LEGGE DI GRUPPO SULLE CURVE ELLITTICHE

ALEX MASSARENTI

Vogliamo definire su una cubica liscia C di $\mathbb{P}^2$ una legge di composizione interna $+$ in modo che (C,+) risulti essere un gruppo abeliano. Troveremo poi delle formule d'addizione esplicite per i punti sulla cubica.

1. Legge di gruppo

Sia $C \subseteq \mathbb{P}^2$ una cubica liscia e sia R una retta di $\mathbb{P}^2$. Dalla versione debole del teorema di Bezout sappiamo che $C \cap R$ consta di tre punti contati con molteplicità. Dobbiamo perciò distinguere tre casi:

(1) $C \cap R$ consta di tre punti distinti.

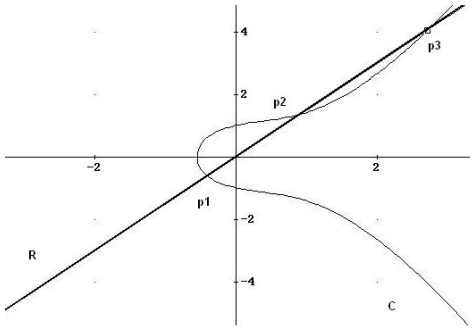

Figura 1. Caso I - Intersezione su tre punti distinti

(2) R è tangente a C e C∩R consta di due punti distinti.

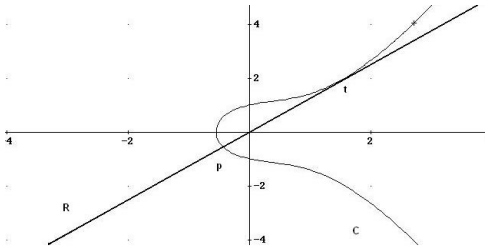

FIGURA 2. Caso II - Intersezione su due punti

(3) R è una tangente di flesso per C, C∩R consta di un solo punto p e i(C,R,p)=3, ovvero p è un flesso di C.

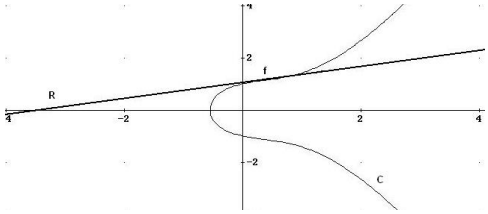

FIGURA 3. Caso III - Intersezione su un punto di molteplicità tre

Introduciamo il terzo punto. Siano a e b due punti sulla cubica C e sia R la retta per a e b. Il terzo punto è l'ulteriore intersezione della retta R con C e si indica con [ab]. Osserviamo che il punto a è un punto di flesso se e solo se [aa]=a.
Fissiamo ora su C un punto O che chiameremo origine e definiamo una legge di composizione interna.

Definizione 1. *Siano p,q due punti di C, allora p+q:=[O,[pq]], cioè p+q è il terzo punto di C∩R dove R è la retta generata da O e da [pq].*

Abbiamo così definito la legge di composizione interna C×C→C che manda (p,q)→p+q.

Lemma 1. *Con le notazioni precedenti si ha:*

(1) Per ogni (p,q)∈C^2, p+q=q+p.
(2) Per ogni p∈C, p+O=O+p=p.
(3) Per ogni p∈C, esiste -p∈C tale che p+(-p)=(-p)+p=O.

Dimostrazione:1) La retta R può essere vista come R=[pq]=[qp] perciò [qp]=[pq] e [O,[qp]]=[O,[pq]]. Dunque p+q=[O,[pq]]∩C=[O,[qp]]∩C=q+p.
2) La retta [Op] interseca ulteriormente C in [Op]. Ora la retta [O[Op]] coincide con [Op] perchè hanno i punti O e p in comune. Quindi la terza intersezione tra [O,[Op]] è proprio p ovvero O+p=p. Da 1) sappiamo poi che p+O=O+p=p.
3)La cubica C è liscia, in particolare O è un punto liscio ed esiste quindi la tangente

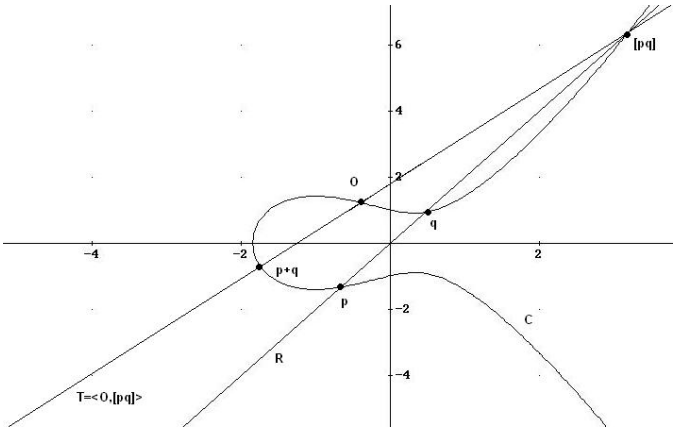

FIGURA 4. Somma di due punti su una cubica

T a C in O. Sia q=[OO] il terzo punto di T∩C. Per ogni punto p∈C poniamo -p=[pq]. Ora la retta [p,-p] coincide con [p,q] quindi [-pp]=q e la retta [q,O] è proprio la tangente T che interseca C in O con molteplicità due. Vediamo così che p+(-p)=-p+p=O. □

A questo punto resta da dimostrare che la legge è associativa ovvero che per ogni (a,b,c)∈C^3 si ha a+(b+c)=(a+b)+c. Ci limitiamo al caso in cui i punti considerati sono distinti. La dimostrazione nel caso generale necessita della teoria degli schemi. Per la dimotrazione completa si può ricorrere ad un argomento di densità, ovvero osservando che i punti fatti intervenire nella dimostrazione dell'associatività sono tutti distinti per un sottoinsieme denso della cubica e argomentando che alla luce di questo la legge può essere estesa su tutta la curva.

Calcoliamo s'=(a+b)+c e t'=(b+c)+a=a+(b+c). In ognuna delle due costruzioni compaiono quattro rette. Riportiamo in figura la prima costruzione. Chiamiamo poi q,q',t,t' i punti delle seconda costruzione corrispondenti a r,r',s,s'.
Nella prima costruzione abbiamo le rette L1=[abr], L2=[cr's], L3=[r'Or], L4=[Os's].

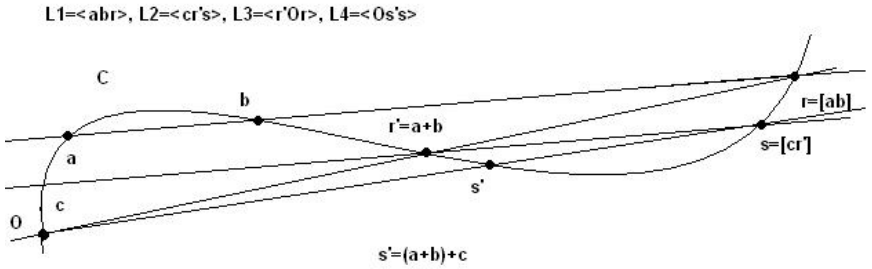

FIGURA 5. Associatività della somma su una cubica

Analogamente nella seconda costruzione abbiamo le quattro rette D1=[bcq], D2=[aq't], D3=[q'Oq], D4=[Ot't]. Vogliamo dimostrare che s'=t'. Chiaramente basta mostrare

che s=t.
Siano ora F=L1∪L2∪D3 e G=D1∪D2∪L3 due cubiche. Si ha:
F∩C={a,b,c,r,r',q',O,q,s} e G∩C={a,b,c,r,r',q',O,q,t}.
Gli otto punti a,b,c,r,r',q',O,q sono otto dei nove punti dell'intersezione F∩C. Per il paradosso di Cramer (Proposizione 41 - Capitolo 6) ogni cubica passante per questi otto punti deve necessariamente passare per il nono punto s. In particolare G deve passare per s e perciò s=t.

