Synopsis for Tuesday, November 13

Cubic curves

Any non-singular conic can be written as the sum of three squares, does something similar hold for cubics? Naively, could any cubic be written as a sum of three cubes? This is impossible, the group of projective linear transformations has $3^2 - 1 = 8$ dimensions, and the family of cubics depend on 10 monomials and thus form a 9-dimensional family. We thus expect a 1 dimensional family of different cubics. Classically we refer to those as the moduli of the cubics.

Our task is now to find different normal forms of cubics, and in order to do so it is convenient to make a digression.

The configuration of flexes

As we have noted the flexes of a cubic correspond to the intersection with its Hessian. Thus we get nine-flexes. They will constitute a very special configuration which we will explore.

First choose co-ordinates x, y, z such that $y = 0, z = 0$ are flexed tangents at the points $(0, 0, 1)$ and $(0, 1, 0)$ respectively. With such a choice of co-ordinates we see that the equation of the cubic can be written under the form

$$yz(ax + by + cz) + dx^3 = 0$$

From this we see that on the line $x = 0$ there will also be a third flex, with flexed tangent $ax + by + cz = 0$, this is simply the residual intersection of $x = 0$ with the cubic. Thus the line through any two distinct flexes meets a third. Thus the flexes lie three and three on lines. How many lines are there? Fix a flex, for any other of the eight choices of flexes we get a second one. Thus we can pair them two and two and we get four lines through each flex. Thus there are $(9 \times 4)/3 = 12$ lines in toto. Combinatorially this is the same as the affine plane over the field $\mathbb{F}_3$ which has 9 points and $1 + 3 + 9 - 1 = 12$ lines through them. (The lines in the affine part correspond to the dual of the projective plane minus the line at infinity.)

Hesse Normal form

If the cubic is non-singular it is easy to see that $abcd \neq 0$ we can thus scale x, y, z appropriately as to make $a = 1, b = -1, c = -1$ and chose $x - y - z$ as a new basic co-ordinate. Thus we can write the cubic as

$$\lambda xyz - (x + y + z)^3$$

This can be seen as a normal form and we clearly see the parameter λ. The normal form is invariant under the symmetric group S_3 of permutations of

variables and we can thus easily identify the possible singular points, as those with orbits of $1, 2$ or 3 elements, as no cubic has six singular points. In particular we see that $(1, 1, 1)$ is a singular point iff $\lambda = 27$ when we have a nodal cubic. No cuspidal cubic can be put in this form as it only has one flexed tangent, and any cubic under this form necessarily has three.

But there is another more beautiful normal form which we will derive from the above. For that purpose we set new variables according to

$$\begin{aligned} x = &\quad u + v + w \\ y = &\quad u + \rho v + \rho^2 w \\ z = &\quad u + \rho^2 v + \rho w \end{aligned}$$

where $\rho \neq 1, \rho^3 = 1$ It is then easily checked that $xyz = u^3 + v^3 + z^3 - 3uvw$ and $x + y + z = 3u$ plugging into the normal form above and doing a rescaling of u and renaming the variables we can set

$$x^3 + y^3 + z^3 - 3\mu xyz$$

This is called Hesse normal form. It has the property that the Hessian of any of its members is of the same form. Thus we have a pencil of cubics, spanned by a cubic and its Hessian. The base points of the pencil will be the common flexes of all the members.

There will be four values of μ for which the cubic becomes singular, namely $\mu = \infty$ and $\mu = \rho^i$ $(i = 1, 2, 3)$. In all of the four cases the singular fiber will split up into three lines. The base points (i.e the flexes) will lie three and three on each of the three lines of a singular member, and in toto there will be twelve lines.

