle \psi} & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \pi} \\ \mathbb{A}^2 & \hookleftarrow & W & \xrightarrow{\varphi_3} & V & \hookrightarrow & \mathbb{P}^2 \end{array}$$

   Quindi π, attorno a Q si comporta analogamente alla mappa ψ, dunque valgono per π tutte le proprietà di ψ.

8. Sia C una curva irriducibile in $\mathbb{P}^2$. Sia $C_0 = C \cap U, C_0' = \pi^{-1}(C_0) \subseteq G$ e C' la chiusura di C_0' in B. Allora $f : C' \to C$ si restringe ad un isomorfismo tra C_0' e C_0. Per quanto visto nel punto precedente, tale isomorfismo ha la stessa forma del caso affine.

Vale quindi la seguente:

Proposizione 1.50. *Sia C una curva proiettiva piana irriducibile, e suppongo che tutti i suoi punti multipli, siano ordinari. Allora esiste una curva non-singolare C' ed una mappa birazionale da C' a C.*

Dimostrazione. Si veda [1] Capitolo 7, Paragrafo 3. □

Per quanto visto quindi, se C è una curva piana proiettiva i cui punti multipli sono ordinari, allora C è birazionalmente equivalente ad una curva non singolare. Adesso dimostro che ogni curva piana è birazionalmente equivalente ad una curva i cui punti multipli sono ordinari.
Siano $P = [0,0,1], P' = [0,1,0], P'' = [1,0,0] \in \mathbb{P}^2$; tali punti sono detti fondamentali. Siano $L = V(Z), L' = V(Y), L'' = V(X)$ e queste rette sono dette eccezionali. Sia infine $U = \mathbb{P}^2 \setminus V(XYZ)$.
Definisco $Q : \mathbb{P}^2 \setminus \{P, P', P''\} \to U \cup \{P, P', P''\}, Q(x,y,z) = [yz, xz, xy]$. Q è un morfismo ed è tale che $Q^{-1}(P) = L \setminus \{P', P''\}$ (e simmetricamente per P', P'').
Osservo ora che se $[x,y,z] \in U$:

$$Q^2(x,y,z) = Q(yz, xz, xy) = [xxyz, yxyz, zxyz] = [x,y,z]$$

Quindi su $U, Q = Q^{-1}$, quindi Q è un isomorfismo di U con se stesso. In particolare induce una mappa birazionale di $\mathbb{P}^2$ con se stesso. La mappa Q è detta trasformazione quadratica

standard.
Sia C una curva irriducibile in $\mathbb{P}^2$, e suppongo non sia una retta eccezionale. Allora $C \cap U$ è una curva chiusa in U. Sia C' la chiusura di $Q(C \cap U) = Q^{-1}(C \cap U)$ in $\mathbb{P}^2$; Q si restringe ad un morfismo tra $C' \setminus \{P, P', P''\}$ e C. Inoltre $(C')' = C$ perché $Q^2 = \mathrm{id}_U$.
Sia $F \in k[X, Y, Z]$, tale che $C = V(F), n = \deg(F)$ definisco la trasformata algebrica di F come: $F^Q = F(YZ, XZ, XY)$. Tale polinomio è omogeneo di grado $2n$.
Valgono i seguenti fatti:

1. Se $m_P(C) = r$, allora, Z^r è la più alta potenza di Z che divide F^Q, e simmetricamente in P', P''.

Se $F^Q = X^{r''}Y^{r'}Z^rF'$, il polinomio omogeneo F' è detto trasformata propria di F.

2. $\deg(F') = 2n - r - r' - r'', (F')' = F, V(F') = C'$.
3. $m_P(C') = n - r' - r''$, e simmetricamente per P', P''.

Suppongo ora che nessuna retta eccezionale sia tangente a C in un punto fondamentale. Una tale curva si dice essere in buona posizione.

4. Se C è in buona posizione, allora, anche C' lo è.

Sia C in buona posizione e che $P \in C$; sia $C_0 = (C \cap U) \cup \{P\}, C_0' = C' \setminus V(XY)$. Allora $f : C_0' \to C_0$ è la restrizione di Q Considero ora il polinomio affinizzato $F_* = F(X, Y, 1)$, e la curva affinizzata $C_* = V(F_*) \subseteq \mathbb{A}^2$; definisco $(F_*)' = F(X, XZ, 1)X^{-r}C_*' = V(F_*') \subseteq \mathbb{A}^2$ ed $f_* : C_*' \to C_*, f_*(x, z) = (x, xz)$.

5. Esiste un intorno W di $(0, 0)$ in C_* e isomorfismi $\varphi : W \to C_0, \varphi' : W' = f_*^{-1}(W) \to C_0'$ tali che $\varphi \circ f_* = \varphi' \circ f$.
6. Se C è in buona posizione e $P_1, \ldots, P_s$ sono punti non-fondamentali su $C' \cap L$, allora, $m_{P_i}(C') \leq I(P_i, C' \cap L)$.

Si dice che la curva C è in posizione eccellente se interseca L trasversalmente in n punti non-fondamentali distinti, ed interseca trasversalmente L', L'' ciascuna in $n - r$ punti non-fondamentali distinti.

7. Se C è in posizione eccellente, allora gli unici punti multipli di C' sono quelli in $C' \cap U$ che corrispondono a quelli in $C \cap U$ e questa corrispondenza rispetta la molteplicità dei punti e se questi sono ordinari o meno; P, P', P'' che sono ordinari di molteplicità $n, n - r, n - r$ rispettivamente e dei punti $P_1, \ldots, P_s$ non fondamentali su $C' \cap L$, di molteplicità tali che $m_{P_i}(C') \leq I(P_i, C' \cap L), \sum_{i=1}^{s} I(P_i, C' \cap L) = r$.

Per C curva piana proiettiva irriducibile, di grado n si definisce $g_*(C) = \frac{(n-1)(n-2)}{2} - \sum_{P\in C} \frac{r_P(r_P-1)}{2}$, dove $r_P = m_P(C)$.

8. Se C è in posizione eccellente allora, $g_*(C') = g_*(C) - \sum_{i=1}^{s} \frac{r_i(r_i-1)}{2}$, dove $r_i = m_{P_i}(C')$ e $P_1, \ldots, P_s$ sono i punti non fondamentali di $C' \cap L$.

