Elliptic Curves

Elliptic curves have equations of the form $w^2 = z^3 + az + b$. For concreteness, we look at

$$\mathbb{E} = \left\{ \ (z, w) \in \mathbb{C}^2 \ \middle| \ w^2 = z^3 - z \ \right\}$$

Let

$$\begin{aligned} \zeta : \quad & \mathbb{E} \to \mathbb{C} & \qquad\qquad \omega : \quad & \mathbb{E} \to \mathbb{C} \\ & (z, w) \mapsto z & & (z, w) \mapsto w \end{aligned}$$

be the projections from $\mathbb{E}$ onto the z and w axes, respectively. We shall often rewrite $z^3 - z = z^2\big(z - \frac{1}{z}\big)$ and use

Lemma.

$$\begin{aligned} z - \tfrac{1}{z} \le 0 \quad &\iff \quad z \le -1 \quad \textit{or} \quad 0 \le z \le 1 \\ z - \tfrac{1}{z} \ge 0 \quad &\iff \quad z \ge 1 \quad \textit{or} \quad -1 \le z \le 0 \end{aligned}$$

The inequality $z \le 0$ means that z is real and the real part of z is less than or equal to zero.

Proof: Write $z = re^{i\theta}$. Then $\operatorname{Im} z = r \sin\theta$ and $\operatorname{Im} \frac{1}{z} = -\frac{1}{r}\sin\theta$. Hence the $\operatorname{Im}\big(z - \frac{1}{z}\big) = \big(r + \frac{1}{r}\big)\sin\theta$ and this vanishes if and only if $\sin\theta = 0$, or equivalently, if and only if z is real. Now walk allong the real axis, starting form $-\infty$. Then $z - \frac{1}{z} = \frac{1}{z}(z-1)(z+1)$ starts negative and changes sign first at $z = -1$, then at $z = 0$ and finally at $z = 1$. ■

Define

$$\begin{aligned} D_R &= \mathbb{C} \setminus \left\{ \ z \in \mathbb{C} \ \middle| \ z \le -1 \text{ or } 0 \le z \le 1 \ \right\} \\ D_I &= \mathbb{C} \setminus \left\{ \ z \in \mathbb{C} \ \middle| \ z \ge 1 \text{ or } \ -1 \le z \le 0 \ \right\} \end{aligned}$$

By the lemma $z - \frac{1}{z}$ maps D_R into $\mathbb{C} \setminus \left\{ \ z \in \mathbb{C} \ \middle| \ z \le 0 \ \right\}$, which is the domain of the unique analytic square root function that always takes values with strictly positive real parts. Similarly $z - \frac{1}{z}$ maps D_I into $\mathbb{C} \setminus \left\{ \ z \in \mathbb{C} \ \middle| \ z \ge 0 \ \right\}$, which is the domain of the unique analytic square root function that always takes values with strictly positive imaginary parts. Thus there are unique analytic functions

$$\begin{aligned} S_R : D_R \to \mathbb{C} \quad & \text{with } S_R(z)^2 = z - \tfrac{1}{z} \quad \operatorname{Re} S_R(z) > 0 \\ S_I : D_I \to \mathbb{C} \quad & \text{with } S_I(z)^2 = z - \tfrac{1}{z} \quad \operatorname{Im} S_I(z) > 0 \end{aligned}$$

Define

$$\begin{aligned}
\mathbb{E}_R^+ &= \left\{ \ (z,w)\in\mathbb{C}^2 \ \middle|\ z\in D_R,\ \ w = zS_R(z) \ \right\} \\
\mathbb{E}_R^- &= \left\{ \ (z,w)\in\mathbb{C}^2 \ \middle|\ z\in D_R,\ \ w = -zS_R(z) \ \right\} \\
\mathbb{E}_I^+ &= \left\{ \ (z,w)\in\mathbb{C}^2 \ \middle|\ z\in D_I,\ \ w = zS_I(z) \ \right\} \\
\mathbb{E}_I^- &= \left\{ \ (z,w)\in\mathbb{C}^2 \ \middle|\ z\in D_I,\ \ w = -zS_I(z) \ \right\}
\end{aligned}$$

Then $\{\mathbb{E}_R^+,\zeta\}$ and $\{\mathbb{E}_R^-,\zeta\}$ are disjoint patches that cover all (z,w)'s except those with $z\le -1$ or $0\le z\le 1$. Similarly, $\{\mathbb{E}_I^+,\zeta\}$ and $\{\mathbb{E}_I^-,\zeta\}$ are disjoint patches that cover all (z,w)'s except those with $z\ge 1$ or $-1\le z\le 0$. So far all of $\mathbb{E}$ is covered except for $(0,0)$, $(1,0)$ and $(-1,0)$. So far, compatibility is trivial, since $\zeta\circ\zeta^{-1}$ is the identity map.