Rimane così definita sulla cubica liscia C una struttura di gruppo.

Osservazione 1. *Ogni cubica liscia di $\mathbb{P}^2$ ha di certo un punto di flesso (Lemma 18 - Capitolo 5). Se fissiamo l'origine su un punto di flesso allora O'=[OO]=O perciò -a=[O'a]=[Oa].*

Lemma 2. *Sia O un punto di flesso della cubica liscia C, allora:*

1. *Per ogni (P,Q,U)∈C^3 P+Q+U=O se e solo se P,Q,U sono allineati.*
2. *P è un punto di flesso se e solo se 3P=O.*
3. *Se P,Q sono due flessi allora anche il terzo punto U=[PQ] è un flesso.*

Dimostrazione: 1) Supponiamo che sia P+Q+U=O, allora -U=P+Q quindi [OU]=-U=P+Q=[O[PQ]] ovvero P,Q,U sono allineati. Viceversa supponiamo che i tre punti siano allineati. Allora [PQ]=U da cui P+Q=[O[PQ]]=[OU]=
=-U essendo O un flesso, ovvero P+Q+U=O.
2) Supponiamo che P sia un flesso allora [PP]=P, quindi 2P=P+P=[O[PP]]=[OP]=-P da cui 3P=2P+P=O. Se invece 3P=O, poichè 2P=P+P=[O[PP]] e -P=[OP], da 2P=-P segue che [O[PP]]=[OP] ovvero [PP]=P e quindi P è un flesso.
3) Siano P,Q due flessi. Abbiamo P+Q+[PQ]=O per 1) allora 3(P+Q+[PQ])=O da cui 3[PQ]=O e per 2) concludiamo che [PQ] è un flesso. □

2. Formule d'addizione su una cubica liscia

Sia C una cubica liscia di $\mathbb{P}^2(\mathbb{C})$. Possiamo scriverla nella forma di Legendre come $Y^2Z=X^3+aX^2+bXZ^2+cZ^3$. Nella carta affine U_Z la curva è data da $y^2=x^3+ax^2+bx+c$. Inoltre C è liscia perciò le sue derivate parziali non devono mai annullarsi su uno stesso punto ovvero il polinomio $p(x,y)=y^2-x^3-ax^2-bx-c$ non deve avere radici multiple e quindi il suo discriminante $D(p)=-4a^3c+a^2b^2+18abc-4b^3-27c^2\neq 0$.
Calcoliamo lo spazio tangente di Zariski alla cubica affine C nel suo punto p=(0,1). Posto $P(X,Y,Z)=Y^2Z-X^3-aX^2-bXZ^2-cZ^3$, si ha che Z=0 è tangente a C in p=(0,1,0). Infatti $P(X,Y,0)=-X^3=0$ se e solo se X=0, vediamo che Z=0 e C si intersecano in p con molteplicità tre quindi p=(0,1,0) è un punto di flesso. Notiamo esplicitamente che p non è singolare infatti $P_Z(0,1,0)=1$.
Per il teorema di Bezout debole la cubica proiettiva C interseca la retta all'infinito Z=0 in tre punti contati con molteplicità. Come abbiamo visto c'è un unico punto d'intersezione, il flesso p=(0,1,0) con molteplicità tre. Esplicitiamo la struttura di gruppo su C prendendo l'origine O=p. Sappiamo che C è il completamento proiettivo della curva affine di equazione $p(x,y)=y^2-x^3-ax^2-bx-c$. Possiamo allora riguardare C in $\mathbb{P}^2$ come l'insieme $\{(x,y)\in\mathbb{C}^2 \text{ tali che } p(x,y)=0\}\cup\{O\}$.
Sia ora $p\in\mathbb{C}^2$ denotiamo con (x(p),y(p)) le sue coordinate. Il nostro scopo è stabilire delle relazioni per le coordinate di P+Q,-P e 2P, dove P,Q sono punti della cubica C.
Sia p≠O un punto di C, sia poi R la retta generata da P e O, essendo O un flesso

il terzo punto di R∩C è -P. La retta R è la retta verticale passante per P ovvero la retta di equazione x=x(P). Essendo C simmetrica rispetto all'asse delle x si ha:

Lemma 3. *Sia P=(x(P),y(P)) un punto di C diverso da O allora -P=(x(P),-y(P)).*

Consideriamo ora la **somma di due punti distinti** sulla cubica. Siano $P=(x_1,y_1)$, $P'=(x_2,y_2)$ due punti distinti di C. Posto $[PP']=(x_3,y_3)$ allora P+P' è il terzo punto di R∩C dove R è la retta generata da O e [PP'], quindi $P+P'=(x_3,-y_3)$. Sia $y=mx+q$ l'equazione della retta D per P e P'(nel caso in cui D sia verticale P=-P' e P+P'=O). Si ha $m=(y_1-y_2)/(x_1-x_2)$ (se $x_1=x_2$ allora P=±P'). Il punto [PP'] è il terzo punto di D∩C, tale intersezione è data da:
$y^2=(mx+q)^2=x^3+ax^2+bx+c$ da cui $m^2x^2+2mxq+q^2-x^3-ax^2-bx-c=0$ ovvero $x^3+x^2(a-m^2)+x(b-2q)+c-q^2=0$.
Questa equazione è verificata da P,P' e [PP'], perciò:
$x^3+x^2(a-m^2)+x(b-2q)+c-q^2=(x-x_1)(x-x_2)(x-x_3)=x^3-x^2(x_1+x_2+x_3)+x(x_1x_2x_2x_3+x_1x_3)-x_1x_2x_3$. Allora deve essere $a-m^2=-x_1-x_2-x_3$ da cui $x_3=m^2-a-x_1-x_2$.
Sappiamo poi che $y_1=mx_1+q$ e $y_2=mx_2+q$ perciò $q=y_1-mx_1=y_2-mx_2$. Infine ricaviamo y_3 dalla relazione $y_3=mx_3+q$. Per riassumere vale il segunte:

Lemma 4. *Siano $P=(x_1,y_1)$ e $P'=(x_2,y_2)$ due punti distinti di C a distanza finita. Allora $P+P'=(x,y)$ è il punto di coordinate:*
$x=m^2-a-x_1-x_2$;
$y=-mx-q$;
dove $m=(y_1-y_2)/(x_1-x_2)$ e $q=y_1-mx_1=y_2-mx_2$.

Ricaviamo ora la **formula di duplicazione**. Sia $P=(x_1,y_1)$ un punto di C, cerchiamo le coordinate di 2P=P+P. Consideriamo la retta tangente a C in P che avrà equazione $-(x-x_1)f'(x_1)+(y-y_1)2y_1=0$. La tangente è verticale se e solo se 2P=O. Se $y_1\neq 0$ la tangente avrà equazione del tipo $y=mx+q$ con $m=f'(x_1)/2y_1=(3x_1^2+2ax_1+b)/2y_1$.
Cerchiamo le intersezioni tra la tangente e C, come prima vale l'equazione $y^2=(mx+q)^2=x^3+ax^2+bx+c$ da cui $m^2x^2+2mxq+q^2-x^3-ax^2-bx-c=0$ ovvero $x^3+x^2(a-m^2)+x(b-2q)+c-q^2=0$. Tale equazione è verificata da P con molteplicità due e da $[PP]=(x_{2p},-y_{2p})$. Possiamo scrivere $x^3+x^2(a-m^2)+x(b-2q)+c-q^2=(x-x_1)^2(x-x_{2p})=x^3-x^2(2x_1x_{2p})+x(x_1^2+2x_1x_{2p})-x_{2p}x_1^2$. Da cui $x_{2p}=m^2-a-2x_1$. Possiamo ora ricavare y_{2p} dalla relazione $-y_{2p}=mx_{2p}+q$.
Abbiamo visto che:

Lemma 5. *Sia $P=(x,y)$ un punto di C a distanza finita allora le coordinate del punto 2P sono:*
$x(2P)=f'(x)^2/4f(x)-a-2x$ e $y(2P)=-mx(2P)-q$, con $m=f'(x)/2y$ e $q=y-mx$.
Se $y=0$ allora $2P=O$.