Abbandono ora le notazioni per punti fondamentali e rette eccezionali che ho usato fino ad ora.

Lemma 1.51. *Sia F una curva piana proiettiva irriducibile e P un suo punto, allora esiste un cambio di coordinate T, tale che F^T è in posizione eccellente e $T(0,0,1) = P$.*

Dimostrazione. Si veda [1] Capitolo 7, Paragrafo 4. □

Se T è un cambio di coordinate omogenee, allora, $Q \circ T$ è detta trasforazione quadratica e $(F^T)'$ è detto trasformata quadratica di F. Se F^T è in posizione eccellente e $T(0,0,1) = P$, allora si dice che la trasformata è centrata in P.
Se $F = F_1, \ldots, F_n = G$ sono curve e F_i è trasformata quadratica di F_{i-1}, allora, si dice che F è trasformata in G da una sequenza finita di trasformazioni quadratiche.

Proposizione 1.52. *Tramite un numero finito di trasformazioni quadratiche, ogni curva piana proiettiva irriducibile può essere trasformata in una curva i cui punti multipli sono ordinari.*

Dimostrazione. Si veda [1] Capitolo 7, Paragrafo 4. □

Teorema 1.53. *Sia C una curva proiettiva. Allora esiste una curva proiettiva non-singolare X ed una mappa birazionale f da X a C. Se $f' : X' \to C$ sono un'altra mappa birazionale ed un altra curva non-singolare, allora esiste un unico isomorfismo $g : X \to X'$ tale che $f' \circ g = f$.*

Dimostrazione. Si veda [1] Capitolo 7, Paragrafo 5. □

Corollario 1.54. *Esiste un corrispondenza biiettiva fra curve proiettive non-singolari e campi di funzioni in una variabile. Se X, X' sono due tali curve, i morfismi dominanti da X a X' corrispondono agli omomorfismi da $k(X')$ a $k(X)$.*

Sia C una curva proiettiva. $f : X \to C$ come nel Teorema 1.53. Si dice che X è il modello non-singolare di C o di $K = k(C)$. Si identifica $k(X)$ con $k(C)$ tramite $\tilde{f}$. I punti di X sono detti posti di C ed un posto $Q \in X$ si dice centrato in $P \in C$ se $f(Q) = P$.
Suppongo ora che C sia piana, $Q \in X, f(Q) = P \in C$. Per ogni altra curva piana G, eventualmente riducibile, sia $G_* \in \mathcal{O}_P(\mathbb{P}^2)$ e sia g l'immagine di G_* in $\mathcal{O}_P(C) \subseteq k(C) = k(X)$. Definisco $\mathrm{ord}_Q(G) = \mathrm{ord}_Q(g)$.

Proposizione 1.55. *Sia C una curva piana proiettiva irriducibile, $P \in C, f : X \to C$ come sopra. Sia G un'altra curva piana, eventualmente riducibile. Allora: $I(P, C \cap G) = \sum_{Q \in f^{-1}(P)} \mathrm{ord}_Q(G)$.*

Dimostrazione. Si veda [1] Capitolo 7, Paragrafo 5. □

Lemma 1.56. *Se P è un punto multiplo ordinario su C di molteplicità r e sia $f^{-1}(P) = \{P_1, \ldots, P_r\}$. Se $z \in k(C)$ e $\mathrm{ord}_{P_i}(z) \geq r - 1$, allora $z \in \mathcal{O}_P(C)$.*

Dimostrazione. Si veda [1] Capitolo 7, Paragrafo 5. □

Proposizione 1.57. *Siano F una curva piana proiettiva irriducibile e P un suo punto multiplo ordinario di molteplicità r e siano $P_1, \ldots, P_r$ i posti di F centrati in P. Siano inoltre G, H altre due curve piane, eventualmente riducibili. Allora le condizioni di Noether sono soddisfatte in P rispetto a F, G, H se e solo se $\forall i \in \{1, \ldots, r\}\, \mathrm{ord}_{P_i}(H) \geq \mathrm{ord}_{P_i}(G) + r - 1$.*

Dimostrazione. Si veda [1] Capitolo 7, Paragrafo 5. □

Capitolo 2

Divisori e lo Spazio L(D)

Per tutto il capitolo C sarà una curva proiettiva irriducibile(tranne dove specificato). X il suo modello non singolare e $f : X \to C$ la mappa birazionale. Inoltre $K = k(C) = k(X)$ è il campo delle funzioni razionali su C. I punti di X sono detti posti di C e ord_P la funzione ordine su K.

2.1 Divisori

Un *divisore* su X è una somma formale $\sum_{P\in X} n_P P$, dove $P \in X.n_P \in \mathbb{Z}$ e $n_P = 0$ per tutti tranne un numero finito di elementi di X. Analogamente, si definisce l'insieme dei divisori su X come il gruppo abeliano libero generato da X e si denota con $\mathrm{Div}(X)$.
Su $\mathrm{Div}(X)$ è definita la mappa $\deg : \mathrm{Div}(X) \to \mathbb{Z}$, che associa ad un divisore $D = \sum_{P\in X} n_P P, \deg(D) = \sum_{P\in X} n_P$. L'immagine di un divisore D è detta *grado del divisore*. La mappa grado è un omomorfismo di gruppi.
Su $\mathrm{Div}(X)$ è definito un ordine parziale $\succ$, definito come: $D = \sum_{P\in X} n_P P, D' = \sum_{P\in X} m_P P, D \succ D' \iff n_P \geq m_P \, \forall P \in X$. Un divisore D è detto *effettivo* se $D \succ 0$.
Sia C una curva piana proiettiva irriducibile di grado n e sia G un'altra curva di grado m, eventualmente riducibile, che non contiene C come componente, allora è ben definito il divisore di G, come $\mathrm{div}(G) = \sum_{P\in X} \mathrm{ord}_P(G)P$. Per la Proposizione 1.55, e per il Teorema di Bezout, $\deg(\mathrm{div}(G)) = mn$.
Sia ora $z \in K, z \neq 0$. Allora è ben definito il divisore di z come $\mathrm{div}(z) = \sum_{P\in X} \mathrm{ord}_P(z)P$, siccome z ha un numero finito di zeri e poli, allora $\mathrm{div}(z)$ è ben definito.
Siano inoltre, $(z)_0 = \sum_{\mathrm{ord}_P(z)>0} \mathrm{ord}_P(z)P$ e $(z)_\infty = \sum_{\mathrm{ord}_P(z)<0} -\mathrm{ord}_P(z)P$. Allora $\mathrm{div}(z) = (z)_0 - (z)_\infty$. Inoltre $\mathrm{div}(zz') = \mathrm{div}(z) + \mathrm{div}(z'), \mathrm{div}(z^{-1}) = -\mathrm{div}(z)$. Ovvero $\mathrm{div} : K \setminus \{0\} \to \mathrm{Div}(X)$ è un omomorfismo di gruppi.

