Elliptic Functions with Simple Symmetries and Fast Addition Formulas

H. Karcher, Bonn

Any two elliptic functions f, g of degree 2 differ only by a torus translation T and a Möbius transformation M, i.e. $g = M \circ f \circ T$. So, how can a particular function be special and how can one speak of "new" functions? There are two reasons. First, elliptic functions are always considered as depending also on the torus, and the moduli space of tori is not simply connected. In fact, a key advantage of the Weierstraß $\wp$-function is that it is well-defined also on the moduli space, since its definition involves only the lattice, and not further choices, like a lattice basis. Secondly, away from their branch points, elliptic functions are coordinates on the torus and one needs at least two functions to have an atlas. In the case of the Weierstraß $\wp$-function one takes $\wp'$ as the other function. The differential equation $\wp'^2 = 4\wp^3 - g_2\wp - g_3$ can then be viewed as describing the coordinate change between the two coordinate functions or also as a parametrization of the solution set of the equation $z_2^2 = 4z_1^3 - g_2 z_1 - g3$; this solution set is called (the Weierstraß normal form of) an "elliptic curve".

Why could one be dissatisfied with the Weierstraß $\wp$-function ? In my work on minimal surfaces I needed functions which treat $0, \infty$ in a symmetric way (like the rational function $z \to z + 1/z$), but only on the square torus is 0 a branch value of $\wp$. Also, with each elliptic function of degree 2 there is associated a Möbius subgroup of order 4 with the following property: let I be an orientation preserving involution of the torus that has fixed points and that permutes the branch points of the elliptic function f (these I form a group of order 4); then there is a Möbius transformation M such that $f \circ I = M \circ f$. I needed this Möbius subgroup to be a group of isometries of the Riemann sphere. For all the functions presented below this Möbius subgroup is the group of 180°-degree rotations around the three coordinate axis, or, using the identification $\mathbb{S}^2 = \mathbb{C} \cup \{\infty\}$, $z \to \pm z, \pm 1/z$. It turned out that there are three functions with all the properties I needed; they will be called u, v, w in this paper (and they are the functions which were called $J_D,\ J_F,\ J_E$ in [HKW]). These three functions are not as invariant as the Weierstraß $\wp$-function, but they only get permuted under lattice basis changes; as a triple they are therefore invariantly attached to the torus. They have surprisingly simple algebraic properties, for example they satisfy cubic equations which are very symmetric with respect to the three functions, namely:

$$w - \frac{1}{w} = -\sqrt{1-\lambda}\,(u - \frac{1}{u}),\ \ \sqrt{1-\lambda}\,(u + \frac{1}{u}) = \sqrt{-\lambda}\,(v + \frac{1}{v}),\ \ w + \frac{1}{w} = \sqrt{-\lambda}\,(v - \frac{1}{v}).$$

This symmetry in the variables leads to simple duplication and addition formulas which give $(u, v, w)(c + z)$ and $(u, v, w)(2z)$ as rational expressions in $(u, v, w)(c)$ and $(u, v, w)(z)$. In our case they do not depend on the torus (but do so for the Weierstraß $\wp$-function), for

example:

$$\text{Addition :} \qquad (a,c)\oplus(u,w) = \left(\frac{a+u}{1+au}\cdot\frac{1+cw}{1-cw},\ \frac{c+w}{1+cw}\cdot\frac{1+au}{1-au}\right).$$

$$\text{Duplication :} \quad 2\odot(u,v) := (u,v)\oplus(u,v) = \left(\frac{2u}{u^2-1}\cdot\frac{v^2-1}{v^2+1},\ \frac{2v}{v^2-1}\cdot\frac{u^2-1}{u^2+1}\right),$$

One aspect of their simplicity is explained in [Chud]: Some cryptographic computations depend on the $\mathbb{Z}$-module structure which these addition formulas give to elliptic curves over finite fields. The addition formulas of our functions u, v, w perform faster than all the elliptic curves considered in [Chud] (and the Weierstraß $\wp$-function is at the end of the list). A slightly different duplication formula allows to compute the preimage, $1/2\odot(u,v)$, of duplication if two square roots (depending on u, v) exist in the field.
And it is also nice that the symmetries of u, v, w allow to derive the above formulas almost without computation, essentially by looking at divisor tables.
Acknowledgement. I thank S. Lang, G. Cornelissen, D. Zagier and R.S. Palais for patiently answering my questions and for helping me focus my explanations.

Two Constructions

For minimal surface applications the symmetries of the functions were most important, therefore they are constructed in [HKW] from that point of view; I give a summary of that construction first. It is one goal of the present paper to make the connection with the standard theory of elliptic functions as short as possible and I hope this will be achieved when I define u, v, w in terms of the Weierstraß $\wp$-function after the geometric construction. Notice the following conceptual difference between the approaches: The geometric construction assumes a complex torus $\mathbb{C}/\Gamma$ as given and it produces conformal maps u, v, w to the Riemann sphere and derives algebraic equations between these maps and ordinary differential equations for them. The algebraic approach assumes a cubic equation as given, the solution set is made into a Riemann surface with two meromorphic functions on it, from these a holomorphic form can be defined whose integral produces a lattice torus $\mathbb{C}/\Gamma$, biholomorphic to the solution set.