3. Punti razionali delle cubiche lisce

Abbiamo messo una struttura di gruppo sulle cubiche lisce di $\mathbb{P}^2(\mathbb{C})$. Una cubica può avere punti razionali, cioè punti a coordinate intere. Lo studio delle soluzioni razionali di equazioni polinomiali a coefficienti interi è oggetto dell'aritmetica diofantea. Un famoso problema di questa branca della matematica è la congettura di Fermat: *"Non esiste una terna di interi (X,Y,Z) con XYZ≠0 soluzione dell'equazione polinomiale $X^n+Y^n=Z^n$ per n≥3"*. Questo problema venne risolto da Wiles nel 1995.

Definizione 2. *Un punto di $\mathbb{P}^2(\mathbb{C})$ è razionale se e solo se ammette delle coordinate intere. Una curva C di $\mathbb{P}^2(\mathbb{C})$ è definita su $\mathbb{Q}$ se ammette un'equazione F(X,Y,Z)=0 con $F(X,Y,Z)\in\mathbb{Q}[X,Y,Z]$. Si denota con $C(\mathbb{Q})$ l'insieme dei punti razionali della curva C.*

Data una cubica liscia E, definita su $\mathbb{Q}$, non si conosce nessun algoritmo per stabilire se $E(\mathbb{Q})$ sia o meno vuoto. Supporremo quindi che la cubica E abbia un punto razionale e che tale punto sia un flesso. Supponiamo che E sia data da un equazione del tipo $y^2=x^3+ax^2+bx+d$ con $a,b,d\in\mathbb{Q}$. Se sciviamo $a=p/q$, $b=m/n$, $d=s/t$ abbiamo $y^2=x^3+(p/q)x^2+(m/n)x+(s/t)$. Posto M=m.c.m.(q,n,t) possiamo scrivere $My^2=x^3+Ax^2+Bx+C$ con $A,B,C\in\mathbb{Z}$ e posto $My^2=Y^2$ si ha $Y^2=X^3+aX^2+bX+c$ con $a,b,c\in\mathbb{Z}$. Inoltre essendo la cubica liscia sappiamo che il discriminante $D=-4a^3c+a^2b^2+18abc-4b^3-27c^2\neq 0$. Il punto all'infinito O=(0,1,0) è un punto razionale per la cubica E. Allora l'insime dei punti razionali di E è costituito dal punto all'infinito O e dai punti a distanza finita ovvero $E(\mathbb{Q})=\{(x,y)\in\mathbb{Q}^2$ tali che $y^2=f(x)\}\cup\{O\}$. Vediamo allora che risolvere l'equazione diofantea $y^2=f(x)$ è equivalente a determinare $E(\mathbb{Q})$ e questo è equivalente a trovare le soluzioni intere di $Y^2Z=X^3+aX^2Z+bXZ^2+cZ^3$.

Proposizione 1. *$E(\mathbb{Q})$ è un sottogruppo di $E(\mathbb{C})$.*

Dimostrazione: Sappiamo che $O\in E(\mathbb{Q})$. Siano $P,Q\in E(\mathbb{Q})$. Usiamo ora le formule esplicite per l'aritmetica su una cubica liscia ricavate in precedenza. Scriviamo $P=(x_p,y_p)$ e $Q=(x_q,y_q)$ con $x_p,y_p,x_q,y_q\in\mathbb{Q}$. Sappiamo che $-Q=(x_q,-y_q)$ e quindi anche -Q è razionale. Ora $P-Q=P+(-Q)=(x,y)$ è dato da: $x=m^2-a-x_p-x_q$ e $y=-mx-q$, con $m=(x_p-x_q)/(y_p-y_q)$ e $q=y_p-mx_p$. Vediamo così che m è razionale essendo rapporto di razionali. Dal fatto che $\mathbb{Q}$ è sottogruppo di $\mathbb{C}$ deriva che x è razionale. Inoltre mx_p è razionale perchè prodotto di razionali, quindi q è razionale e ancora $y=-mx-q$ è razionale. □

Consideriamo ad esempio la curva di Fermat definita da $X^3+Y^3=Z^3$. Grazie al teorema di Wiles possiamo concludere che gli unici punti razionali di F sono (1,0,1), (1,-1,0) e (0,1,1) ovvero $F(\mathbb{Q})=\{(1,0,1);(1,-1,0);(0,1,1)\}$.

Più in generale sia X una curva ellittica su un campo K algebricamente chiuso. Supponiamo che X possa essere definita tramite un'equazione f(X,Y,Z)=0 a coefficienti in un campo k contenuto nel campo K, diciamo allora che X è definita si k. A questo punto è evidente, grazie alla natura geometrica della legge di composizione su X, che l'insieme X(k) dei punti di X a coordinate in k è un sottogruppo del gruppo su X.
In particolare se $K=\mathbb{C}$ e $k=\mathbb{Q}$ possiamo supporre f(X,Y,Z) a coefficienti in $\mathbb{Z}$ avendo su $\mathbb{P}^2$ delle coordinate omogenee. Ci riduciamo così a cercare le soluzioni intere

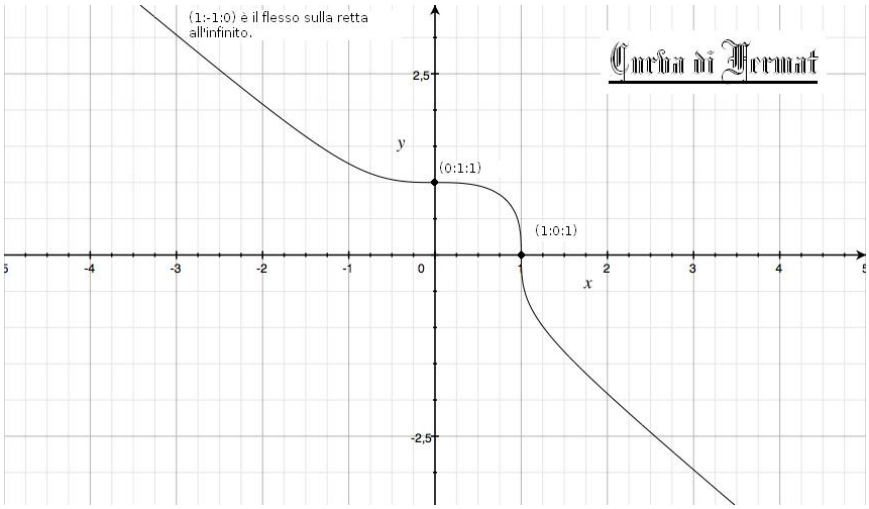

FIGURA 6. Curva di Fermat

dell'equazione cubica diofantea f(X,Y,Z)=0.
Il teorema di Mordell da' un'informazione importante rigurado al gruppo X($\mathbb{Q}$), afferma infatti che X($\mathbb{Q}$) è un gruppo abeliano finitamente generato.
Un altro importante risultato è dovuto a Faltings. Se C è una curva liscia in $\mathbb{P}^2(\mathbb{C})$ di grado d$\geq$4 definita da un' equazione a coefficienti interi, allora C ha un numero finito di punti razionali.
Grazie a questo teorema possiamo affermare che l'equazione di Fermat $X^n+Y^n=Z^n$ ha al più un numero finito di soluzioni intere per ogni n$\geq$4.

Varietà Abeliane

«Una realtà completamente indipendente dallo spirito che la genera, la vede, o la sente, è un'impossibilità; un mondo talmente esterno a noi che, anche se esistesse, ci sarebbe per sempre inaccessibile.»