Proposizione 2.1. *Se $z \in K$ è non nullo allora* $\deg(\mathrm{div}(z)) = 0$.

Dimostrazione. Se $z \in K \setminus \{0\}$, allora esistono degli omogenei dello stesso grado $g, h \in \Gamma_h(C)$ tali che $z = \frac{g}{h}$, ma allora g, h sono immagini di polinomi omogenei dello stesso grado $G, H \in k[X, Y, Z]$, dunque $\mathrm{div}(z) = \mathrm{div}(G) - \mathrm{div}(H)$, da cui segue la tesi perché avendo G, H lo stesso grado anche i loro divisori hanno grado uguale. □

Corollario 2.2. *Sia $z \in K, z \neq 0$. Le seguenti affermazioni sono equivalenti:*

a $\mathrm{div}(z) \succ 0$*;*

b $z \in k$*;*

c $\mathrm{div}(z) = 0$.

Corollario 2.3. *Siano $z, z' \in K$ entrambi non-nulli. Allora* $\mathrm{div}(z) = \mathrm{div}(z') \iff z = \lambda z'$ *per un opportuno $\lambda \in k$ non nullo.*

Definizione 2.4. Siano $D, D' \in \mathrm{Div}(X)$. D, D' si dicono *linearmente equivalenti*, e si scrive $D \equiv D'$ se e solo se esiste $z \in K$ tale che $D = D' + \mathrm{div}(z)$.

Proposizione 2.5. *Valgono i seguenti fatti:*

1. *La relazione di equivalenza lineare è un'equivalenza su* $\mathrm{Div}(X)$*;*
2. $D \equiv 0 \iff D = \mathrm{div}(z)$ *per un'opportuna $z \in K$;*
3. *Se $D \equiv D'$ allora,* $\deg(D) = \deg(D')$*;*
4. $D \equiv D', E \equiv E' \Longrightarrow D + E \equiv D' + E'$*;*
5. *Se C è una curva piana, allora $D \equiv D'$ se e solo se esistono due curve G, G' dello stesso grado tali che $D + \mathrm{div}(G) = D' + \mathrm{div}(G')$*

Dimostrazione. Che la lineare equivalenza sia un'equivalenza è ovvio. Sia $D \in \mathrm{Div}(X)$ tale che $D \equiv 0$, allora, esiste $z \in K$ tale che $D = \mathrm{div}(z)$. Viceversa, se $D = \mathrm{div}(z)$ per un'opportuna $z \in K$, allora $D \equiv 0$.
Se $D \equiv D'$, allora, esiste $z \in K$ tale che $D = D' + \mathrm{div}(z)$; calcolando il grado: $\deg(D) = \deg(D') + \deg(\mathrm{div}(z)) = \deg(D')$.
Siano $z, w \in K$, tali che $D = D' + \mathrm{div}(z), E = E' + \mathrm{div}(w)$, allora, $D + E = D' + E' + \mathrm{div}(zw)$.
Sia ora C piana, e siano $D = D' + \mathrm{div}(z)$, ma $z = \frac{G'}{G}$, con G, G' polinomi omogenei dello stesso grado, dunque $D + \mathrm{div}((G)) = D' + \mathrm{div}(G')$. Il viceversa è analogo. □

Sia ora il caso di una curva piana proiettiva irriducibile, i cui punti multipli sono tutti ordinari; per ciascun posto Q della curva, definisco $r_Q = m_{f(Q)}(C)$. Sia il divisore $E = \sum_{Q \in X}(r_Q - 1)Q$. E è un divisore effettivo di grado $\sum_{Q \in X} r_Q(r_Q - 1)$.
Una curva piana proiettiva G tale che $\mathrm{div}(G) \succ E$, è detta *aggiunta* di C.

Teorema 2.6 (del Residuo)**.** *Siano C, E come sopra. Siano D, D' divisori effettivi di X linearmente equivalenti. Sia G una aggiunta di C di grado m tale che* $\operatorname{div}(G) = D + E + A$*, per un opportuno divisore effettivo A. Allora esiste un'altra aggiunta G' di C di grado m tale che* $\operatorname{div}(G') = D' + E + A$*.*

Dimostrazione. Per la Proposizione 2.5 esistono H, H' curve dello stesso grado tali che $D + \operatorname{div}(H) = D' + \operatorname{div}(H')$. Allora:

$$\operatorname{div}(GH) = D' + \operatorname{div}(H') + E + A \succ \operatorname{div}(H') + E$$

Per la Proposizione 1.57 le condizioni di Noether rispetto a F, H', GH sono soddisfatte in ogni $P \in X$, quindi, esistono $F', G' \in k[X, Y, Z]$ omogenei tali che $GH = F'F + G'H'$. Per il Teorema di Noether $\deg(G') = m$. Inoltre:

$$\operatorname{div}(G') = \operatorname{div}(GH) - \operatorname{div}(H') = D' + E + A$$

□

2.2 Lo spazio vettoriale L(D)

Sia $D = \sum_{P \in X} n_P P$ un divisore di X fissato, allora considero l'insieme $L(D) = \{f \in K : \mathrm{ord}_P(f) \geq -n_P \, \forall P \in X\} \cup \{0\} = \{f \in K : \mathrm{div}(f) + D \succ 0\} \cup \{0\}$.
Con le usuali operazioni di somma e prodotto per scalare è uno spazio vettoriale sul campo k. Denoto la dimensione di $L(D)$ con $\ell(D)$.