Those singular elements of the pencil can be written down explicitly

μ	
∞	xyz
1	$(x + y + z)(x + \rho y + \rho^2 z)(x + \rho^2 y + \rho z)$
ρ	$(x + \rho^2 y + \rho^2 z)(x + y + \rho z)(x + \rho y + z)$
ρ^2	$(x + \rho y + \rho z)(x + \rho^2 y + z)(x + y + \rho^2 z)$

We can easily write down the nine flexes explicitly by setting $x = 0, y = 0, z = 0$ respectively and get

$$\begin{gathered} (0, 1, -1) \\ (0, 1, -\rho) \\ (0, 1, -\rho^2) \\ (-1, 0, 1) \\ (-\rho, 0, 1) \\ (-\rho^2, 0, 1) \\ (1, -1, 0) \\ (1, -\rho, 0) \\ (1, -\rho^2, 0) \end{gathered}$$

Note that e.g. $(0,1,-1)$ lie on the four lines $x, x+y+z, (x+\rho y+\rho z), (x+\rho^2 y+\rho^2 z)$ one from each fiber.

This so called $(9_4, 12_3)$ configuration (four lines through each nine points, three points on each twelve lines) is actually isomorphic to the affine space $\mathbb{F}_3^2$ of pairs (X,Y) and lines $aX+bY+c=0$ with the exception of the line at infinity $c=1$. (There are of course 13 lines in $\mathbb{F}_3P^2$ removing the line at infinity, twelve remain.)

Each triplet of lines in the table above corresponds to three parallel lines in $\mathbb{F}_3^2$. So let us try to make an explicit correspondence between the flexes and $\mathbb{F}_3^2$. So let us correspond the line $x=0$ to $X=0$ and $x+y+z=0$ to $Y=0$ and set up a tentative table

(X,Y)	0	1	-1
0	$(0,1,-1)$	$(0,1,-\rho)$	$(0,1,-\rho^2)$
1	$(-1,0,1)$		
-1	$(1,-1,0)$		

Now consider the line $x+\rho y+\rho^2 z$ it will correspond to $Y+\pm 1$ but which? The points on the line are easily found, namely $(0,1,-\rho^2), (-\rho^2,0,1), (1,-\rho^2,0)$. One of those points $(0,1,-\rho^2)$ is already marked and is in the -1 column, where should we put the others? The following is natural as $y=0$ correspond to $X=1$

(X,Y)	0	1	-1
0	$(0,1,-1)$	$(0,1,-\rho)$	$(0,1,-\rho^2)$
1	$(-1,0,1)$		$(-\rho^2,0,1)$
-1	$(1,-1,0)$		$(1,-\rho^2,0)$

It should now be clear how to complete the table

(X,Y)	0	1	-1
0	$(0,1,-1)$	$(0,1,-\rho)$	$(0,1,-\rho^2)$
1	$(-1,0,1)$	$(-\rho,0,1)$	$(-\rho^2,0,1)$
-1	$(1,-1,0)$	$(1,-\rho,0)$	$(1,-\rho^2,0)$

The principle on which the table is constructed is by making the following correspondence

$$\left|\begin{array}{c|c} x & X \\ y & X=1 \\ z & X=-1 \end{array}\right\| \left|\begin{array}{c|c} x+y+z & Y \\ x+\rho^2 y+\rho z & Y=1 \\ x+\rho y+\rho^2 z & Y=-1 \end{array}\right|$$

we can now check that the following correspondce follows

$$\left|\begin{array}{c|c} x+\rho^2 y+\rho^2 z & X+Y=0 \\ x+y+\rho z & X+Y=-1 \\ x+\rho y+z & X+Y=1 \end{array}\right\| \left|\begin{array}{c|c} x+\rho y+\rho z & X-Y=0 \\ x+\rho^2 y+z & X-Y=1 \\ x+y+\rho^2 z & X-Y=-1 \end{array}\right|$$