Jules Henri Poincaré (1854-1912)

Nella prima parte di questo capitolo viene introdotto lo spazio tangente ad una varietà algebrica X in un suo punto x, al fine di dimostrare alcune proprietà sui punti lisci e singolari delle varietà. Vengono poi dimostrate alcune importanti proprietà riguardo alle varietà abeliane. In particolare mostriamo che una varietà associata a un gruppo algebrico è sempre liscia, che una varietà abeliana è sempre commutativa e che due varietà abeliane isomorfe come varietà algebriche sono isomorfe anche come gruppi. L'ultima parte mostra che la legge di gruppo sulle curve ellittiche può essere rivista attraverso la teoria delle funzioni ellittiche, in particolare usando alcune proprietà di una delle più semplici funzioni ellittiche non costanti, la $\wp$ di Weierstrass. Grazie alla $\wp$ assoceremo ad un toro complesso una curva ellittica.

4. Punti lisci e punti singolari sulle varietà algebriche

Vogliamo ora dimostrare alcuni importanti teoremi sulle varietà abeliane. Per fare questo è necessario introdurre la nozione di spazio tangente a una varietà algebrica X in un suo punto x.
Definiamo lo spazio tangente a X in x come l'insieme delle rette per il punto

$x \in X$ tangenti alla varietà X. Riguardiamo $X \subseteq \mathbb{A}^n$ e fissiamo $x=(0,...,0)$. Allora la generica retta L passante per x è della forma $L=\{ta$ tali che $t \in K\}$ con $a \neq 0$ punto fissato in $\mathbb{A}^n$. Al fine di studiare l'intersezione $X \cap L$ supponiamo che la varietà X sia definita dall'ideale $I=(F_1,...,F_m)$. Allora $X \cap L$ è dato dalle equazioni $F_1(ta)=...=F_m(ta)=0$. Stiamo ora considerando polinomi nella sola variabile t, le loro radici comuni sono le radici del loro massimo fattore comune. Supponiamo che sia $f(t)=hcf\{F_1(ta),...,F_m(ta)\}=A\prod(t-a_i)^{ki}$. I valori $t=a_i$ corrispondono ai punti di intersezione tra X e L. Osserviamo che ad ogni a_i è associata una molteplicità k_i che viene interpretata geometricamente come la molteplicità dell'intersezione tra la retta L e la varietà X nel punto corrispondente ad a_i. Notiamo che poichè $0 \in X \cap L$, una delle radici di f(t) è t=0. Possiamo ora dare la seguente definizione.

Definizione 3. *La molteplicità dell'intersezione di una retta L con una varietà X nel punto x=0 è la molteplicità di t=0 come radice del polinomio* $f(t)=hcf\{F_1(ta),...,F_m(ta)\}$.

Vediamo allora che la molteplicità dell'intersezione è la più grande potenza di t che divide tutti gli $F_i(ta)$. Tale molteplicità è certamente maggiore o uguale ad 1, poichè $0 \in X \cap L$. Se gli $F_i(ta)$ sono identicamente nulli si assume la molteplicità come $+\infty$.
Osserviamo inoltre che $f(t)=hcf\{F_1(ta),...,F_m(ta)\}=hcf\{F(ta)$ tali che $F \in I\}$. Infatti se f(t) è il massimo fattore che divide tutti gli $F_i(ta)$, f(t) divide certamente ogni F(ta) con $F \in I$ ed è anche il massimo a fare ciò perchè in particolare gli $F_i \in I$. Se viceversa f(t) è il massimo fattore che divide tutti gli $F(ta) \in I$ a maggiore ragione sarà il massimo a dividere gli $F_i(ta)$. Vediamo così che la molteplicità dell'intersezione non dipende dai generatori di I che abbiamo scelto. Possiamo dare ora la seguente definizione.

Definizione 4. *Una retta L è tangente alla varietà X nel punto x=0 se ha intersezione di molteplicità maggiore o uguale a 2 con X nel punto x=0.*

Osserviamo ora che poichè $0 \in X$ ogni polinomio $F_i(T)$ ha termine costante nullo. Per i=1,...,m, scriviamo $F_i=L_i+G_i$ dove L_i è il termine lineare e G_i è costituito dai termini di grado maggiore o uguale a 2. Allora $F_i(at)=L_i(at)+G_i(at)=tL_i(a)+G_i(at)$. Ora i $G_i(at)$ sono divisibili per t^2, quindi F_i è divisibile per t^2 se e solo se $L_i(a)=0$ per i=1,...,m. Allora possiamo riscrivere la relazione di tangenza come

$$L_1(a)=...=L_m(a)=0.$$

Diamo ora la definizione di spazio tangente.

Definizione 5. *Il luogo geometrico di tutti i punti appartenti alle rette tangenti a X in x si dice spazio tangente a X in x e viene denotato con* T_xX.

Il nostro prossimo obiettivo è mostrare che se $f:X \to Y$ è un isomorfismo tra varietà algebriche allora lo spazio tangente a X in x e lo spazio tangente a Y in f(x) sono isomorfi. Per fare questo tradurremo la nozione di spazio tangente in termini dell'anello dello coordinate K[X].
Se $F(T_1,...,T_N)$ è un polinomio e $x=(x_1,...,x_N)$ un punto, allora F può essere espresso in serie di Taylor come

$$F(T)=F(x)+F^1(T)+...+F^k(T),$$

Dove F^i è un polinomio omogeneo di grado i nelle variabili T_j-x_j. La forma lineare F^1 è il differenziale di F in x e viene denotato con d_xF, abbiamo

$$d_xF=\sum_{i=1}^{N}(\partial F/\partial T_i)(x)(T_i\text{-}x_i).$$

Valgono allora le relazioni: $d_x(F+G)=d_xF+d_xG$ e $d_x(FG)=d_xFG+Fd_xG$.
Attraverso le nuove relazioni possiamo scrivere lo spazio tangente a x in X tramite il sistema lineare

$$d_xF_1=...=d_xF_m=0 \text{ o } \sum_{i=1}^{N}(\partial F_j/\partial T_i)(x)(T_i\text{-}x_i)=0 \text{ per } j=1,...,m,$$

dove $I=(F_1,...,F_m)$ è l'ideale di definizione della varietà X.
Supponiamo che $g\in K[X]$ sia definita restringendo un polinomio G alla varietà X. Poniamo $d_xg=d_xG$. Ci chiediamo ora se d_xg dipende dal polinomio G scelto. Poichè $I=(F_1,...,F_m)$ se $F\in I$ allora $F=P_1F_1+...+P_mF_m$. Ora poichè $d_x(P_iF_i)=d_xP_iF_i+P_id_xF_i$ e $F_i(x)=0$, abbiamo che $d_xF=P_1(x)d_xF_1+...+P_m(x)d_xF_m$. Da $d_xF_1=...=d_xF_m=0$ si ha che $d_xF=0$ su T_x per ogni $F\in I$. Allora se definiamo d_xg come la restrizione della forma lineare d_xG a T_x abbiamo una mappa che manda ogni funzione $g\in K[X]$ in una ben definita forma lineare d_xg su T_x.

Definizione 6. *La forma lineare d_xg appena definita di dice differenziale di g in x.*

Abbiamo ora un morfismo $d_x:K[X]\to T_x^*$, dove T_x^* è lo spazio vettoriale delle forme lineari su T_x. Poichè $d_xa=0$ per ogni $a\in K$ è sufficiente studiare la mappa $d_x:M_x\to T_x^*$, dove $M_x=\{f\in K[X] \text{ tali che } f(x)=0\}$. Notiamo che M_x è un ideale di K[X]. Infatti $0\in M_x$, se $u,v\in M_x$ allora $(u\text{-}v)(x)=u(x)\text{-}v(x)=0$ ovvero $u\text{-}v\in M_x$ e se $f\in K[X]$ e $u\in M_x$ allora $(fu)(x)=f(x)u(x)=0$, ovvero $fu\in M_x$.