Proposizione 2.7. *Valgono i seguenti fatti:*

1. *Se $D \prec D'$, allora $L(D)$ è sottospazio di $L(D')$ e $\dim_k \frac{L(D')}{L(D)} \leq \deg(D' - D)$;*
2. *$L(0) = k, L(D) = 0$ se $\deg(D) < 0$;*
3. *$L(D)$ è di dimensione finita per ogni D e se $\deg(D) \geq 0$, allora $\ell(D) \leq \deg(D) + 1$;*
4. *Se $D \equiv D'$, allora $\ell(D) = \ell(D')$.*

Dimostrazione. Siccome $D' = D + P_1 + \ldots + P_s$, è sufficiente dimostrare il primo enunciato per $D' = D + P$.
Sia $t \in \mathcal{O}_P(X)$ un parametro uniformizzante e sia $r = n_P$, il coefficiente in D di P.
Definisco $\varphi : L(D + P) \to k$, come $\varphi(f) = (t^{r+1} f)(P)$; chiaramente φ è lineare, e $\ker(\varphi) = L(D)$, dunque $\bar{\varphi} : \frac{L(D+P)}{L(D)} \to k$ è iniettiva, dunque $\dim_k \frac{L(D+P)}{L(D)} \leq 1$.
$L(0) = \{f \in K : \mathrm{div}(f) \succ 0\} = k$; Sia D di grado negativo, allora, una funzione in $L(D)$ ha $\mathrm{div}(f) \succ 0$ e ha degli zeri, dunque $f = 0$.
Sia D fissato e sia $\deg(D) = n$. Allora $D' = D - (n+1)P$, per $P \in X$ fissato è tale che $L(D') = 0$, da cui $\dim_k L(D) = \dim_k \frac{L(D)}{L(D')} \leq n + 1$.
Sia $g \in K$, tale che $D = D' + \mathrm{div}(g)$, allora la mappa $\psi : L(D) \to L(D')$ definita come $\psi(f) = fg$ è lineare ed è un isomorfismo. Segue $\ell(D) = \ell(D')$. □

Sia ora $S \subseteq X$ arbitrario, allora si definisce $L^S(D) = \{f \in K : \mathrm{ord}_P(f) \geq -n_P \, \forall P \in S\}$. e $\deg^S(D) = \sum_{P \in S} n_P$.

Lemma 2.8. *Se $D \prec D'$, allora $L^S(D) \subseteq L^S(D')$. Inoltre, se S è finito, $\dim_k \frac{L^S(D)}{L^S(D')} = \deg^S(D)$.*

Dimostrazione. Analoga a quella nel caso $S = X$. □

Proposizione 2.9. *Sia $x \in K \setminus k, (x)_0$ il suo divisore degli zeri e sia $n = [K : k(x)]$. Allora:*

1. *$(x)_0$ è un divisore effettivo di grado n;*
2. *Esiste una costante τ tale che $\ell(r(x)_0) \geq rn - \tau$ per ogni r.*

Dimostrazione. Sia $Z = (x)_0 = \sum_{P \in X} n_P P$ e sia $m = \deg(Z)$. Dimostro che $m \leq n$.
Sia $S = \{P \in X : n_P > 0\}$. Siano $v_1, \ldots, v_m \in L^S(0)$ tali che $\bar{v_1}, \ldots, \bar{v_m}$ siano una base per $\frac{L^S(0)}{L^S(-Z)}$. $v_1, \ldots, v_m$ sono linearmente indipendenti su $k(x)$.
Sia per assurdo una combinazione $\sum_{i=1}^m g_i v_i = 0, g_i = \lambda_i + x h_i, x h_i \in L^S(-Z) \, \forall i$, con i λ_i non tutti nulli (posso sempre ricondurmi a questa forma a meno di moltiplicare per denominatori e potenze di x).
Ma allora $\sum_{i=1}^m \lambda_i v_i = -x \sum_{i=1}^m h_i v_i \in L^S(-Z)$, quindi $\sum_{i=1}^m \lambda_i \bar{v_i} = 0$, con i λ_i non tutti nulli. Assurdo. Ciò prova che $m \leq n$.
Dimostro ora la disuguaglianza in 2.
Sia $w_1, \ldots, w_n$ una base di K su $k(x)$. Allora per ogni i esiste un polinomio $F_i \in k(x)[T]$ tale che $F_i(w_i) = 0$; sia a_{ij} il j-esimo coefficiente di F_i. Allora $a_{ij} \in k[x^{-1}]$.
Allora $\mathrm{ord}_P(a_{ij}) \geq 0$ se $P \notin S$. Inoltre, se $\mathrm{ord}_P(w_i) < 0, P \notin S$, allora $\mathrm{ord}_P(w_i) < \mathrm{ord}_P(a_{ij} w_i^{n_i - j})$, ma questo è in contraddizione col fatto che $F_i(w_i) = 0$.
Allora esiste $t > 0$, tale che $\mathrm{div}(w_i) + tZ \succ 0, i \in \{1, \ldots, n\}$. Allora, $w_i x^{-j} \in L^S((r + t)Z)$, $\forall i \in \{1, \ldots, n\}, j \in \{0, \ldots, r\}$.
Siccome i w_i sono indipendenti su $k(x)$ e $1, \ldots, x^{-r}$ lo sono su k, $\{w_i x^{-j} : i \in \{1, \ldots, n\}, j \in \{0, \ldots, r\}\}$ è un insieme indipendente su k, dunque $\ell((r+t)Z) \geq n(r+1)$, ma d'altro canto $\ell((r+t)Z) = \ell(rZ) + \dim_k \frac{L((r+t)Z)}{L^S(Z)} \leq \ell(rZ) + tm$.
Riordinando, segue la tesi in 2. Osservo ora però che:

$$rn - \tau \leq \ell(rZ) \leq rm + 1 \Longrightarrow \ell(rZ) \leq r(m-n) + c$$

E la quantità a secondo membro è non-negativa per ogni $r \in \mathbb{N}$, ne segue $n \leq m$. □

2.3 Il Teorema di Riemann

Teorema 2.10 (di Riemann)**.** *Esiste una costante g tale che $\ell(D) \geq \deg(D) + 1 - g$, per ogni divisore D.*