I start with the **geometric construction** of section 3 of [HKW] because it emphasizes the global mapping behaviour of the functions: every 180°-rotation of $\mathbb{C}$ decends to an involution I of any torus $T^2 := \mathbb{C}/\Gamma$, where Γ is a lattice in $\mathbb{C}$. Since I has four fixed points on T^2, the quotient T^2/I is a sphere, i.e. biholomorphic to the Riemann sphere $\mathbb{S}^2$. Metrically this quotient map is very elementary: represent the torus $\mathbb{C}/\Gamma$ by a parallelogram fundamental domain (opposite edges identified) with the midpoint being one of the fixed points of I; cut the parallelogram by the shorter diagonal in two and observe that each half is a fundamental domain for I, and that this domain is made into a tetrahedron by the identifications (cut this triangular fundamental domain into four triangles which

are similar to it, note that the total angle at each vertex is $2\pi/2$). The identification between T^2/I and $\mathbb{S}^2$ becomes unique if we specify three points in T^2/I as the preimages of $0, 1, \infty \in \mathbb{S}^2 = \mathbb{C} \cup \{\infty\}$. In other words, such a specification turns the quotient map $T^2 \to T^2/I$ into a meromorphic function $T^2 \to \mathbb{C} \cup \{\infty\}$. There are three other orientation preserving involutions I_1, I_2, I_3 of T^2, each with four fixed points and each permuting the fixed points of I. The fixed points of each of these other three involutions I_j are four of the twelve midpoints between the fixed points of I, see the first of the following diagrams. These twelve midpoints have six image points in the quotient T^2/I and under the identification with $\mathbb{S}^2$ we can send three of these six points to $0, \infty, +1 \in \mathbb{S}^2$. In this way the quotient map is made into a function $J : T^2 \to \mathbb{S}^2$ with the following

$$\text{Symmetries :} \qquad J(I_1(z)) = -J(z),\ J(I_2(z)) = 1/J(z),\ J(I_3(z)) = -1/J(z).$$

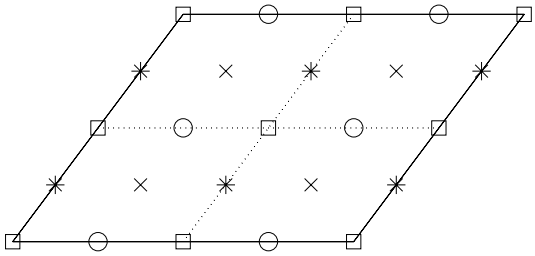
In [HKW] we construct three such functions $J = u, v, w$ by making three choices for the involution I. In the first diagram the fixed points of these three involutions are marked $\times, \circ$ resp. $*$. In each of the three cases take the midpoint of the parallelogram as one preimage of $0 \in \mathbb{S}^2$ and also choose this point as the origin of the the torus group (notation: O, or $z = 0$). The other preimage of 0 is of course $I(O)$, a 2-division point (these are defined by the condition $2 \odot P := P \oplus P = 0$). As the two preimages of $\infty \in \mathbb{S}^2$ we take the other two 2-division points, see the next three diagrams which show the divisors of the functions u, v, w. To make the identification between T^2/I and $\mathbb{S}^2$ unique, we have to choose the preimage of $1 \in \mathbb{S}^2$, we take a pair of the remaining 4-division points as in the diagrams. (This choice is not quite unique, see below.) Clearly, the three functions are odd with respect to the origin (and also with respect to the 2-division points), therefore the preimage of -1 is implied. The remaining special values $\pm i \in \mathbb{S}^2$ are assumed at the remaining 4-division points, because the involution (=: I_3) with these fixed points interchanges the preimages of 0 and ∞ and also the preimages of $+1$ and -1 so that the three functions u, v, w satisfy $J(I_3(z)) = -1/J(z)$ and must have the values $\pm i$ at the four fixed points of I_3.
This abstract construction is very close to computational ones. Observe that each of the logarithmic derivatives $u'/u, v'/v, w'/w$ has the same divisor as two of the functions $J \pm 1/J$. The constant is determined since the logarithmic derivatives at the origin $z = 0$ have the residue $+1$. Therefore the following diagrams with the special values of u, v, w imply immediately a very symmetric system of first order ODEs and simultanously cubic equations for each pair of these functions; note that these *cubics are of degree 2 in each variable*:

$$\begin{aligned}
\frac{u'}{u} &= v'(0)\left(\frac{1}{v} - v\right) = w'(0)\left(\frac{1}{w} + w\right) \\
\frac{v'}{v} &= w'(0)\left(\frac{1}{w} - w\right) = u'(0)\left(\frac{1}{u} - u\right) \\
\frac{w'}{w} &= u'(0)\left(\frac{1}{u} + u\right) = v'(0)\left(\frac{1}{v} + v\right).
\end{aligned}$$

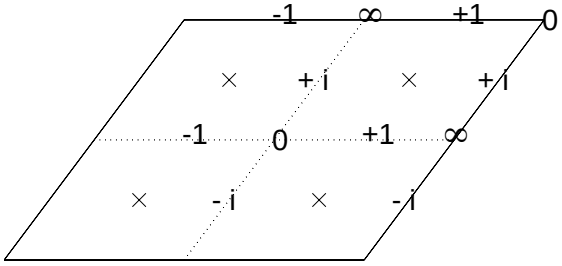
These imply first order differential equations for each function, e.g.