Proposizione 2. *La mappa d_x definisce un isomorfismo di spazi vettoriali tra M_x/M_x^2 e T_x^*.*

Dimostrazione: Sia f una forma lineare su T_x. Certamente f è indotta da una qualche funzione lineare F su $\mathbb{A}^N$ e $d_xF=f$. Abbiamo così mostrato che l'applicazione è suriettiva. Supponiamo ora $x=(0,...,0)$ e che $g\in M_x$ con $d_xg=0$. Supponiamo poi che g sia indotta da un polinomio $G\in K[T_1,...,T_N]$. Allora la forma lineare d_xG è nulla su T_x, perciò è combinazione lineare delle forme che definiscono T_x. Possiamo scrivere $d_xG=a_1d_xF_1+...+a_md_xF_m$. Poniamo ora $G_1=G\text{-}a_1d_xF_1\text{-}...\text{-}a_md_xF_m$. Per come è definito G_1 non ha termini di grado 0 o 1 nelle variabili $T_1,...,T_N$ e quindi $G_1\in(T_1,...,T_N)^2$. Inoltre $G_1(x)=G(x)=g(x)$ per ogni $x\in X$, e quindi $g\in(t_1,...,t_N)^2$ dove $t_i=T_{i|X}$. Ora dal fatto che $M_x=(t_1,...,t_N)$ segue la tesi. □

Lo spazio vettoriale M_x/M_x^2 si dice spazio cotangente a X in x. Ora T_x è isomorfo al suo duale T_x^* che per la proposizione precedente è isomorfo a M_x/M_x^2. Quindi abbiamo un isomorfismo tra T_x è M_x/M_x^2. Ovvero lo spazio tangente e lo spazio cotangente ad una varietà X nel punto x sono isomorfi.
Siano ora X e Y due varietà algebriche e $F:X\to Y$ una mappa regolare. Allora F induce una mappa $f:K[Y]\to K[X]$ e si ha $f(M_{F(X)})\subseteq M_x$ e $f(M_{F(X)}^2)\subseteq M_x^2$, quindi F induce una mappa $f:M_{F(X)}/M_{F(X)}^2\to M_x/M_x^2$. Per la proposizione precedente T_x e $T_{F(x)}$ sono isomorfi rispettivamente a M_x/M_x^2 e a $M_{F(x)}/M_{F(x)}^2$. Abbiamo così una mappa $T_x\to T_{F(x)}$ detta differenziale di F in x e denotata con d_xF. Ora se $G:Y\to Z$ è un'altra mappa regolare allora il differenziale $d_x(G\circ F)=d_xG\circ d_xF$. Inoltre se $F:X\to X$ è l'identità allora il differenziale di F è l'identita su T_x per ogni $x\in X$.
Tutto questo ci dice che sotto un isomorfismo tra varietà gli spazi tangenti in punti corrispondenti sono isomorfi. In particolare spazi tangenti in punti corrispondenti hanno la stessa dimensione.

Definizione 7. *Una varietà X si dice liscia nel punto x∈X se dim(T_x)=dim(X). In caso contrario X si dice singolare in x.*

Proposizione 3. *Siano X e Y due varietà algebriche isomorfe è F:X→Y un isomorfismo. Allora X è liscia in x se e solo se Y è liscia in F(x).*

Dimostrazione: L'isomorfismo F tra X e Y induce un isomorfismo f tra gli spazi tangenti T_x e $T_{F(x)}$ che quindi hanno la stessa dimensione. Ora X è liscia in x se e solo se dim(X)=dim(T_x). Ma per ipotesi dim(X)=dim(Y). Quindi X è liscia in x se e solo se dim(Y)=dim($T_{F(x)}$), se e solo se Y è liscia in F(x). □

Al fine di dimostrare la prossima proposizione assumiamo il seguente fatto del quale non diamo la dimostrazione.
Ogni varietà quasi affine Y, con dim(Y)=n, è birazionalmente equivalente ad un'ipersuperficie di $\mathbb{A}^{n+1}$.

Proposizione 4. *Sia Y una varietà quasi-affine, l'insieme dei punti non singolari di Y contiene un aperto non vuoto.*

Dimostrazione: Cominciamo col supporre che Y=$\mathbf{V}$(F) sia un'ipersuperficie di $\mathbb{A}^n$, quindi F è un polinomio non costante e irriducibile. Sappiamo che y∈Y è singolare se e solo se tutte le derivate parziali F'$_i$(y)=(∂F/∂T$_i$)(y) sono nulle. Quindi i punti singolari di Y formano un chiuso di Y. Se ogni punto di Y è singolare allora le derivate parziali si annullano su Y ovvero F'$_i$∈$\mathbb{I}$(Y)=(F), dunque F divide F'$_i$. Se la variabile X_i compare in F allora $\deg_{Xi}$(F'$_i$)<$\deg_{Xi}$(F) e quindi deve essere F'$_i$=0. Ora se char(K)=0 e tutte le derivate parziali sono nulle si ha che F è costante e siamo arrivati ad una contraddizione. Se char(K)=p interi positivo, F'$_i$=0 implica che F è un polinomio in X_i^p. Poichè questo vale per ogni i prendendo delle radici p-esime dei coefficienti di F (K algebricamente chiuso), abbiamo F=G^p, assurdo perchè F è irriducibile. La proposizione risulta provata nel caso delle ipersuperfici. Se ora Y è una varietà quasi-affine qualsiasi sappiamo che esiste un'ipersuperficie Z di $\mathbb{A}^n$ e due aperti U⊆Y, V⊆Z, e un isomorfismo f:U→V. Grazie alla prima parte della dimostrazione sappiamo che l'insieme dei punti lisci di Z è un aperto non vuoto W di Z. Poichè Z è irriducibile anche V∩W è un aperto non vuoto. Quindi f^{-1}(V∩W) è un aperto costituito da punti lisci di Y. □

Proposizione 5. *Sia Y una varietà quasi-affine. Per ogni t∈$\mathbb{A}$ posto Y_t={y∈Y tali che dim(T_y Y)≥t} si ha che Y_t è chiuso rispetto alla topologia di Zariski in Y.*

Dimostrazione: Sia $\mathbb{I}$(Y)=(P_1,...,P_m) e sia J(y) la matrice Jacobiana dei P_i nel punto y. Ora dim(T_yY)≥t se e solo se rango(J(y))≤n-t se e solo se tutti i minori di ordine n-t+1 di J(y) sono nulli. Quindi Y_t è l'intersezione di Y con $\mathbf{V}$(M_1,...,M_i,...) dove gli M_i sono i minori di ordine n-t+1 della matrice Jacobiana J(P_1,...,P_m). □

Proposizione 6. *Sia Y una varietà quasi-affine. Allora per ogni y∈Y dim(T_y Y)≥dim(Y). In particolare Sing(Y), insieme dei punti singolari di Y, è un chiuso proprio di Y.*

Dimostrazione: Sia dim(Y)=n, sappiamo dalla proposizione precedente che Y_n è un chiuso di Y e che Y_n contiene un aperto di punti non singolari, quindi Y_n=Y. Questo significa che per ogni y∈Y si ha dim(T_yY)=dim(Y) oppure dim(T_yY)>dim(Y). Sappiamo che l'insieme dei punti singolari è chiuso in Y ed è un chiuso proprio perchè l'insieme dei punti lisci di Y contiene sempre un aperto non vuoto. □

5. Gruppi algebrici e varietà abeliane

Definizione 8. *Un gruppo algebrico è una varietà algebrica V con una legge di composizione interna + tale che:*

- *(V,+) sia un gruppo;*
- *la mappa $\chi: V \to V$ definita da $\chi(v)=-v$ sia un'applicazione regolare;*
- *la mappa $\tau: V \times V \to V$ definita da $\tau(v_1,v_2)=v_1+v_2$ sia un'applicazione regolare.*

Definizione 9. *Un gruppo algebrico A su una varietà proiettiva viene detto una varietà abeliana.*

Diamo alcuni esempi di gruppi algebrici.