Dimostrazione. Sia, per ogni $D, S(D) = \deg(D) + 1 - \ell(D)$; cerco $g \geq S(D)$ per ogni D. Siccome $S(0) = 0, g$, se esiste, è non-negativo. Inoltre dalle proprietà della lineare equivalenza, $D \equiv D' \Longrightarrow S(D) = S(D')$. Infine se $D \prec D'$, allora $\ell(D') - \ell(D) \leq \deg(D') - \deg(D) \Longrightarrow S(D) \leq S(D')$.
Siano $x \in K \setminus k, Z = (x)_0$ e τ il più piccolo intero che soddisfa la relazione della Proposizione 2.9. Siccome dalla stessa Proposizione, $S(rZ) \leq \tau + 1 \, \forall r$, allora, definitivamente deve essere $S(rZ) = \tau + 1$. Pongo $g = \tau + 1$.
Per completare la dimostrazione, è sufficiente dimostrare che per ogni divisore D, esiste D' linearmente equivalente a D tale che $D' \prec rZ$, definitivamente in r: siano $Z = \sum_{P \in X} n_P P, D = \sum_{P \in X} m_P P$, e cerco f razionale tale che $m_P - \mathrm{ord}_P(f) \leq n_P, \forall P \in X$.
Sia $y = x^{-1}$ e considero l'insieme $T = \{P \in X : m_P > 0 \text{ e } \mathrm{ord}_P(y) \geq 0\}$. Definisco $f = \prod_{P \in T} (y - y(P))^{m_P}$.
Se $\mathrm{ord}_P(y) \geq 0$, allora $m_P - \mathrm{ord}_P(f) \leq 0 \leq n_P$; altrimenti, se $\mathrm{ord}_P(y) < 0$, per r sufficientemente grande $m_P - \mathrm{ord}_P(f) \leq r n_P$, da cui la tesi. □

Definizione 2.11. Il più piccolo g che soddisfa la relazione del teorema di Riemann è detto il genere della curva C

Corollario 2.12. *Se $\ell(D_0) = \deg(D_0) + 1 - g$ e $D \equiv D' \succ D_0$, allora $\ell(D) = \deg(D) + 1 - g$.*

Corollario 2.13. *Sia $x \in K \setminus k$, allora $g = \deg(r(x)_0) + 1 - \ell(r(x)_0)$ per r sufficientemente grande.*

Corollario 2.14. *Esiste un intero N tale che ogni divisore di grado superiore ad N è tale che $\ell(D) = \deg(d) + 1 - g$.*

Dimostrazione. Sia D_0 tale che $\ell(D_0) = \deg(D_0) + 1 - g$ e sia $N = \deg(D_0) + g$. Allora $\deg(D - D_0) + 1 - g > 0$, da cui $\ell(D - D_0) > 0$.
Esiste f razionale tale che $D - D_0 + \mathrm{div}(f) \succ 0 \Longrightarrow D \equiv D + \mathrm{div}(f) \succ D_0$, quindi si conclude per il primo corollario. □

Proposizione 2.15. *Sia C una curva piana proiettiva i cui punti multipli sono tutti ordinari. Siano n il grado di C, e $r_P = m_P(C)$. Allora il genere di C è $g = \frac{(n-1)(n-2)}{2} - \sum_{P \in C} \frac{r_P(r_P - 1)}{2}$.*

Dimostrazione. Si veda [1] Capitolo 8, Paragrafo 3. □

Corollario 2.16. *Sia C una curva piana proiettiva. Allora $g \leq \frac{(n-1)(n-2)}{2} - \sum_{P \in C} \frac{r_P(r_P - 1)}{2}$.*

Dimostrazione. Si veda [1] Capitolo 8, Paragrafo 3. □

Considero ora di nuovo C piana proiettiva i cui punti multipli sono ordinari. Siano $P_1, \ldots, P_n$ i punti di intersezione tra C e la retta Z. Pongo $E_m = m \sum_{i=1}^{n} P_i - E$, per ogni $m \in \mathbb{N}$, dove E è il divisore definito nel Paragrafo 2.1.

Proposizione 2.17. *Ogni $h \in L(E_m)$ si può scrivere nella forma $h = \frac{H}{Z^m}$ dove H è un'aggiunta di C di grado m. Inoltre, se $m = n - 3$, allora,* $\deg(E_m) = 2g - 2, \ell(E_m) \geq g$.

Dimostrazione. Si veda [1] Capitolo 8, Paragrafo 3. □

Capitolo 3

Differenziali ed il Divisore Canonico

3.1 Derivazioni e Differenziali

Sia R un anello che contiene k, ed M un R-modulo. Una derivazione di R in M su k è una funzione k-lineare $D : R \to M$ tale che $D(xy) = xD(y) + yD(x)$ per ogni $x, y \in R$.

Lemma 3.1. *Sia R un dominio con campo dei quozienti K e sia $D : R \to M$ una derivazione. Allora esiste un'unica derivazione $\tilde{D} : K \to M$ che estende D.*

Dimostrazione. Sia $z \in K$, allora esistono $x, y \in, y \neq 0$, tali che $z = \frac{x}{y}$. Allora $x = yz$, da cui, imponendo che valga la condizione sui prodotti e riordinando, si trova la formula $\tilde{D}(z) = y^{-1}(D(x) - zD(y))$. Siccome D è k-lineare, anche $\tilde{D}$ lo è. Allora, se $z = \frac{x}{y}, w = \frac{u}{v}$:

$$\tilde{D}(zw) = \frac{D(xu) - zwD(yv)}{yv} = \\ = z\frac{D(u)}{v} + w\frac{D(x)}{y} - z\frac{D(v)}{v} - w\frac{D(y)}{y} = z\tilde{D}(w) + w\tilde{D}(z)$$

□

Voglio definire i differenziali di R come elementi della forma $\sum x_i dy_i, x_i, y_i \in R$. Un modo per fare ciò è la seguente costruzione: sia per $x \in R$ il simbolo $[x]$, e sia F il R-modulo libero generato da $\{[x] : x \in R\}$. Sia inoltre N il sottomodulo di F generato dagli insiemi $\{[x + y] - [x] - [y] : x, y \in R\}, \{[\lambda x] - \lambda[x] : x \in R, \lambda \in k\}, \{[xy] - x[y] - y[x] : x, y \in R\}$. Allora il modulo quoziente $\Omega_k(R) = \frac{F}{N}$ è detto *modulo dei differenziali di* R e la mappa $d : R \to \Omega_k(R)$, definita come $dx = \pi([x])$, è una derivazione.