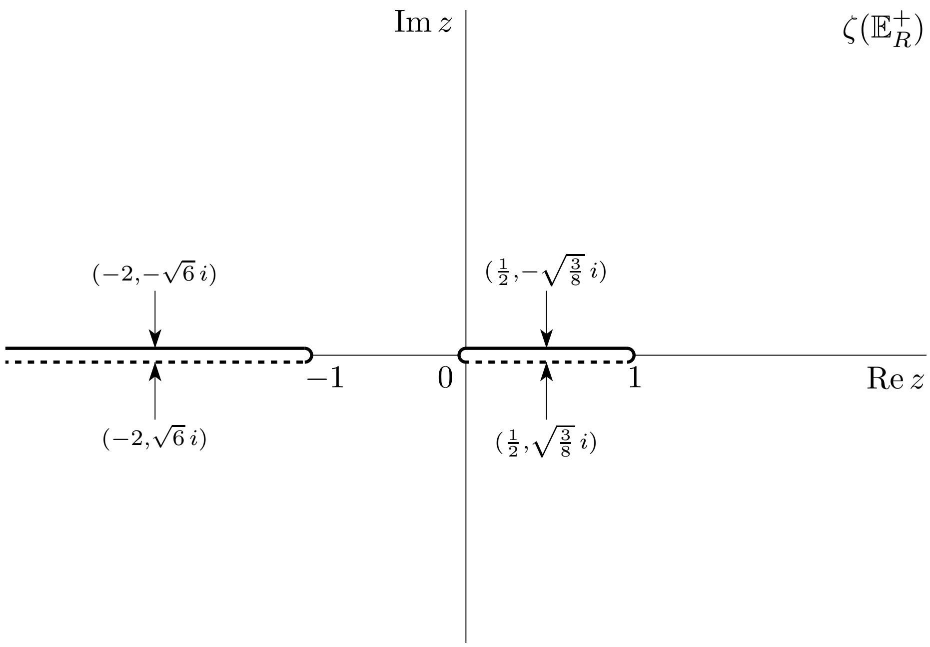
Let $f(z)=z^3-z$, $z_0=0$, $z_1=1$ and $z_2=2$. Then for $i=0,1,2$, $f(z_i)=0$ and $f'(z_i)=3z_i^2-1\ne 0$. Consequently, there is a small neighbourhood B_i of z_i such that $f(z)$ is 1–1 on B_i with analytic inverse, $f_i^{-1}(w)$ on $f(B_i)$. Note that $0\in f(B_i)$ and $f_i^{-1}(0)=z_i$. Define

$$\mathbb{E}_i = \left\{ \ (z,w)\in\mathbb{C}^2 \ \middle|\ w^2\in f(B_i),\ \ z=f_i^{-1}(w^2) \ \right\}$$

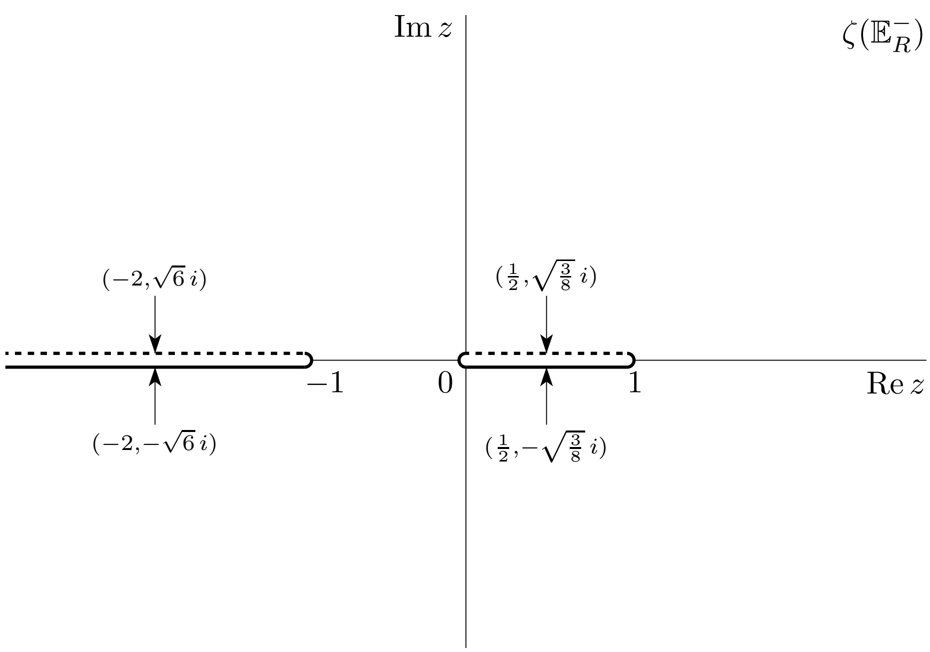
Note that $(z_i,0)\in\mathbb{E}_i$ and that $\mathbb{E}_i\subset\mathbb{E}$ since, if $(z,w)\in\mathbb{E}_i$, $f(z)=f\big(f_i^{-1}(w^2)\big)=w^2$. Then the four previously defined patches, together with $\{\mathbb{E}_i,\omega\}$, $i=0,1,2$ provide an atlas for $\mathbb{E}$. To check the compatibility of $\{\mathbb{E}_i,\omega\}$ and, for example, $\{\mathbb{E}_R^+,\zeta\}$, it suffices to observe that

$$\begin{aligned}
\zeta\circ\omega^{-1}(w) &= \zeta\big((f_i^{-1}(w^2),w)\big) = f_i^{-1}(w^2) \\
\omega\circ\zeta^{-1}(z) &= \omega\big((z,zS_R(z))\big) \quad = zS_R(z)
\end{aligned}$$

are analytic.



Im z
$\zeta(\mathbb{E}_R^+)$
$(-2,-\sqrt{6}\,i)$
$(\frac{1}{2},-\sqrt{\frac{3}{8}}\,i)$
-1
0
1
Re z
$(-2,\sqrt{6}\,i)$
$(\frac{1}{2},\sqrt{\frac{3}{8}}\,i)$



Im z
$\zeta(\mathbb{E}_R^-)$
$(-2,\sqrt{6}\,i)$
$(\frac{1}{2},\sqrt{\frac{3}{8}}\,i)$
-1
0
1
Re z
$(-2,-\sqrt{6}\,i)$
$(\frac{1}{2},-\sqrt{\frac{3}{8}}\,i)$