(1) La retta affine $\mathbb{A}^1$ con la somma usuale tra le coordinate dei punti e la varietà $\mathbb{A}^1$-(0) con la moltiplicazione tra le coordinate dei punti.

(2) Le cubiche lisce di $\mathbb{P}^2$ con la legge di composizione interna definita nel capitolo precedente. Infatti abbiamo visto che se C è una cubica liscia allora (C,+) è un gruppo.
Inoltre sappiamo che dato un punti P∈C di coordinate (X,Y) si ha che -P=(X,-Y) ovvero la mappa χ:V→V della definizione è data da $\chi((X,Y))=(X,-Y)$ e evidentemente è una mappa regolare.
Infine la mappa τ:V×V→V è data da $\tau(P_1,P_2)=P_1+P_2=(X,Y)$, dove:
$X=(\frac{Y1-Y2}{X1-X2})^2$-a-$X_1$-$X_2$ e
$Y=-\frac{Y1-Y2}{X1-X2}((\frac{Y1-Y2}{X1-X2})^2$-a-$X_1$-$X_2)$-$Y_1+\frac{Y1-Y2}{X1-X2}X_1$.
Quindi indicati con $P_1=(X_1,Y_1)$ e $P_2=(X_2,Y_2)$ due punti distinti su C si ha:

$$\tau(P_1,P_2)=(X,Y), \text{ con}$$
$$X=((Y_1-Y_2)^2-(a+X_1+X_2))/(X_1-X_2)^2 \text{ e}$$
$$Y=((Y_1-Y_2)(X_1(X_1-X_2)^2-(Y_1-Y_2)^2-(a+X_1+X_2))/(X_1-X_2)^3$$

Possiamo supporre $X_1 \neq X_2$, infatti in caso contrario avremmo $P_1=\pm P_2$. Se $P_1=-P_2$ allora $P_1+P_2=O$. Quindi la funzione τ è regolare su C.
Consideriamo ora il caso $P_1=P_2$. Dalla formula di duplicazione abbiamo:

$$\tau(P_1,P_1)=(f'(X_1)^2/4f(X_1)-a-2X_1,\ -m(f'(X_1)^2/4f(X_1)-a-2X_1)-q)$$
$$\text{con } m=f'(X_1)/2f(X_1) \text{ e } q=f(X_1)-mX_1.$$

Anche in questo caso l'applicazione τ risulta regolare perchè $Y_1=f(X_1)\neq 0$. Infatti se $Y_1=0$ abbiamo visto che la tangente in P_1 a C è verticale e allora $2P_1=O$.
Più brevemente si può concludere che χ e τ sono mappe regolari grazie **al principio delle costruzioni algebro-geometriche**. Infatti nella costruzione geometrica della legge di gruppo in sostanza abbiamo considerato intersezioni tra curve algebriche ovvero operazioni geometriche che possono essere tradotte in linguaggio algebrico. Abbiamo così definito sulle curve ellittiche una struttura di gruppo algebrico. Possiamo perciò concludere che **le curve ellittiche sono varietà abeliane di dimensione uno in** $\mathbb{P}^2$.

Teorema 1. *La varietà associata a un gruppo algebrico G è non singolare.*

Dimostrazione: Per ogni h∈G consideriamo la mappa F_h:G→G, che manda g↦h+g. Per la definizione di gruppo algebrico si ha che F_h è un automorfismo della varietà G. Per ogni g_1,g_2∈G abbiamo $F(g_1)=g_2$ se prendiamo $h=g_2-g_1$. Sappiamo che un punto singolare è invariante sotto un isomorfismo (Proposizione 44). Allora se G avesse un punto singolare g ogni punto di G risulterebbe essere singolare, assurdo perchè Sing(G) è un chiuso proprio di G (Proposizione 47). Concludiamo che ogni punto di G è liscio. □

Enunciamo ora un lemma necessario in seguito senza darne una dimostrazione[1].

Lemma 6. *Siano X e Y due varietà algebriche con X varietà proiettiva, e sia f:X× Y→Z una famiglia di applicazioni da X in una varietà Z di base Y. Supponiamo che esista y_0∈Y tale che f(X×y_0)=z_0∈Z sia un punto. Allora f(X×y) è un punto per ogni y∈Y.*

Teorema 2. *Una varietà abeliana è sempre commutativa.*

Dimostrazione: Consideriamo una famiglia di mappe da G in G di base G date da f(g,h)=-g+h+g. Per $h=0_G$ abbiamo f(g,0_G)=0_G e allora per il lemma precedente f(G,h) è un punto per ogni h. Quindi f(g,h)=f(0_G,h)=h. Vediamo così che -g+h+g=h ovvero h+g=g+h per ogni g,h∈G e quindi G è un gruppo abeliano.

□

Teorema 3. *Se F:G→H è una mappa regolare tra una varietà abeliana G e un gruppo algebrico H, allora F(g)=F(0_G)+f(g) dove f:G→H è un morfismo di gruppi.*

Dimostrazione: Poniamo f(g)=-F(0_G)+F(g) e consideriamo la seguente famiglia di mappe da G in H e di base G:

T:G×G→H date da T(g',g)=f(g')+f(g)-f(g'+g).

Notiamo che f(0_G)=0_H dunque T(G,0_G)=0_H. Per il lemma T(G,g) è un singolo punto per ogni g∈G ovvero T(g',g) non dipende da g'. Posto g'=0_G si ha che T(g',g)=T(0_G,g)=0_H dunque f(g')+f(g)-f(g'+g)=0_H ovvero f(g'+g)=f(g')+f(g) ed f è un morfismo di gruppi. □

Teorema 4. *Se due varietà abeliane sono isomorfe come varietà allora sono isomorfe come gruppi.*

Dimostrazione: Sia F:X→Y l'isomorfismo tra la varietà abeliane X e Y. Possiamo riguardare F come una mappa regolare tra la varietà X e il gruppo algebrico Y. Per il teorema precedente F induce un isomorfismo di gruppi f:X→Y. Sappiamo inoltre che f(x)=-F(0_X)+F(x)=A+F(X), dove A=-F(0_X) è costante. Vediamo allora che essendo F biettiva anche f lo è, dunque f:X→Y è un isomorfismo di gruppi. □

[1]Per la dimostrazione del lemma si veda I.Shafarevich - Basic Algebraic Geometry, pag.191.

6. Funzione $\wp$ di Weierstrass e legge di gruppo sulle curve ellittiche

Consideriamo ora il campo dei numeri complessi $\mathbb{C}$. Siano $v_1, v_2 \in \mathbb{C}$ linearmente indipendenti su $\mathbb{R}$, il reticolo generato da v_1 e v_2 è

$$\Gamma = \{pv_1 + qv_2 \text{ tali che } p,q \in \mathbb{Z}\}.$$

Sia f una funzione meromorfa e sia P_f l'insieme dei suoi periodi.

Teorema 5. *Una funzione ellittica rispetto a* Γ *è una funzione meromorfa tale che* $P_f \cup \{0\} \supseteq \Gamma$.

