Elliptic Curves / crs of genus 1

- . A lattice / C , N= Ze, &Ze2
- . CA C--- C/A & S'XS' A & R/Z X R/Z S CRS with complex structure depending on 1.

eg: N=an acc*

C must c unique mate C/ a C/N'
by a

This is the only way two mule complex structures on s'xs' can be biholomorphic.

Suppose given $\varphi: \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda'$

we can lift this, to some

ψ: e --- C with ψ (0) = 0. Claim: + 4 (x+) - 4(x) - 4(x) (x) is constant

Assuming this, we get $\psi'(x+\lambda) = \psi'(x) + \# \chi \lambda$

syransam So we get 4 (x=) = ax + b

4(0)=0 gives 4,(0)=b=0 => 4(x)=and

e Now if we are also given that & P is biholo. we will get \$ [\ = a \]

weisteass & function / 6:

 $y(z) = \frac{1}{2} + \sum_{\lambda \in \Lambda - \{n\}} \left(\frac{1}{(z - \lambda)^3} - \frac{1}{\sqrt{2}} \right)$

Doubly periodic: 8(s) = 8(2+2) SEN

8 - meromorphic function on 6/1

· M ((14) = ((8,8;))

Can find e, e, basis for 1 st. 812 = 4 (8-e,) (8-e2) (8 - e1+e2)

.
$$C/\Lambda \stackrel{\sim}{=} E \stackrel{\rightarrow}{=} P^2$$

| projective closure of the affine curve

$$y^2 = 4(x-e_1)(x-e_2)(x-e_2) = \frac{e_1+e_2}{2} \qquad (x-e_1)(x-e_2)(x-e_2) = \frac{e_1+e_2}{2}$$

| $g(x)$ $g(y)$ $g(x+y)$ = 0

| $g(x)$ $g(y)$ $g'(x+y)$ = 0

This gives [8(x); 8'(x)], [8(y): 8'(y)], [8(x+y), 8(x+y)] are colinear! Fantastic.

allows to teamslate the group structure of C/n to the usual group structure transditionally done given on elliptic curves.

· Any son non-singular cubic curve can be put in the form of (*).

Having done that we get a way offer getting from em elliptic curve to the complex toxus.

of be curved on E, I corresponding on C/A

$$\int \frac{d\pi}{dy} = \int \frac{d}{dy} \frac{\phi(z)}{(z)} dz = \Gamma(b) - \Gamma(a)$$

If 17 begins at 0 (indentification with complex plane ()

Div (x) = set of divisors

Divo(x):= deg 0

Pico(x):= Divo(x)

Divisors coming from m (x) (zeroes & polus) **不(x)**

Jacobi.

Pic

· Abel Jacobi:

Ingeneral, Pico (M29) is a torus of genus g. with lot more structure.

NN lattices in a set. and set. and section as cas then I accome Jemma: such that N=an.

Hence we have a majo

{ Nathices in () < - > Compad R.S. of genus 1

upper enouth / SI2(Z) was This space is inferent a non-compact Riemann Surface I holomorphic J: It/SI(2,72) - C bijective plane

(becomes moduli space for from Complex Toril

Weirstrass 8-function:

1 lattice in C,

Zemma: ∑ 1 1w13 < ∞

Proof: (w, w) be bosh for 1

det P= {4w,+ Bcox | x,B>0, 4+B=1} U {xw,+ Bw2 | x,B>0 , x+13=1}

LHS = $\sum_{|n+m_1|=n} \frac{1}{|n_1\omega_1+n_2\omega_2|^3}$

 $= \sum_{N=1}^{\infty} \sum_{|m_1|+|m_2|=N} \frac{n^3}{\left|\frac{n_1}{N},\omega_1+\frac{n_2}{N},\omega_2\right|}$ This EP

 $\leq \sum_{n=1}^{\infty} \frac{K}{n^3}$ for appropriate constant K

$$\Psi(\omega) := \frac{1}{Z^2} + \sum_{\omega \neq 0} \left[\frac{1}{(Z-\omega)^2} + \frac{1}{\omega^2} \right]$$

$$\omega \in \Lambda$$

&(w) converges uniformly on compact subsets of C-A.

Proof: De:= {z: |z|<5}

· if Iwle 29 and ZEDs then -> 121 < 1 and 12-61 > 121

For E compact, suppose E = Dg, then

For ZEE, IWI>29 we get

 $\left|\frac{1}{(2-\omega)^2} + \frac{1}{\omega^2}\right| \leq \frac{10 \, \mathrm{g}}{1\omega 1^3}$

Since \(\sum_{1\omega]3} < \approx \tag{and} \) and there are only finite lattice points inside & Dag we are done.