$$\left(\frac{u'}{u}\right)^2 = v'(0)^2\left((\frac{1}{v}+v)^2-4\right) = u'(0)^2\left(\frac{1}{u}+u\right)^2 - 4v'(0)^2.$$

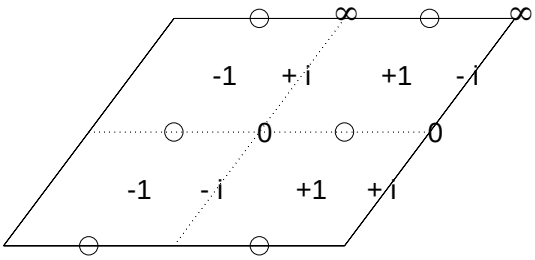
These have the same form $J'^2 = J'(0)^2\left(J^4+1-m\cdot J^2\right)$ as for the Jacobi elliptic functions.



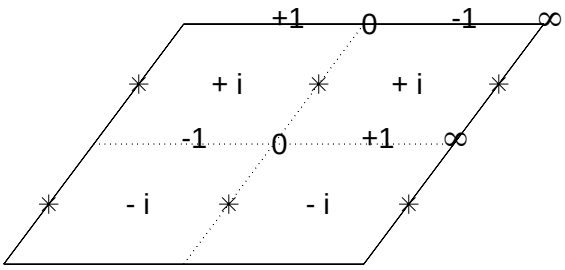
The fixed point sets of four related involutions are midpoints of each other.



Branchpoints ($\times$), divisor and other special values of the function u.



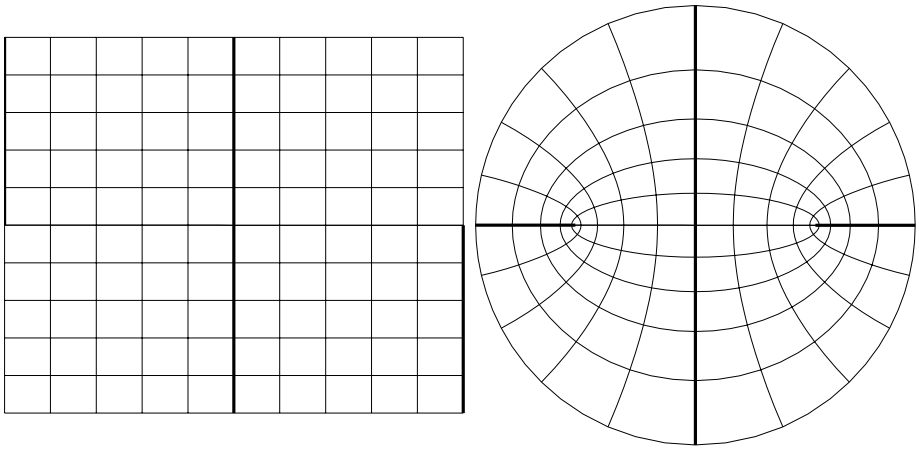
Branchpoints ($\circ$), divisor and other special values of the function v.



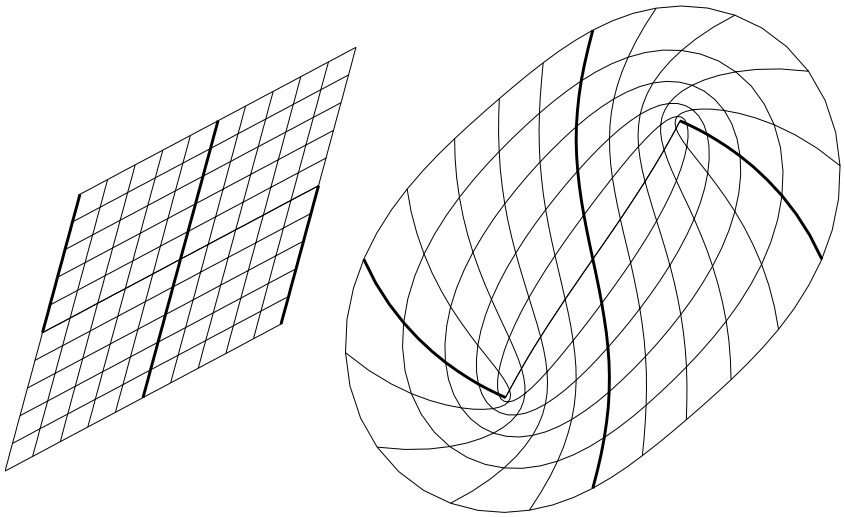
Branchpoints ($*$), divisor and other special values of the function w.

The functions u, v, w resemble the Jacobi elliptic functions sn, cn, dn. Defined as quotients of theta functions these are only well defined for sublattices of index 2. All three are well defined for the sublattice $2\cdot\Gamma$ of index 4, but on the quotient $\mathbb{C}/2\cdot\Gamma$ these elliptic functions are of degree 4, not 2. Also, I have not seen the multiplicative normalization chosen to have simple symmetries and therefore simple values at the 4-division points.

The following diagrams show the mapping properties of the function v on a domain that covers one quarter of a rectangular torus, resp. a parallelogram torus. The remaining values are obtained with the symmetries.



The function v maps one quarter of a rectangular torus to the unit disc.
The parameter lines in the image are two orthogonal families of confocal spherical ellipses (ellipses and hyperbolae are not different on the sphere, one only has to change one focal point to its antipode to go from constant sum of distances to constant difference). The branch values of v are the focal points and the antipodes of the foci.
The thick lines from the branch values to ± 1 are slits in the image domain, also in the image below.