Consideriamo ora la serie $(1/z^2)+\sum_{p,q\in\mathbb{Z}}(1/(z-pv_1-qv_2)^2)-(1/(pv_1+qv_2)^2)$, si ha che tale serie converge in norma su $\mathbb{C}$ e in particolare converge uniformemente. Poniamo

$$\wp(z) = (1/z^2)+\sum_{p,q\in\mathbb{Z}}(1/(z-pv_1-qv_2)^2)-(1/(pv_1+qv_2)^2).$$

La funzione così definita è la $\wp$ di Weierstrass. Tale funzione è meromorfa e ha poli nei punti di Γ. Si dimostra che $\wp$ e $\wp$' appartengono al campo delle funzione ellittiche su Γ e che inoltre $E(\Gamma) = \mathbb{C}(\wp, \wp')$ ovvero $E(\Gamma)$ è il campo generato dalle funzioni $\wp$ e $\wp$' relative al reticolo Γ.
Inoltre la $\wp$ può essere riguardata come funzione inversa dell'integrale ellittico

$$u = \int_y^\infty (1/(4v^3 - Av - B)^{1/2})dv, \text{ con A,B costanti.}$$

ovvero $y = \wp(u)$.
Le propietà per noi più importanti della $\wp$ sono le seguenti[2]:

- La $\wp$ di Weierstarss soddisfa ad un teorema di addizione e in particolare alla relazione determinantale
$$\mathrm{Det}\begin{pmatrix} \wp(z) & \wp'(z) & 1 \\ \wp(y) & \wp'(y) & 1 \\ \wp(z+y) & -\wp'(z+y) & 1 \end{pmatrix} = 0$$
- La funzione $\wp(z)$ di Weierstrass soddisfa all'equazione differenziale
$$(\wp')^2 = 4(\wp)^3 - A\wp - B \text{ dove A,B sono costanti.}$$

Posto $\wp' = y$ e $\wp = x$ abbiamo l'equazione $y^2 = 4x^3 - Ax - B$, che definisce una cubica parametrizzata da $(\wp, \wp')$.
Se ora reinterpretiamo tale curva come ottenuta per deomogeneizzazione dell'equzione di una curva piana proiettiva abbiamo, $y = Y/Z$ e $x = X/Z$. Da cui $(Y/Z)^2 = 4(X/Z)^3 - A(X/Z) - B$ ovvero $Y^2Z = 4X^3 - AXZ^2 - BZ^3$, che è l'equazione di una curva ellittica.
Ora i punti della cubica $y^2 = 4x^3 - Ax - B$ sono della forma $(x,y,1) = (\wp(z), \wp'(z), 1)$.
Grazie al teorema d'addizione per la $\wp(z)$, sappiamo che vale la seguente relazione determinantale

$$\mathrm{Det}\begin{pmatrix} \wp(z) & \wp'(z) & 1 \\ \wp(y) & \wp'(y) & 1 \\ \wp(z+y) & -\wp'(z+y) & 1 \end{pmatrix} = 0$$

e quindi i punti $P_1 = (\wp(z), \wp'(z), 1)$, $P_2 = (\wp(y), \wp'(y), 1)$ e $P_{1,2} = (\wp(z+y), -\wp'(z+y))$ sulla cubica sono allineati. La cubica che stiamo considerando è simmetrica rispetto all'asse delle ascisse, $P_{1,2}$ non è altro che il terzo punto. Se fissiamo l'origine O sul punto all'infinito (0:1:0) della cubica e poniamo $P_1 + P_2 = P_S$ dove P_S è il simmetrico di $P_{1,2}$ rispetto all'asse delle ascisse, ovvero la terza interzezione della retta per O e

[2]Per un approfondimento sulla funzione $\wp$ di Weierstrass e per la dimostrazione delle proprietà enunciate si veda Serge Lang - Elliptic Functions.

$P_{1,2}$ con la cubica riotteniamo la struttura di gruppo definita sulle curve ellittiche nel capitolo precedente.

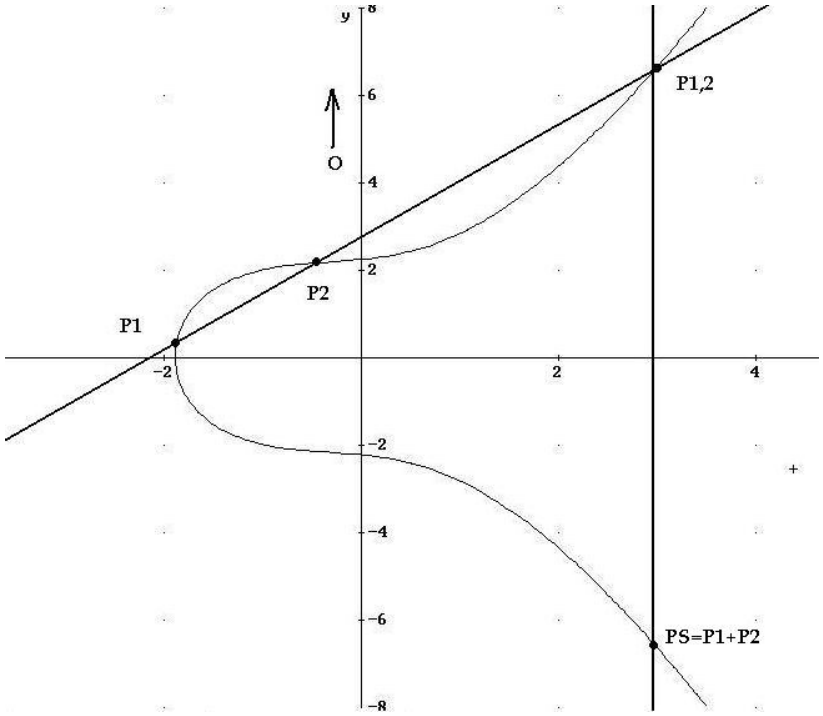

FIGURA 7. Legge di composizione sulla cubica attraverso la funzione $\wp$

7. Curve ellittiche e tori complessi

Consideriamo la seguente definizione:

Definizione 10. *Una varietà complessa di dimensione uno si dice una superfice di Riemann. Una superfice di Riemann compatta è una varietà topologica di dimensione due, compatta e orientabile.*

Consideriamo ancora le curve ellittiche come caso particolare di varietà abeliane. Come sappiamo il genere di un curva piana proiettiva e irriducibile è

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

dove n è il grado della curva. Una curva ellittica è una curva piana di genere uno. E' noto che le varietà topologiche compatte e orientabili di dimensione due sono classificate dal loro genere g. Infatti tali varietà sono omeomorfe ad una sfera con g manici dove g è un numero naturale.
Consideriamo ora una curva ellittica. Possiamo visulizzare la sua traccia reale ma non possiamo fare lo stesso per la sua traccia complessa che vive in uno spazio quadridimensionale. Tuttavia possiamo considerarne la superfice di Riemann che può essere immersa in uno spazio tridimensionale. Consideriamo la cubica definita da $y^2=x^3-x$. La sua traccia reale è riportata in figura.

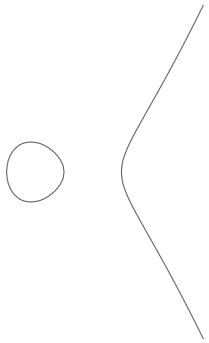

FIGURA 8. Traccia reale della cubica $y^2=x^3-x$

La funzione di variabile complessa associata alla cubica è $f(z)=\sqrt{z^3-z}$. Notiamo esplicitamente che la funzione che stiamo considerando è algebrica, sappiamo dalla teoria generale sulle superfici di Riemann[3] che vale la seguente proposizione:

Proposizione 7. *Sia* $\boldsymbol{A}$ *una funzione analitica. La superfice di Riemann associata ad* $\boldsymbol{A}$ *è compatta se e solo se* $\boldsymbol{A}$ *è algebrica.*