The symmetry group of the flexes

We made the identification by chosing a line for the x-axis and a non-parallel line for the y-axis. We also made an arbitrary choice of what should be the points $(0,1)$ and $(1,0)$. There is hence a total of $12 \times 9 \times 4 = 2^4 3^3 = 432$ possibilities of making the identification. Another way of putting it is to take a point as the origin and chosing two independent vectors in $\mathbb{F}_3^2$. This gives a count of $9 \times 8 \times 6 = 432$ as well, as the origin can be chosen as any point, for a non-zero vector we have $9 - 1 = 8$ choices and for the other vector independent of the first $9 - 3 = 6$. The projective transformations of $\mathbb{F}_3$ are given by $PGL(3, \mathbb{F}_3$. This has a subgroup given by matrices

$$\begin{pmatrix} a_{11} & a_{12} & b_1 \\ a_{21} & a_{22} & b_2 \\ 0 & 0 & 1 \end{pmatrix}$$

which preserves the affine plane given by $(x, y, 1)$. An element of this sugroup can be thought of as a translation followed by an element of $G = GL(2, \mathbb{F}_3)$. There are 9 translations and the group G has in general $(p^2-1)(p^2-p)$ elemenst which in our case translates into 48 as we have computed above. This group is the automorphism group of the configuration, moving points and hence lines preserving the incidence relation between the points and the lines.

The group can be denoted the affine group $A(\mathbb{F}_3)$ where the translations T is easily checked to be a normal subgroup $(A^{-1}(AX + t) = X + A^{-1}t$ i.e. the conjugate of a translation is a (different) translation) and we have a sequence.

$$0 \to T \to A(\mathbb{F}) \to GL(2, \mathbb{F}) \to 1$$

If we restrict to the normal subgroup $SG = SL(2, \mathbb{F}_3)$ of matrices with determinant 1 we cut down to 24 and are considering a group of 216 elements, which we can refer to as the special affine group $SA(\mathbb{F})$.

This group can actually be represented in $PGL(3, \mathbb{C})$ in the following manner.

To understand that we simply need to observe that any subgroup of $PGL(3, \mathbb{C})$ that preserve the flexes must permute the cubics in the Hessian pencil, as any cubic that pass through the nine base-points must belong to the pencil. Conversely any element that preserves the pencil, i.e. permutes its members, must preserve the basepoints.

Now it is easy because of the special form of the cubics in the pencil to write down linear transformations which preserve them. First we have the group S_3 of permutation of the variables, then we can add to those transformations of type $(x, y, z) \mapsto (x, \rho y, \rho^2 z)$. The latter are conjugated by the involutions, and hence they commute with the cyclic permutations, and we conclude that they form a normal subgroup, and generate along with the obvious permutations, a group of order 18 containing a commutative subgroup $\mathbb{Z}_3^2$.

We can look at the latter more closely. First we note that it is generated by the two linear transformations $A(x, y, z) = (z, x, y)$ and $B(x, y, z) = (x, \rho y, \rho^2 z)$

and that those correspond to the translations $(X, Y) \mapsto (X+1, Y)$ and $(X, Y) \mapsto (X, Y+1)$ respectively.

Next we consider $C(x, y, z) = (x, z, y)$ it will leave the configuration invariant and fix the origin $(0, 1, -1)$ and we have $C(1, 0) = (-1, 0)$ and $C(0, 1) = (0. - 1)$ and thus C is a representation of the element $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.

Those are the only transformations that keep the cubics invariant, and it can be described as the group generated by the translations and the center of the group $SL(2, \mathbb{F}_3)$. Another interesting linear transformation is $D(x, y, z) = (x, \rho y, \rho z)$ and we note that $D(1, 0) = (1, -1)$ while $D(0, 1) = (0, 1)$ thus D represents $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$. Now C belongs to the center and is of order two, while D has order three. Together they generate a cyclic subgroup of order 6. Thus note that while $|SL(2, \mathbb{F}_3)| = 24$ it cannot be the symmetric group S_4 with 24 elements and permuting four letters, as the latter does not have any elements of order 6.