→ Let uc open, Ifn3 seq of holomorphic functions on U, converging uniformly on compact subsets of U

Note: For a locally compact space, fr-of uniformly on compact subsets iff it converges locally uniformly.

1 be a closed path in a a disc in U,

$$\left| \int_{\Gamma} (f_n - f) dz \right| \leq \left| \int_{\Gamma} (|f_n|^2 - \xi f|^2) (dz) \right|$$

$$\leq \sup_{z \in \Gamma} |f_n - f|(z)| \cdot \operatorname{length}(\Gamma)$$

< E for n> N does not depend on z because of uniform convergence

Hence, If dz = lim fn dz = 0

f is holomorphic (because f haves a primitive if it is o on every closed loop) For sufficiently small circles C, we have for $z \in interior of C$ $|f_n'(z) - f'(z)| = \left|\frac{1}{2\pi i} \int_{z=0}^{\infty} \frac{f(z) + f(z)}{(z_0 - z)^2} d\omega\right|$ $\leq K \sup |f_n(\omega) - f(z)|$ $z \in C$

=> fn - f' uniformly on Binterior of C, hence uniformly locally.

Applying this to \$1(2) gives,

Th^m: g(z) is holomorphic add on $C \setminus \Lambda$ g(z) = term by term differentiation of series of g(z)= $-2\sum_{\omega \in \Lambda} \frac{1}{(z-\omega)^2}$

y(z) = y(-z), y'(z) = -y'(-z)

2) $\wp'(z+\omega) = \wp'(z)$

3) $\beta(z+\omega) = \beta(z)$ [ook of $(\beta(z+\omega) - \beta(z))'$ =) $\beta(z+\omega) - \beta(z) = c(\omega)$ Set $z=-\frac{\omega}{2} \Rightarrow \beta(\frac{\omega}{2}) - \beta(-\frac{\omega}{2}) = c(\omega)$

= \$, p' meromorphic on C/A

and this is the only pole in C/N

=) [M(S(1) M(S(1))] = 2

5) $8^{3}(z) \neq -8^{3}(-2)$ $\Rightarrow 8^{3}(z) \notin C(z) \longrightarrow M(6/h)$ $\Rightarrow M(6/h) = C(2), 8^{3}$ and 8^{3} satisfies a quadratic in 8^{3} .

6) Sp'EM(EK) has bole of order 3 at OEGA & no other

For
$$\omega \in \Lambda$$

$$\varphi^{*}(z+\omega) = \beta(z)$$

$$\Rightarrow \qquad \varphi^{*}(\underline{\omega}) = - \varphi(\underline{\omega})$$

=) 8(\omega)=0

r

in particular 8 hos zeroes 21, 45 w, w2, w1+w2

Hence, 8' has exactly there 3 zeroes. In C/A and each 0 is a simple 0.

Let $e_1 = \beta\left(\frac{\omega_1}{2}\right)$, $e_2 = \beta\left(\frac{\omega_2}{2}\right)$, $e_3 = \beta\left(\frac{\omega_1 + \omega_2}{2}\right)$

Then there are distinct

Because \$\beta(z) - e_1\$ and \$\beta'(z)\$ are \$\text{0}\$ at \$\frac{\omega}{2}\$

So that \$\frac{\omega}{2}\$, is dero of order 2

and hence \$\beta(z) - e_1\$ has no other 0.

7) Define fec(8,81) = M(C/N) by

$$f = \frac{\varphi'(z)^2}{(\varphi(z) - e_1) (\varphi(z) - e_2) (\varphi(z) - e_3)}$$

Possible poles: $0, \frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1 + \omega_2}{2}$

By counting orders of vanishing one can find show that f has no poles!

=) f is constant and bood substitution in senies will give f(0)=4

$$y'(z)^2 = 4 (p(z)-e_1)(y(z)-e_2)(y(z)-e_3)$$

fx: Gk := 5 WEN-for wak

Show, $p(z)^2 = 4 p(z)^3 - 140 \cdot G_2 \cdot p(z) - 60 G_3$.