Lemma 3.2. *Per ogni R-modulo M, ed ogni derivazione $D : R \to M$, esiste un unico omomorfismo di R-moduli $\varphi : \Omega_k(R) \to M$ tale che $\varphi(dx) = D(x)$ per ogni $x \in R$.*

Proposizione 3.3. *Sia K un campo di funzioni algebriche in una variabile su k. Allora, $\Omega_k(K)$ è uno spazio di dimensione 1 su K. Inoltre se $x \in K \setminus k$, allora dx è una base per $\Omega_k(K)$ su K.*

Dimostrazione. Sia $F \in k[X,Y]$ una curva affine che ha per campo di funzioni razionali K. Allora $R = \frac{k[X,Y]}{(F)} = k[x,y], K = k(x,y)$. In particolare posso supporre $F_Y \neq 0$, quindi F non divide F_Y, perciò $F_Y(x,y) \neq 0$.
Il fatto che $K = k(x,y)$ prova che dx, dy generano $\Omega_k(K)$ Ma:

$$0 = d(F(x,y)) = F_X(x,y)dx + F_Y(x,y)dy \Longrightarrow dy = -\frac{F_X(x,y)}{F_Y(x,y)}dx$$

quindi, dx genera $\Omega_k(K)$ e $\dim_K(\Omega_k(K)) \leq 1$.
Dimostro ora che $\Omega_k(K) \neq 0$: per farlo mi basta dimostrare che esiste una derivazione su K. Sia $G \in k[X,Y]$, e sia $\bar{G}$ la sua immagine in R. Allora definisco $D : R \to K, D(\bar{G}) = G_X(x,y) - \frac{F_X(x,y)}{F_Y(x,y)}G_Y(x,y)$. D è k-lineare perché le derivate di polinomi e le combinazioni lineari lo sono. Allora fissati $\bar{G}, \bar{H} \in R$, e omettendo x, y:

$$D(\bar{G}\bar{H}) = (GH)_X - \frac{F_X}{F_Y}(GH)_Y = \\ = G_X H + GH_X - \frac{F_X}{F_Y}G_Y H - \frac{F_X}{F_Y}GH_Y = HD(G) + GD(H)$$

Per il Lemma 3.1 posso quindi estenderla ad una derivazione su K. □

Da questa Proposizione segue che per ogni $f, t \in K, t \notin k$, esiste un unico $v \in K$, tale che $df = vdt$, quindi, scriverò $v = \frac{df}{dt}$ e dirò che v è la *derivata* di f rispetto a t.

Proposizione 3.4. *Sia K come nella Proposizione 3.3 e sia $\mathcal{O} \leq K$ un DVR di K e sia $t \in \mathcal{O}$ un parametro uniformizzante. Allora: $f \in \mathcal{O} \Longrightarrow \frac{df}{dt} \in \mathcal{O}$.*

Dimostrazione. Nelle stesse notazioni della dimostrazione della Proposizione 3.3, sia $\mathcal{O} = \mathcal{O}_P(F)$, con $P = (0,0)$, un punto semplice di F. Introduco la seguente notazione $z' = \frac{dz}{dt}, z \in K$.
Sia $N \in \mathbb{N}$, tale che $\mathrm{ord}_P(x), \mathrm{ord}_P(y) \geq -N$, allora, se $f \in R = k[x,y], f' = f_X(x,y)x' + f_Y(x,y)y'$, perciò $\mathrm{ord}_P(f') \geq -N$.
Sia $f \in \mathcal{O}$, allora esistono $g, h \in R$, tali che $f = \frac{g}{h}, h(P) \neq 0$. Allora, da $f' = h^{-2}(hg' - gh')$, ne deduco che $\mathrm{ord}_P(f') \geq -N$ Sia $f \in \mathcal{O}$; se $f = \sum_{i=0}^{N-1} \lambda_i t^i + gt^N$, per opportuni $\lambda_i \in k, g \in \mathcal{O}$ (una tale scrittura esiste sempre), allora $f' = \sum_{i=1}^{N-1} i\lambda_i t^{i-1} + gNt^{N-1} + t^N g'$, ma allora, tutti gli addendi sono in $\mathcal{O}$, dunque $f' \in \mathcal{O}$. □

3.2 Divisori Canonici

Sia C curva proiettiva, X il suo modello non-singolare, K il loro campo delle funzioni razionali,$\Omega = \Omega_k(K)$, lo spazio dei differenziali.
Sia $\omega \in \Omega, \omega \neq 0$ e sia $P \in X$ un posto. Definisco l'ordine di ω in P nel seguente modo: fissato $t \in \mathcal{O}_P(X)$ un parametro uniformizzante, esiste un'unica $f \in K$, tale che $\omega = fdt$. Allora, pongo $\mathrm{ord}_P(\omega) = \mathrm{ord}_P(f)$.
La definizione è una buona definizione: sia $u \in \mathcal{O}_P(X)$ un altro parametro uniformizzante, allora, $\omega = fdt = gdu$. Per la Proposizione 3.4, $\frac{f}{g} = \frac{du}{dt}, \frac{g}{f} = \frac{dt}{du} \in \mathcal{O}_P(X)$, dunque $\mathrm{ord}_P(f) = \mathrm{ord}_P(g)$.
Sia quindi ora per $\omega \in \Omega, \omega \neq 0, \mathrm{div}(\omega) = \sum_{P \in X} \mathrm{ord}_P(\omega)P$, il divisore associato ad ω. Un divisore di questo tipo è detto *canonico*.
Sia $W = \mathrm{div}(\omega)$ e sia $\omega' \in \Omega$ un altro differenziale non nullo. Allora, esiste un'unica $f \in K$ tale che $\omega' = f\omega$, dunque $W' = \mathrm{div}(\omega') = \mathrm{div}(f) + W$, ovvero W, W' sono linearmente equivalenti. Viceversa se $W' \equiv W = \mathrm{div}(\omega)$, allora $W' = W + \mathrm{div}(f)$, $\exists\, f \in K \Longrightarrow W' = \mathrm{div}(f\omega)$.
Ho dimostrato che i divisori canonici sono una classe di equivalenza rispetto alla lineare equivalenza. In particolare hanno tutti lo stesso grado.