The function v of a parallelogram torus maps one quarter of it to one half of $\mathbb{S}^2$.
This image domain is congruent to its complement under $z \mapsto 1/z$.

These geometrically constructed functions u, v, w of course must be expressible in terms of the Weierstraß $\wp$-function and its derivative. This allows to give an **algebraic construction** for them (which I find more difficult to motivate than the geometric one), and known properties of the Weierstraß $\wp$-function translate into the mentioned cubic equations for u, v, w. Recall that the λ-invariant is the cross ratio of the branch values of *any* degree 2 elliptic function (on the *same* torus), i.e. $\lambda = (e_3 - e_1)/(e_2 - e_1)$ if one works with the Weierstraß $\wp$-function. In much of the study of cubic equations it is

common to break the invariance of the Weierstraß $\wp$-function and to define two functions $x := (\wp - e_1)/(e_2 - e_1)$, $y := const \cdot \wp'$ that satisfy the simpler cubic equation $y^2 = x(x-1)(x-\lambda)$. Since the cross ratio assumes six different values if one permutes its four arguments, it is not correct that $\lambda \in \mathbb{S}^2 \setminus \{0, 1, \infty\}$ is the modular invariant of tori. But almost, it is the invariant of tori with marked 2-division points. The corresponding group is the congruence subgroup $\Gamma(2) \subset \mathrm{SL}(2, \mathbb{Z})$; the quotient of the upper halfplane by this group is covered by six of the fundamental domains of $\mathrm{SL}(2, \mathbb{Z})$, it is a three punctured sphere with its complete hyperbolic metric.
Over $\mathbb{C}$ the constant in $y := const \cdot \wp'$ is irrelevant since it can be chosen by scaling the size of the domain: $\wp(z) \to \wp(const \cdot z)$. In fields of other characteristic one does not have this possibility since one only works with the solution set of the cubic equation. If the field is not algebraically closed then the cubic curves $y^2 = x(x-1)(x-\lambda)$ and $d \cdot y^2 = x(x-1)(x-\lambda)$ are only equivalent if $\sqrt{d}$ is in the field in question. I think the following will be clear enough if I start from $y^2 = x(x-1)(x-\lambda)$, not from $\wp, \wp'$. In the geometric construction (summarized above) the 4-division points play an important role, therefore I assume that $i = \sqrt{-1}$ is in the field under consideration. Moreover, to get the symmetries that were emphasized above, I need $\sqrt{\lambda}, \sqrt{1-\lambda}$ in the field (this means that the square root of the cross ratios of the branch values in any order, i.e. $\sqrt{\{\lambda, 1/\lambda, 1-\lambda, 1/(1-\lambda), 1-1/\lambda, \lambda/(\lambda-1)\}}$, are in the field). The signs of these square roots require further choices which are not preserved by the group $\Gamma(2)$ but are invariant under $\Gamma(4)$. I hope this is enough to orient the reader. I now return to the complex numbers, having stated what is required if one wants to consider the resulting cubics over other (in particular finite) fields.

First I define from x and y three functions q_0, q_1 and q_λ of degree two whose simple zeros and poles are at the four branch points of x or $\wp$, as in the geometric construction above. The branch points of any two of these functions are disjoint, therefore any pair is an atlas for the torus.

Definition and relations with x, y :

$$q_0 := \frac{y}{x},\ q_1 := \frac{y}{x-1},\ q_\lambda := \frac{y}{x-\lambda},$$
$$q_1 \cdot q_\lambda = x,\ q_0 \cdot q_\lambda = x-1,\ q_0 \cdot q_1 = x-\lambda,\ q_0 \cdot q_1 \cdot q_\lambda = y.$$

Taking differences between the second line equations gives:

$$q_0 \cdot (q_1 - q_\lambda) = 1-\lambda, \quad q_1 \cdot (q_\lambda - q_0) = \lambda, \quad q_\lambda \cdot (q_0 - q_1) = -1,$$
$$q_1 - \frac{\lambda}{q_1} = q_0 + \frac{1-\lambda}{q_0},\ q_\lambda - \frac{1}{q_\lambda} = q_0 - \frac{1-\lambda}{q_0},\ q_\lambda + \frac{1}{q_\lambda} = q_1 + \frac{\lambda}{q_1}.$$

The first line shows that any two of the functions and the inverse of the third satisfy a linear relation. The second line gives cubic equations between any two of these degree 2 functions, so that each function can be obtained, by solving a quadratic equation, from any

of the other two. So far we are compatible with the group $\Gamma(2)$. But we need one more multiplicative normalization (not unique because of the sign of the square roots) to obtain the functions with the desired symmetries and the same cubic equations (of degree 2 in each variable) as in the geometric construction.

$$u := \sqrt{1-\lambda}/q_0, \quad v := q_1/\sqrt{-\lambda}, \quad w := q_\lambda,$$

Cubic Equations :

$$\sqrt{-\lambda}\cdot(v+\frac{1}{v}) = \sqrt{1-\lambda}\cdot(u+\frac{1}{u}), \quad (w-\frac{1}{w}) = -\sqrt{1-\lambda}\cdot(u-\frac{1}{u}),$$
$$(w+\frac{1}{w}) = \sqrt{-\lambda}\cdot(v-\frac{1}{v}).$$