. A be a lattice $\overline{Z}\omega$, $\overline{\omega}\overline{Z}\omega_2$ $\underline{S}(z) = \frac{1}{22} + \sum_{\omega \in \Lambda \setminus \{0\}} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right]$ we have shown,

-> P is uniformly convergent on compact subsect of

$$\frac{1}{\omega} \Rightarrow \{ g'(z) = -2 \sum_{\omega \in \Lambda} \frac{1}{(z - \omega)^3} \\
\rightarrow \{ g'(z)^2 = 4 p(z)^3 - g_1 g(z) - g_3 \\
\rightarrow \{ g'(z)^2 = 4 (g(z) - e_1) (g(z) - e_2) (g(z) - e_3) \\
e_1 = \{ g(\underline{\omega}_1) = e_2 = \{ g(\underline{\omega}_2) = e_3 = \{ g(\underline{\omega}_1 + \omega_2) = e_1 \} \} \\
\rightarrow \underbrace{m}_{1} (g/_{\Lambda}) = \{ (g/_{\Lambda})^{g'} \}$$

E be affine curve given by y= 4(x-e)(x-e)(x-e) · Let E be its projective closure.

Claim: E is a smooth projective curve.

$$-\frac{3}{3y} = 0 \Rightarrow y = 0 \Rightarrow x = e_1 \text{ or } e_2 \text{ or } e_3$$
at any $\frac{3}{3x} \neq 0$ as e_i 's are distinct:

. At as , i.e. 0 = 423 solution is [0;1:0]

Emough to check Z= 4(x-e,z) (x-e,z) (x-e,z) has non-zero gradient is at (0,0) ??

· By implicit function thm, E 1-dim complex manifold, compact

TFAE:

1) E is connected

3) E = Q m (c//)

1) If p(a) = g(b) and p'(a) = g'(b), then a= b S. 8,8' soperate points.

3) => 1) ... R(x) is connected for any function field F 2) =) 2) Look at the diagram. $E \rightarrow E$ fibre ~~ 8 fibre cardinality 2

It is well known that (Shafarevich | by 321)
Here is a different proof;

$$\varphi \longrightarrow \& (\&,\&,)$$

$$\varphi \longrightarrow \& \& (c/V)$$

$$C[\emptyset,\emptyset'] = \frac{C[x,y]}{y^2 - 4(x-e_1)(x-e_2)(x-e_3)}$$

A point $(x_0,y_0) \in E$ corresponds to a maximal ideal of $C[\beta,\beta']$ By localizing at a dur, = $\left\{\frac{f(\beta,\beta')}{g(\beta,\beta')} \mid g(x_0,y_0) \neq 0\right\}$

This dur is a member of RM(Ch) and maps to (x_0, y_0) in £ under $(P_*, 8_*)$, So $(P_*, 8_*)$ is surjective. Since RM(Ch) is connected, £ is connected a we have £ is connected.

· Addition Theorem: Via up, E acquires the structure of an abelian group (£ ≤ 1P², with addition ⊕) of Elliptic curve

Thm: Suppose P1, p2, p3 EE, Then p1, p2, p3 are colinear iff p10 p20 p3=0

· if $p_1=p_2$, tangent at p_1 meets curve in p_3 · if $p_1=p_2=p_3$ we have boint of inflection

The only point of inflexion is [0:1:0]. The tangent line at [0:1:0] is the line at ∞ .

In terms of P, the addition theorem says for x, y = 4/1 to} (800), 800), (80), 8'0), (800-x-y), 8'(-x-y),

are colinear, Le.

8(x) p(x)

8(x)

9(y)

1 = 0

Here x, y can be thought as

points in C or C/N

Fix $u \neq 0$, Define $g(t):= \begin{cases} g(t) & g'(t) \\ g(u) & g'(u) \end{cases}$ g(t+u) = g(t+u) + g(t

Check that q(f) has poles at amost re=0, t=-4. By expanding p(t), we can check that there is no pole at t=0. And because q(t) = -q(-t-u) q does not have pole at t=-u. \Rightarrow q is constant, $q(u)=0'\Rightarrow q=0$.

·Addition the implies, that the group law on E is given by rational functions. (a, l'), (B,B'), (7,7') colinear

 $\Rightarrow \forall = -d - \beta + \frac{1}{4} \left(\frac{\beta - d}{\beta - d} \right)^2$ =) $8(x+y) = -8(x) - 8(x) + \frac{4}{4} - \left[\frac{8(x) - 8(x)}{8(x) - 8(x)}\right]$

- Every meromorphic function, on C/A satisfies an "addition th" ie. I a polynomial A s.t. A (A(x), A(y), A(x+y))=0.

Abel's theorem for O/A Let f∈ M(C/), f≠0. Let airian be zeroes of f with reportions allowed. Let bi... by be poles. Then,

and ait ... +an = bit... +bn ... (mod A)

Proof of Geometric addition the using Abel's theorem:

L line in 1P2 worksetby + 200

{P,Q,R} = LN E

let u,u,u be boints inside a fundamental parallelopiped grom corn to B.C.R. we need to show POQOR=0

enough to show u+ u+ w = 0 mod 1

Let f be the doubly periodic function, f=xp+ B + x zeroes of f are at u,u, was and poles at o.