Proposizione 3.5. *Sia C una curva piana di grado $n \geq 3$ i cui punti multipli sono ordinari. Sia E come in 2.1 e sia G una curva piana di grado $n-3$. Allora,* $\mathrm{div}(G) - E$ *è un divisore canonico.*

Dimostrazione. Siano X, Y, Z delle coordinate omogenee per $\mathbb{P}^2$ tali che Z interseca C in n punti distinti $P_1, \ldots, P_n, [1,0,0] \notin C$ e le rette tangenti ai punti multipli di C non contengano $[1,0,0]$.
Allora $x = \frac{X}{Z}, y = \frac{Y}{Z} \in K$. Se F è un polinomio che definisce C, allora, pongo $f_X = F_X(x,y,1), f_Y = F_Y(x,y,1)$.
Sia $E_m = m\sum_{i=1}^n P_i - E$, e sia $\omega = dx$. Siccome i divisori della forma $\mathrm{div}(G) - E, \deg(G) = n-3$, sono linearmente equivalenti, è sufficiente dimostrare che $\mathrm{div}(\omega) = E_{n-3} + \mathrm{div}(f_Y) \iff \mathrm{div}(dx) - \mathrm{div}(F_Y) = -2\sum_{i=1}^n P_i - E$.
Siccome $f_Y = \frac{F_Y}{Z^{n-1}}, dx = -\frac{f_Y}{f_X}dy = -\frac{F_Y}{F_X}dy \iff \mathrm{ord}_Q(dx) - \mathrm{ord}_Q(F_Y) = \mathrm{ord}_Q(dy) - \mathrm{ord}_Q(F_Y)\, \forall Q \in X$.
Se Q è centrato in $P_i \in Z \cap C$, allora y^{-1} è parametro uniformizzante di $\mathcal{O}_{P_i}(C)$ e $dy = -y^2 d(y^{-1})$, dunque $\mathrm{ord}_Q(dy) = -2$, inoltre $F_X(P_i) \neq 0$, perché altrimenti Z sarebbe tangente a C in P_i, ma questo contraddice le ipotesi sul riferimento.
Sia Q centrato in $P = [a,b,1]$; a meno di una traslazione, che non cambia i differenziali, sia Q centrato in $P = [0,0,1]$. Se Y è tangente a C in P, P non è multiplo, quindi x è parametro uniformizzante e $F_Y(P) \neq 0$. Allora $\mathrm{ord}_Q(dx) = \mathrm{ord}_Q(F_Y) = 0$. Infine se Y non è tangente, y è parametro uniformizzante, quindi $\mathrm{ord}_Q(dy) = 0, \mathrm{ord}_Q(f_X) = r_Q - 1$. □

Corollario 3.6. *Se W è divisore canonico, allora,* $\deg(W) = 2g-2, \ell(W) \geq g$.

Dimostrazione. Siccome i divisori canonici sono una classe di equivalenza per la lineare equivalenza, è sufficiente fare il calcolo per un divisore. Sia $W = E_{n-3}$. Per la Proposizione 2.17 si conclude. □

Capitolo 4

Il Teorema di Riemann-Roch e la sua dimostrazione

Questo teorema è un raffinamento del Teorema di Riemann, ovvero, la relazione dell'enunciato di Riemann, nel Teorema di Riemann-Roch diventa un'uguaglianza, grazie all'aggiunta di un opportuno addendo.
Un risultato cruciale nella dimostrazione del teorema è:

Lemma 4.1 (di Riduzione di Noether)**.** *Siano W un divisore canonico su X, D un qualunque divisore su X e $P \in X$. Allora, se $\ell(D) > 0$ e $\ell(W - D - P) \neq \ell(W - D)$, allora, $\ell(D) = \ell(D + P)$.*

Dimostrazione. Sia C piana i cui punti multipli sono ordinari e sia $P \in C$ semplice, e siano delle coordinate omogenee in $\mathbb{P}^2$ tali che Z intersechi C in n punti distinti. Sia $E_m = m\sum_{i=1}^{n} P_i - E$; siccome la tesi del teorema è invariante per classi di equivalenza di divisori, allora posso supporre $W = E_{n-3}$ e $D \succ 0$. In particolare $L(W - D) \subseteq L(E_{n-3})$.
Sia $h \in L(W - D) \setminus L(W - D - P)$, allora $h = \frac{G}{Z^{n-3}}$, dove G è un'aggiunta di C di grado $n - 3$. Allora $\mathrm{div}(G) = D + E + A, A \succ 0, A \not\succ P$.
Sia L una retta che non contiene alcun P_i, e tale che intersechi C in P ed altri $n - 1$ punti semplici tutti distinti da P.
Considero $f \in L(D+P)$ e pongo $D' = D+\mathrm{div}(f)$. Devo provare che $f \in L(D) \iff D' \succ 0$. Siccome $D + P \equiv D' + P$, ed entrambi sono effettivi, esiste una curva H di grado $n - 2$ tale che $\mathrm{div}(H) = D' + P + E + A + B$, dove B è il divisore che ha come unici punti con coefficiente non nullo quelli di $L \cap C$ diversi da P con coefficiente 1.
Osservo ora che H è una curva di grado $n - 2$ che contiene $n - 1$ punti allineati, cioè $P + B$, quindi per Bezout L è una componente di H, dunque $P \in H$, ovvero $\mathrm{div}(H) = D'+P+E+A+B \succ P$, ma P non compare in $E+A+B$, dunque $D'+P \succ P \Longrightarrow D' \succ 0$. □

Ora posso procedere con l'enunciato e la dimostrazione del Teorema di Riemann-Roch:

Teorema 4.2 (di Riemann-Roch)**.** *Sia W un divisore canonico su X, allora per ogni divisore su X,*

$$\ell(D) = \deg(D) + 1 - g + \ell(W - D)$$

Dimostrazione. Per un divisore D fissato, considero l'equazione

$$\ell(D) = \deg(D) + 1 - g + \ell(W - D) \tag{4.1}$$

Distinguo due casi:

1. $\ell(W-D) = 0$: siccome $g \leq \ell(W)$ e $\ell(W) \leq \ell(W-D)+\deg(D)$, ne segue che $\ell(D) \geq 1$ per il Teorema di Riemann. Allora procedo per induzione su $\ell(D)$: sia $\ell(D) = 1$, se 4.1 fosse falsa, allora per il Teorema di Riemann, $\ell(D) > 1$, assurdo. Sia quindi n, tale che per ogni divisore tale che $\ell(D) = n - 1$ e $\ell(W - D) = 0$ valga il Teorema di Riemann-Roch. Sia quindi D tale che $\ell(D) = n, \ell(W - D) = 0$ e sia $P \in X$ tale che $\ell(D-P) = \ell(D)-1$, allora per il Lemma di Riduzione, $\ell(W-(D-P)) = \ell(W-D) = 0$. Dunque per ipotesi induttiva

$$\ell(D) = \ell(D - P) + 1 = \deg(D - P) + 1 - g + 1 = \deg(D) + 1 - g$$

2. $\ell(W - D) > 0$: questo caso si verifica per $\deg(D) \leq 2g - 2$; per assurdo sia D un divisore per cui non vale il Teorema di Riemann-Roch. Allora sia un tale D di grado massimo, ovvero tale che $D + P$ soddisfa 4.1 per ogni $P \in X$, sia quindi P tale che $\ell(W - (D + P)) = \ell(W - D) - 1$, quindi per il Lemma di Riduzione, $\ell(D) = \ell(D + P)$. Allora

$$\ell(D) = \ell(D + P) = \deg(D + P) + 1 - g - \ell(W - (D + P)) = \\ = \deg(D) + 1 - g + \ell(W - D)$$

   Ma quindi per D vale il Teorema di Riemann-Roch, assurdo.

□

Corollario 4.3. *Se W è un divisore canonico, allora, $\ell(W) = 1$.*

Corollario 4.4. *Se $\deg(D) \geq 2g - 1$, allora, $\ell(D) = \deg(D) + 1 - g$.*

Corollario 4.5. *Se $\deg(D) \geq 2g$, allora $\ell(D - P) = \ell(D) - 1$ per ogni $P \in X$.*

Capitolo 5

Applicazioni

Dal Teorema di Riemann-Roch discendono alcuni risultati e costruzioni fondamentali.

5.1 Caratterizzazione delle Curve Ellittiche

Voglio dimostrare che una curva algebrica proiettiva irriducibile ha genere 1 se e solo se è birazionalmente equivalente ad una cubica non-singolare.
Sia C una curva di genere 1, allora ogni divisore canonico W su C, è di grado $2 \cdot 1 - 2 = 0$, dunque $L(W - P) = 0$ per ogni $P \in X$. Applicando Riemann-Roch, segue che $\ell(P) = 1$, per ogni $P \in X$.
Analogamente, $\ell(rP) = r$ per ogni $r \in \mathbb{N}, r \neq 0, P \in X$. In particolare $L(P) = k, L(rP) \neq k$ per $r > 1, P \in X$. Sia $P \in X$ fissato.
Sia $\{1, x\}$ una base per $L(2P)$, allora $\mathrm{ord}_P(x) = -2$ altrimenti $\mathrm{ord}_P(x) \geq -1$, dunque $x \in L(P) = k$, ma questo è assurdo in quanto, in tal caso, $\{1, x\}$ non sarebbe una base di $L(2P)$. Sia ora $\{1, x, y\}$ una base di $L(3P)$, allora $\mathrm{ord}_P(y) = -3$, altrimenti, analogamente a prima, $\{1, x, y\}$ non sarebbe una base di $L(3P)$.
Siccome $1, x, y, xy, x^2, x^3, y^2 \in L(6P)$, ma sono linearmente dipendenti, esiste una relazione del tipo:

$$ay^2 + (bx + c)y = Q(x)$$

in cui Q è un polinomio di grado minore o uguale a 3, con i coefficienti di questa combinazione non tutti nulli.
Se $Q = 0$, allora $ay^2 + (bx + c)y = 0$, ma per motivi di ordine, allora tutti i coefficienti devono essere nulli, quindi $Q \neq 0$. Inoltre, essendo Q non nullo, allora, calcolando l'ordine in entrambi i membri, segue che se $a = 0$, allora, non ci sarebbe uguaglianza di ordini, in quanto $\mathrm{ord}_P(bxy + cy) \in \{-5, -3\}$, mentre $\mathrm{ord}_P(Q(x)) \in \{-6. - 4, -2, 0\}$, quindi non varrebbe l'uguaglianza. Quindi ne segue che $a \neq 0$, ma allora $\deg(Q) = 3$. Suppongo $a = 1$.

Con il cambio di base che mappa y in $y + \frac{1}{2}(bx + c)$, l'equazione diventa della forma:

$$y^2 = \prod_{i=1}^{3}(x - \alpha_i)$$

Se per assurdo due degli α_i sono uguali tra loro, ad esempio $\alpha_1 = \alpha_2$, allora, $(\frac{y}{x-\alpha_1})^2 = x-\alpha_3$, da cui $x, y \in k(\frac{y}{x-\alpha_1})$, ma $\mathrm{ord}_P(\frac{y}{x-\alpha_i}) = -1$, quindi $\frac{y}{x-\alpha_i} \in L(P) = k$, ovvero $x, y \in k$, ma questo è assurdo.
Per quanto visto $K = k(x, y)$, in virtù della Proposizione 1.37 e per la Proposizione 2.9. Allora, K è isomorfo a $K(C)$ con $C = V(Y^2Z - X(X - Z)(X - \lambda Z)), \lambda \neq 0, 1$ che è una cubica non-singolare.
Viceversa sia C una curva birazionalmente equivalente ad una cubica non-singolare, allora, $X = V(Y^2Z - X(X - Z)(X - \lambda Z)), \lambda \neq 0, 1$. Per la Proposizione 2.15 segue $g = \frac{2\cdot 1}{2} = 1$.

Definizione 5.1. Una curva C, di genere 1, è detta *ellittica*.

Bibliografia

[1] William Fulton. *Algebraic Curves*. W. A. Benjamin, 1969.

[2] James S. Milne. Fields and galois theory (v5.00), 2021. Available at www.jmilne.org/math/.