COMMENTS. The square torus has $\lambda = -1$, so the factor $\sqrt{-\lambda}$ is real for this torus (and all other rectangular tori). The definition of u proportional to $1/q_0$ makes the functions u, v, w linearly dependent, i.e. we have the

Linear Relation : $$w = \sqrt{-\lambda}\cdot v - \sqrt{1-\lambda}\cdot u.$$

In spite of this linear dependence it is more natural to have all three functions (rather than select two) because the divisor tables show that the *three* functions u, v, w get permuted among themselves if we change the lattice basis and thereby choose a different fundamental parallelogram. Recall that the branch point $x = 0$ was chosen as the *origin* of the torus. Here the three functions u, v, w are 0 and the 2-division points are the only points at infinity, on each of the three cubics. The projective coordinates (t, u, v, w) of the 2-division points are:

$$(0,1,0,-\sqrt{1-\lambda}),\ (0,\sqrt{-\lambda},\sqrt{1-\lambda},0),\ (0,0,1,\sqrt{-\lambda}).$$

In the geometric construction one of the derivatives $u'(0), v'(0), w'(0)$ could be chosen arbitrarily by scaling the domain ($u(const\cdot z)$ instead of $u(z)$ etc.), now we can interprete their quotients by comparing the geometrically and the algebraically derived cubics:

$$v'(0)/u'(0) = \sqrt{-\lambda/(1-\lambda)},\ u'(0)/w'(0) = -\sqrt{1-\lambda},\ v'(0)/w'(0) = -\sqrt{-\lambda}\ .$$

The *symmetries*, which are in the geometric picture simply 180°-rotations, each with four *4-division points* as fixed points, are given by the following formulas (use the linear relation between u, v, w):

$(u,v,w)(-z) = -(u,v,w)(z)$, fixed points: origin and three 2-division points,
fixed values: zeros and poles,

$(u,v,w) \to (1/u, v, 1/w)$, fixed values: $(u=\pm1,\ (w+\sqrt{1-\lambda}\cdot u)/\sqrt{-\lambda}\,,\ w=\pm1)$,
the four branch values of the function v are : $(\pm1+\sqrt{1-\lambda}\cdot(\pm1))/\sqrt{-\lambda}$,

$(u,v,w) \to (u, 1/v, -1/w)$, fixed values: $((-w+\sqrt{\lambda}\cdot v)/\sqrt{1-\lambda}\,,\ v=\pm1,\ w=\pm i\,)$,
the four branch values of the function u are : $(\mp i+\sqrt{\lambda}\cdot(\pm1))/\sqrt{1-\lambda}$,

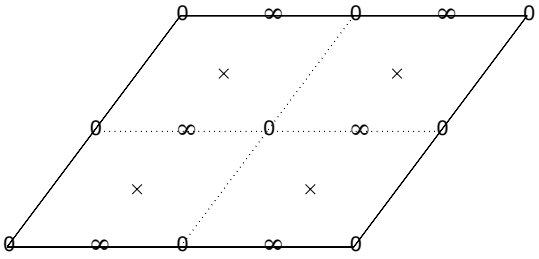
$(u,v,w) \to (-1/u, -1/v, w)$, fixed values: $(u=\pm i\,,\ v=\pm i\,,\ \sqrt{-\lambda}\cdot v-\sqrt{1-\lambda}\cdot u)$,
the four branch values of the function w are : $\sqrt{-\lambda}\cdot(\pm i)-\sqrt{1-\lambda}\cdot(\pm i)$.

Again we see that these functions are well adapted to the subgroup of order 16, generated by the 4-division points.

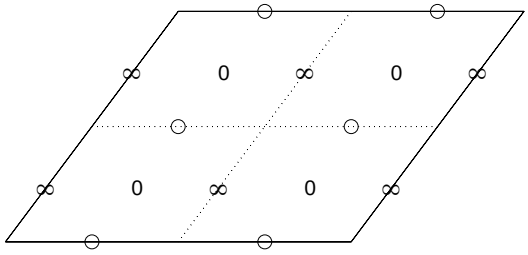
The above linear relation is also responsable for an entertaining picture. Assume we consider tori with marked 2-division points. These are parametrized by (the cross ratio of the branch values) $\lambda \in \mathbb{S}^2 \setminus \{0, 1, \infty\}$. Assume further that we have chosen the signs of the square roots $\sqrt{\{-1, -\lambda, 1-\lambda\}}$ (the preceeding list shows that this marks the 4-division points). Now observe that the coefficients of the linear relation determine the coefficients of the three cubics and vice versa. We map each torus (with the extra structure pointed out) via our functions (u, v, w) into $\mathbb{C}^3$ (or projectively into $\mathbb{C}P^3$), we find the image of each torus in its own projective plane (given by the linear relation). The collection of the occuring projective planes is the moduli space of these structured tori, it is the quadric $\alpha^2 = \beta^2 + \gamma^2$ minus the points which do not occur as coefficients of the linear relation due to the condition that the four branch values of each of u, v, w must be disjoint. Finally, because of the skewsymmetry of the functions we can project each elliptic curve 2-1 to the projective line at infinity; the branchpoints of this projection are the 2-division points. Therefore we can view this map as the Weierstraß $\wp$-function, for all tori simultanuously.