By Abol's the we are done.

· Pick a fundamental il such that ais, bis are in the interior

$$a_1 + \dots + a_n - b_1 - \dots - b_n$$

$$= \frac{1}{2\pi i} \int \frac{z f'(z)}{f(z)} dz$$

· Using doubly beridicity

$$\int \frac{zf'(z)}{f(z)} dz = -\int (z+\omega_z) \cdot \frac{f(z)}{f(z)} dz = -\omega_z \int \frac{f'(z)}{f(z)} dz + \int ...$$

So the summation becomes

-
$$(\omega_1)$$
 $\int \frac{xf'(z)}{f(z)} dz$ because evinding no $f(z)$ + ω_1 this should be an integer

ie = Myw2 + now

Divisors:

deg:
$$\Sigma Div(x) \longrightarrow Z$$

 $\Sigma n_i P_i \longmapsto \Sigma n_i$

Dév°X = ker (deg) Subgrip of \$\ Div(x) 2 meromorphic for divisors sit here Principal divisors

$$Pic^{*}(X) = \frac{Div^{*}(X)}{Principal divisors}$$
 $Pic^{*}(X) = \frac{Div^{*}(X)}{Principal divisors}$
 $Pic^{*}(X) = \frac{Div^{*}(X)}{Principal divisors}$

```
i a mab

Ji € Div (C/N) → C/N
  Ch we have a map
                 Ji Ed Div (a/n) -

Enjai Surjective
Abels them => Principal divisors & kerj
So we have an Abel-Jacobi map
   AJ. Picceln - 6/n
Abel Jacobi The: AJ is an isomorphism.
  Geometric addition says
            [a]+[a]+ {-a,-a]}-3.0 is principal
 · Take a, =0 above to get

[a,]+ (-a,] - 2.{0} is principal
   Lemma: {a3+fa3+...+fan3+ n=0 (-a,-a2...-an) - (n+1)fof= a. In Dix Principal
   Proof:
           n=1, $2 as above
            n>3
                (a1+...+an-1+ (-a1-...-an-1) - n.0)
                   -(a_1+\cdots+a_{N-1}) - (-a_1-\cdots-a_N) + 2.0 = 0
   Proposition: Let a,... an bi...bn'EC. Let c= \sum_{i=1}^{n} a_i - \sum_{i=1}^{n} b_i
                    \sum a_i \triangleq \sum b_i = -\sum -a_i + \sum -b_i \qquad \text{in Pic} \quad CC/\Lambda)
                     2) Zai - Zbi = {c3 - 403 in Pic (0/N)
        \Sigma a_i + \Sigma - a_i = - \{\Sigma a_i - \Sigma a_i\} + (n+i) \{0\}
    1)
                   = - {\(\Si\) - \(\Si\) + (n+1) \(\lambda\) = \(\Si\) + \(\Si\) - \(\Si\)
        (-\Sigma_{bi} + \{o\}) - (\{-\Sigma_{ai}\} + \{c\}) = +\{a_i - c\} - \{\Sigma_{bi}\} = 0
                                                                 Ø
```

j. Div ° CEK) ---- CK induces AJ: Pic°CC/h) --- C/h

Abel Jacobi: AJ is an somerphism. principal Proof: Enough to show ke x & kerj >> x principal $x \in \ker j = 1$ $x = \sum ta_i - \sum b_i$

= {c3 - fo} + principal

= principal o + principal Market so x & ker, = c=0 = x eprincipal. en de la companya de la co

D= {b}-fo}. Suppose D were principal ithen ramification Example: degree would be 1. Making Riemann surface isomosphic to EIP.

Comment of the market want

((x) := { f ∈ \(\frac{1}{2}\) (x) / f ≠ 0, (f) + D ≥ 0 } u f o }. · Effective divisor:= D= Enibi s.t. nizo Vi : Equivalence D~D' if D-D'= principal divisor والمتعاقف والإنهاز المحارف والمعادية ويرار كالمعا

Riemann:

dim L(D) = deg D + 1- g

Riemann-Roch:

dim L(D) - dim &L(K-D) = deg D+ 1-3. K= "canonical divisor"

X = (1), dim x (x-0) = 9 the almays

because degree of a comprised divisor is /20-2. dim L(D) = 10 dep = 0

deg D ≤0 => dim L(D) = 0

deg D = 0 = f ∈ (D) => (f) + D ≥ 0 deg((f)+D)=0 $\Rightarrow (f)+D=0$

a D principal

(b) = C' if D principal = o else