Per quanto detto la superfice associata alla cubica deve essere compatta e pertanto omeomorfa ad una sfera con g=1 manici avvero ad un toro complesso.
Infatti sulla sfera di Riemann $\mathbb{C}^\infty$ la funzione algebrica $f(z)=\sqrt{z^3-z}$ ha quattro punti di diramazione. Tale funzione da luogo a due rami distinti ovvero a due copie distinte di $\mathbb{C}$ che però si intersecano in z=0, z=1, z=-1 e $z=\infty$ che sono punti di diramzione di ordine k=2.
Consideriamo il caso z=0. Poniamo $\xi=z^3-z$. Per z in un intorno dello zero si ha che anche $\xi\in S(0,r)$ e abbiamo $F(\xi)=\xi$, vediamo allora che z=0 è punto di diramazione ordinaria per f, perchè la funzione F ottenuta per sostituzione da f risulta olomorfa in un intorno dello zero.
Consideriamo ora $z=\infty$. Posto $z^3-z=1/\xi^2$ si ha $F(\xi)=1/\xi$. Se z è in un intorno di ∞ allora ξ è in un intorno dello zero. Dunque $z=\infty$ è un punto di diramazione algebrica semplice per f perchè abbiamo ottenuto per F uno sviluppo in serie di Laurent troncato alla prima potenza negativa di ξ.
Per z=1 e z=-1 si ha rispettivamente $F(\xi)=\xi-1$ e $F(\xi)=\xi+1$ e quindi entrambi risultano essere punti di diramazione ordinaria. Possiamo visualizzare la superfice di Riemann associata alla curva tagliando ognuna delle due copie di $\mathbb{C}^\infty$ lungo due archi che congiungono i punti di diramazione è incollandone i bordi. La superfice che otteniamo è proprio un toro.
Si dimostra che se due curve sono birazionalmente equivalenti allora sono isomorfe. Notiamo che la curva considerata non è razionale infatti abbiamo visto che la cubica è omeomorfa ad un toro mentre $\mathbb{P}^1$ essendo una retta e quindi una curva di grado uno e genere g=0 è omeomorfo ad una sfera.

$$\Downarrow$$

[3]Per una trattazione approfondita della teoria sulle superfici di Riemann si veda Farkas, Kra - Riemann Surfaces.

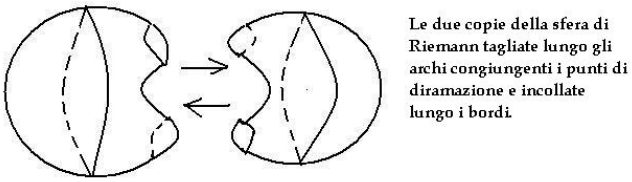

FIGURA 9. Le due copie della sfera di Riemann opportunamente tagliate

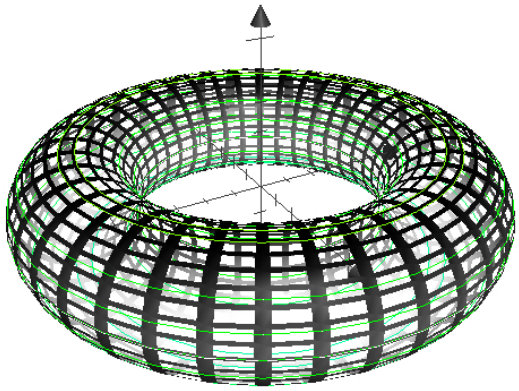

FIGURA 10. Toro complesso

Notiamo che lo studio fatto per la nostra particolare cubica vale in generale per ogni cubica liscia. Sappiamo infatti che ogni cubica liscia pùo essere scritta in forma di Weierstrass come $Y^2Z=X^3+aX^2Z+bZ^3$ e che il discriminante del polinomio $P(x)=x^3+ax^2+b$ è non nullo. Dunque la funzione di variabile complessa $f(z)=\sqrt{P(z)}$, $z\in\mathbb{C}$, presenterà quattro punti di diramazione distinti situati nei tre zeri di $P(z)$ e in $z=\infty$. Perciò la superfice di Riemann ad essa associata sarà ancora un toro.

Vogliamo ora formalizzare quanto detto. Consideriamo ancora la funzione $\wp$ di Weierstrass che sappiamo essere una funzione ellittica rispetto ad un reticolo Γ generato dai suoi periodi primitivi e avente poli esattamente nei punti di Γ.
Notiamo che $\Gamma=\mathbb{Z}v_1+\mathbb{Z}v_2$ è il gruppo additivo libero generato da v_1 e v_2 e in particolare è un sottogruppo normale di $\mathbb{C}$. Ha senso allora considerare il quoziente $\mathbb{C}/\Gamma$. Notiamo che $\mathbb{C}/\Gamma$ è dotato:

- di una struttura di gruppo abeliano ereditata dal gruppo additivo di $\mathbb{C}$.
- della struttura di superfice di Riemann compatta con la topologia quoziente su $\mathbb{C}$. Infatti se per ogni $y\in\mathbb{C}/\Gamma$ consideriamo un $x\in\mathbb{C}$ e un intorno di U_x di x, che contenga al più un punto di Γ allora si ha che la collezione degli U_x forma un atlante per $\mathbb{C}/\Gamma$ se si prendono come mappe di transizione

l'identità o la traslazione.

Il quoziente T=$\mathbb{C}/\Gamma$ si dice un toro complesso. Si ha che T è una varietà complessa di dimensione uno e la sua struttura complessa è determinata dal fatto che la proiezione canonica Π:$\mathbb{C}\longrightarrow\mathbb{C}/\Gamma$ è olomorfa. Topologicamente $\mathbb{C}/\Gamma$ è un $\mathbf{S}^1\times\mathbf{S}^1$. Infatti ogni punto di $\mathbb{C}$ ha un rappresentante nel paralellogramma generato da v_1 e v_2, detto parallelogramma fondamentale, se identifichiamo i lati opposti del paralellogramma percorsi nella medesima direzione otteniamo proprio un toro.

Sappiamo ora che la $\wp$ e la $\wp$' soddisfano alla relazione $(\wp')^2=4\wp^3+A\wp+B$. Inoltre

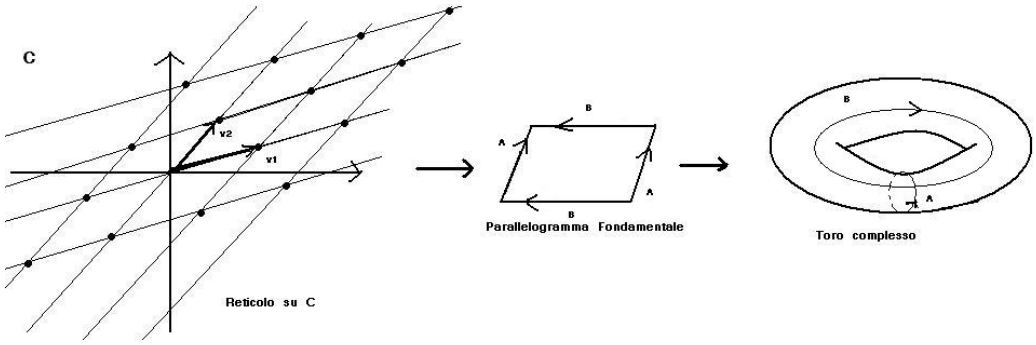

FIGURA 11. Costruzione del toro complesso

in T abbiamo identificato tutti i punti di $\mathbb{C}$ sui quali $\wp$ e $\wp$' assumono lo stesso valore. Tenendo conto di queste osservazioni si dimostra che

Proposizione 8. *La mappa*

$$\Theta{:}T\longrightarrow\mathbb{P}^2 \text{ che manda } [z]\mapsto(\wp(z){:}\wp'(z){:}1)$$

è un'immersione olomorfa del toro complesso T in $\mathbb{P}^2$ *che ha per immagine la curva ellittica di equazione* $Y^2Z=4X^3+AXZ^2+BZ^3$.

Allora una curva ellittica è isomorfa ad un toro complesso. Riassumendo dopo aver dato la definizione di varietà abeliana abbiamo verificato che le curve ellittiche appartengono a questa particolare classe di varietà e abbiamo definito su tali curve una struttura di gruppo algebrico prima dal punto di vista della geometria algebrica e poi usando strumenti dell'analisi complessa. Poi si è introdotto il genere di una curva algebrica, piana e proiettiva. Abbiamo osservato che il genere può essere riguardato attraverso la sua connotazione topologica e che ad una curva ellittica è possibile associare un toro complesso attraverso la teoria delle superfici di Riemann.

DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DI FERRARA, VIA MACHIAVELLI 35, 44100 FERRARA ITALIA

E-mail address: alex.massarenti@student.unife.it