Duplication and Addition

Duplication. Since the functions $z \to u(z), v(z), w(z)$ have one zero at the origin and have the other zero and the two poles at the three 2-division points, it is clear that the degree 8 functions $z \to u(2z), v(2z), w(2z)$ have their (simple) zeros and poles exactly on the group of 4-division points. There the functions u, v, w have the special values $0, \infty, \pm 1, \pm i$ so that we see that the degree 4 functions $u \pm 1/u,\ v \pm 1/v,\ w \pm 1/w$ and their degree 4 quotients $(f + 1/f)/(f - 1/f)$ have their zeros and poles at 8 of the 16 points of the 4-division group, and it follows that the duplication functions $u \circ 2,\ v \circ 2,\ w \circ 2$ (where $u \circ 2(z) := u(2z)$ etc.) are proportional to products of two of them. The factor is determined by the derivatives at the origin $z = 0$. For example the function $u \circ 2$ is the product of the following two functions and thus gives the first duplication formula below (the others are similar):



Branchpoints ($\times$) of u and divisor of the function $2/(u - 1/u)$.



Branchpoints ($\circ$) of v and divisor of the function $(v - 1/v)/(v + 1/v)$.

Duplication formulas:

$$\begin{aligned}
u\circ 2 &= \frac{2u}{u^2-1}\cdot\frac{v^2-1}{v^2+1} = \frac{-2u}{u^2+1}\cdot\frac{w^2+1}{w^2-1}\\
v\circ 2 &= \frac{2v}{v^2-1}\cdot\frac{u^2-1}{u^2+1} = \frac{-2v}{v^2+1}\cdot\frac{w^2-1}{w^2+1}\\
w\circ 2 &= \frac{2w}{w^2-1}\cdot\frac{v^2+1}{v^2-1} = \frac{-2w}{w^2+1}\cdot\frac{u^2+1}{u^2-1}\\
u\circ 2 &= \frac{\sqrt{1-\lambda}}{-1}\cdot\frac{2w}{w^2-1}\cdot\frac{v^2-1}{v^2+1} = \frac{\sqrt{1-\lambda}}{-\sqrt{-\lambda}}\cdot\frac{2v}{v^2+1}\cdot\frac{w^2+1}{w^2-1}.
\end{aligned}$$

Comments. The formulas without the square root factors at first look nicer, but the terms in the last line, for $u\circ 2$, each resemble one of the terms for $v\circ 2$ and one for $w\circ 2$ so that they allow (i) faster computation and (ii) compute **preimages under duplication** if certain square roots exist:

$$(u\circ 2)\cdot(w\circ 2) = \frac{\sqrt{1-\lambda}}{-1}\cdot\left(\frac{2w}{w^2-1}\right)^2, \qquad (u\circ 2)\cdot(v\circ 2) = \frac{\sqrt{1-\lambda}}{\sqrt{-\lambda}}\cdot\left(\frac{2v}{v^2+1}\right)^2.$$

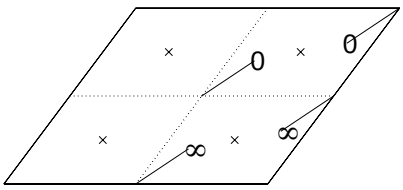
More precisely if one of the four solutions for w has been choosen then u^2, v^2 can be obtained rationally from $w, w\circ 2$ and then u resp. v can be rationally obtained using $u\circ 2$ resp. $v\circ 2$. This is in analogy to $\cos\alpha = \sqrt{(1+\cos 2\alpha)/2}$, $\sin\alpha = \sin 2\alpha/(2\cos\alpha)$.

Addition. A similar strategy works for addition (subtraction). The divisors of the three functions $z\to u(z-s)$, $v(z-s)$, $w(z-s)$ are simply obtained by shifting the divisors of u, v, w. Also, there are 24 Möbius transformations of u, v, w having one zero and one pole correct, and the other pair incorrect. It is then possible to multiply two such functions so that the wrong pair of zero and pole cancels while the others combine to give the desired divisor, i.e., the desired function up to a multiplicative constant. This constant is easily determined at $z=0$. Let f be one of the functions u, v, w. Consider the eight Möbius transformations (with $a := u(s), b := v(s), c := w(s)$ viewed as constants and $f(s)\neq 0$ in the third case):

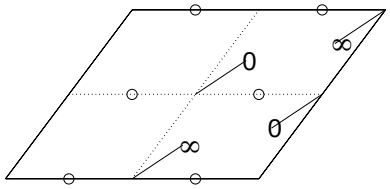
$$\frac{f(z)\pm f(s)}{f(z)\mp f(s)}, \quad \frac{f(z)\pm f(s)}{1\pm f(z)f(s)} \text{ (4 cases)}, \quad \frac{-1\pm f(z)f(s)}{1\pm f(z)f(s)}.$$

The poles of $z\to f(z)$ clearly cancel from numerator and denominator. To see the zeros of numerator and denominator observe the following: If we know one point $s\in T^2$ with $a = u(s)$ then the symmetries from the geometric construction give us **all** the points where u assumes the values $\pm a, \pm 1/a$ and similarly for v, w. Therefore we indeed know the zeros of numerators and denominators of the listed Möbius transforms of u, v, w. For example, the product of the first and third of the following functions has the same divisor (and derivative at $z=0$) as the function $z\mapsto u(z-s)$ and the quotient of the second by the

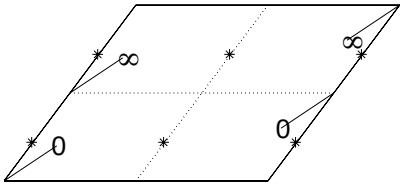
third function has the same divisor as $z \mapsto v(z-s)$. Therefore these diagrams suffice to prove the first two of the subtraction formulas below.



divisor of the function $(u-a)/(1-ua)$.



divisor of the function $(v-b)/(1-vb)$.



divisor of the function $(1-wc)/(1+wc)$.

Case by case check shows: If f is one of u, v, w then each of these 24 Möbius transformations has indeed one zero and one pole in the same location as one of the three wanted functions $z \to u(z-s), v(z-s), w(z-s)$. Moreover, for each case the complementary case (i.e., with the other correct zero and pole and with the cancelling zero pole pair) is also there. This gives a fairly long list of alternative addition formulas of which I only list two for each function. (Recall that (u, v, w) means $(u(z), v(z), w(z))$ and (a, b, c) means $(u(s), v(s), w(s))$:

Subtraction Formulas

$$\begin{pmatrix} u \\ v \\ w \end{pmatrix} \ominus \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} \dfrac{u-a}{1-ua} \cdot \dfrac{1-wc}{1+wc} \\ \dfrac{v-b}{1-vb} \cdot \dfrac{1+wc}{1-wc} \\ \dfrac{w-c}{1-wc} \cdot \dfrac{1-ua}{1+ua} \end{pmatrix} = \begin{pmatrix} \dfrac{v-b}{v+b} \cdot \dfrac{u+a}{1-ua} \\ \dfrac{v-b}{1+vb} \cdot \dfrac{1+ua}{1-ua} \\ \dfrac{v-b}{v+b} \cdot \dfrac{w+c}{1-wc} \end{pmatrix}$$

Comments. These formulas have a rather similar looking trigonometric limit: The graph $\{(x, y = 2x/(x^2+1));\ x \in \mathbb{C}\}$ is a cubic curve that on the one hand is a limit of our cubics, and on the other is parametrized by $x = \tan(z/2),\ y = \sin(z),\ z \in \mathbb{C} \bmod 2\pi\mathbb{Z}$, and the addition formulas for tan and sin give an addition of points on this graph:

$$(x, y) \ominus (a, b) = \big((x-a)/(1+xa),\ y(1-ab) - b(1-xy)\big).$$

After rotation by i, i.e. $x = \tan(iz/2),\ y = \sin(iz)$, one parametrizes the graph $\{(x, y = 2x/(1-x^2));\ x \in \mathbb{C}\}$ and the addtion formulas are

$$(x, y) \ominus (a, b) = \big((x-a)/(1-xa),\ y(1+ab) - b(1+xy)\big).$$

The real part consists ot two copies of $\mathbb{R}$, one through 0, the other through the 2-division point$(\infty, 0)$. They are two opposite straight lines on the cylinder $\mathbb{C} \bmod 2\pi\mathbb{Z}$.

Although the elliptic addition formulas were derived as identities between complex functions, they can now be used, since they have integer coefficients, to define addition on the cubics given by the above equations *over any field*. Associativity holds if we work over $\mathbb{C}$, since the addition formulas only express on the cubic the associative addition in $\mathbb{C}/\Gamma$.

But associativity for our addition formulas is expressed by a polynomial identity that is independent of the field and therefore holds over any field once we know it over $\mathbb{C}$.
Over large finite fields it is much faster to multiply than to divide. Therefore [Chud] propose to compute numerators and denominators of the sum from numerators and denominators of the summands by multiplications alone. They discuss addition on standard cubic equations and their minimum number of multiplications is twelve for one addition on the elliptic curve. With the above addition formulas ten multiplications suffice. For the duplication formulas [Chud] obtain a minimum of eight multiplications; in our duplication formulas eight multiplications also suffice.

Collinearity and Addition. Over fields other than $\mathbb{C}$ one prefers cubic equations over meromorphic maps $\mathbb{C}/\Gamma \to \mathbb{S}^2$ and *defines* addition on a cubic by first observing that any line through two points $P_1,\ P_2$ on the cubic C intersects the cubic in a third point $P_3 := (P_1P_2)\cdot C$. Choose a point $O \in C$ and define $P_1 \oplus P_2 := (OP_3)\cdot C$. Then associativity has to be proved. On the other hand, if one emphasizes the meromorphic maps, then addition on $\mathbb{C}/\Gamma$ is already defined (with associativity) and transferred via addition formulas for the functions to addition on the cubic. In that situation one wants to prove that $P_1,\ P_2$ and $-(P_1 + P_2)$ are collinear. In our case, we map the torus minus the three 2-division points into $\mathbb{C}^3$ by $z \mapsto (u(z), v(z), w(z))$ (i.e., we map the torus into $\mathbb{C}P^3$ by $z \mapsto (1, u, v, w)$), $0 \in \mathbb{C}^3$ is the origin and we have to prove that $P := (u, v, w),\ Q := (a, b, c)$ and $R := -\big((a, b, c) \oplus (u, v, w)\big)$ are collinear. This means that there has to exist a function $t(z)$ such that $R = (1 - t)P + tQ$ or

$$\textbf{Claim}: \qquad t(z) = \frac{-u(z+s) - u(z)}{u(s) - u(z)} = \frac{-v(z+s) - v(z)}{v(s) - v(z)} = \frac{-w(z+s) - w(z)}{w(s) - w(z)}.$$

Each of the three fractions is a degree 4 function because the poles of $z \mapsto u(z),\ z \mapsto v(z),\ z \mapsto w(z)$ in the numerator and denominator cancel. We prove that these three fractions are in fact the same function: They have the same **four** zeros of the numerator since the functions u, v, w are **odd** with respect to the 2-division points (including $z = 0$) so that the numerator zeros for all three fractions are: $z_o = -s/2 + (a\ \textit{2-division point})$. The four poles of the three fractions are also at the same points: Let f be u, v or w; the zeros of the denominator are at $z = s$ and at $z = z_{f1} - s$, where z_{f1} is the other zero of f, i.e. one of the three 2-division points (origin excluded) and the remaining poles of the numerator are the poles of $z \mapsto -f(z + s)$, i.e. $z = z_{f2} - s,\ z = z_{f3} - s$, where z_{f2}, z_{f3} are the **other two** 2-division points. The three fractions thus have the same divisor and they have the same value -1 at $z = 0$, therefore they agree and the collinearity is proved.

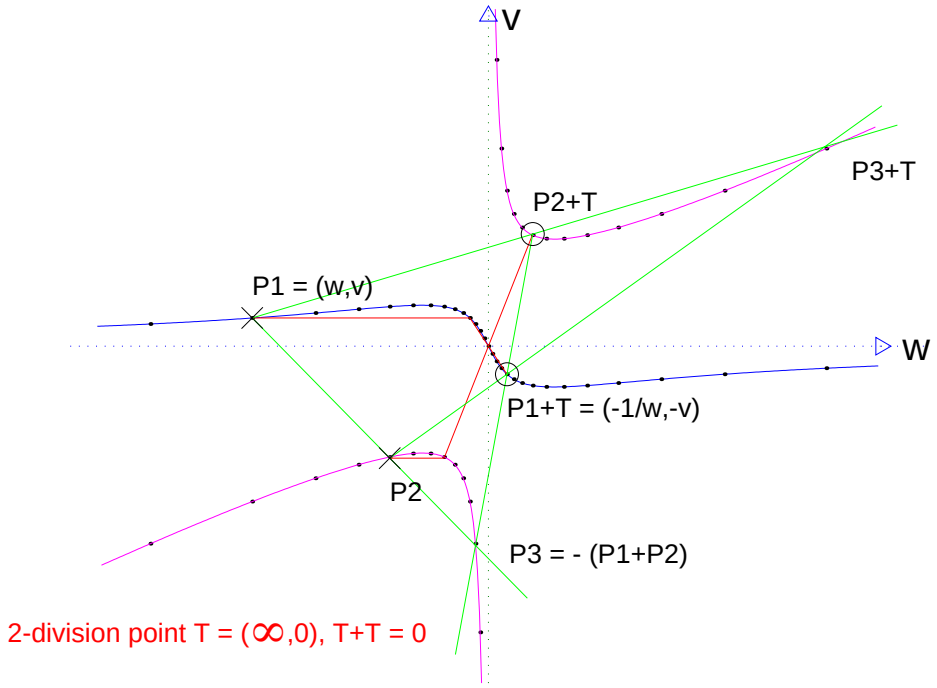
This allows simple geometric constructions. First, the addition formulas specialize for the addition of 2-division points (for the curve shown these are the three points at infinity) as follows:

$$(u, v, w) \oplus (\infty, 0, \infty) = (-1/u, -v, -1/w), \qquad (u, v, w) \oplus (\infty, \infty, 0) = (1/u, 1/v, -w).$$

To do these additions one needs the unit circle and straight lines in order to construct $1/u, 1/v, 1/w$. Further additions can then be done by just intersecting two lines, because twice a 2-division point, like $T := (\infty, 0, \infty)$, drops out since $T \oplus T = 0$. Hence:

$$(u, v, w) \oplus (a, b, c) = \big((u, v, w) \oplus (\infty, 0, \infty)\big) \oplus \big((a, b, c) \oplus (\infty, 0, \infty)\big).$$

This means (see the following figure): to obtain $P_3 := -(P_1 + P_2)$ from P_1, P_2 it is not necessary to intersect the line through P_1, P_2 with the *cubic*, it suffices to intersect this line with the *line* through $P_1 + T, P_2 + T$. Furthermore, $P_3 + T$ is obtained by intersecting the lines through $P_1, P_2 + T$ and $P_1 + T, P_2$, thus allowing iterated additions without using circles. The discrete subgroup (fat dots in the figur) should help to see the addition.



The cubic $w + 1/w = 2(v - 1/v)$, with addition of pairs $(P, P \oplus T)$.

Bibliography

[Chud] Chudnovsky, D.V. and Chudnovsky, G.V.: Sequences of numbers generated by addition in formal groups and new primality and factorization tests. Adv Appl Math 7 (1986), 385 - 434.

[HKW] Hoffman, D., Karcher, H. and Wei, F.: The genus one helicoid and the minimal surfaces that led to its discovery. pp 119 - 170 in: Global Analysis in Modern Mathematics, K. Uhlenbeck (ed.), Publish or Perish, Inc. 1993.

Hermann Karcher unm416@uni-bonn.de
Math. Inst., Beringstr. 1
D-53115 Bonn, GERMANY