The group D acts on the pencil by sending μ to $\rho^2\mu$, and thus permuting the three singular fibers corresponding to $\mu = \rho^i$. As the four singular fibers should play symmeric roles we are looking for a transformation that maps the fiber at ∞ given by xyz to any of the other three. This can be done in a number of ways. Let us choose the map

$$\begin{array}{rcl} x & \mapsto & x + y + z \\ y & \mapsto & x + \rho y + \rho^2 z \\ z & \mapsto & x + \rho^2 y + \rho z \end{array}$$

One checks that indeed it leaves $(0, 0)$ invariant and sends $(1, 0)$ to $(0, 1)$ and $(0, 1)$ to $(-1, 0)$ and thus corresponds to the matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

Summarizing our discussion we have a composition of $SA(\mathbb{F}_3)$ as follows

$$0 \to \mathcal{D}_{18} \to SA(\mathbb{F}_3)_{216} \to PSL(2, \mathbb{F}_3)_{12} \to 1$$

Where $\mathcal{D}_{18}$ is a kind of dihedral group, built on $\mathbb{Z}_3^2$ instead of on a cyclic group, and by letting an involution ε act by $x \mapsto -x$. Thus $\mathcal{D}_{18}$ is the semi-direct product of $\mathbb{Z}_3^2$ with $\mathbb{Z}^2$. Furthermore $PSL(2, \mathbb{F}_3)_{12}$ consists of the even permutations of four elements (the four singular fibers) and becomes a subgroup of $PSL(2, \mathbb{C})$ permuting the members of the pencil. There is thus a natural representation and it can be made explict as D is represented by $\begin{pmatrix} \rho^2 & 0 \\ 0 & 1 \end{pmatrix}$ $(z \mapsto \rho^2 z)$ and E by $\begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix}$ or $z \mapsto \frac{z+2}{z-1}$.

Thus each non-singular member has in general an orbit of 12 elements, the singular members only 4 elements, meaning that their stabilizers are bigger, in fact they are also invariant under conjugates of D (D itself stabilizes ∞). It is all reminiscent of the symmetries of the tetrahedron, except the points ρ^i, ∞

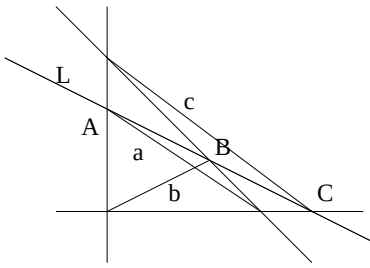
are not regularly placed on the sphere, using the standard mapping of $\mathbb{C}$ via projection from the north pole.

Now there are other values of μ for which the stablizers are bigger. To find them we only need to look at the fixed points of D and E and their orbits.

The fix-points of D are clearly $0, \infty$ and the orbit of 0 should have four points, and the others are $-2 = E(0), -2\rho, -2\rho^2$. The standard example $\mu = 0$ corresponds to the Fermat cubic. It enjoys D as well in its automorphism group which is then a group of 54 elements and an extension of $\mathcal{D}_{18}$ with $\mathbb{Z}_3$.

Remark 1 The Fermat cubic has the property that we may find three flexes such that the corresponding flexed tangents go through a point. Those three flexes will then necessarily lie on a line. The Fermat cubic is characterized by this property of three flexed tangents going through a point. In fact the above property holds for all flexing lying on a line.

To see it look at the map $P^2 \to P^2$ given by $(x, y, z) \mapsto (x^3, y^3, z^3)$ this is a $9:1$ map but ramified $3:1$ over the co-ordinate axi and totally ramified $1:1$ over the vertices. Let L be a line in the target that intersect those in points A, B, C and let a, b, c be the lines passing through the vertices and the corresponding points see figure below, then each of the lines a, b, c split up into three lines.



The inverse image of L will be a Fermat cubic, and the split up lines will meet the cubic in three coinciding points each, hence become flexed tangents. We can make this explicit by chosing L given by $x + y = z = 0$. Then we are looking at the lines $x + y = 0, x + z = 0, y + z = 0$ in the target space. The pullbacks $x^3 + y^3, x^3 + z^3, y^3 + z^3$ split up as $(x + y)(x + \rho y)(x + \rho^2 y)$ etc, which will be flexes as we have $(x + y)(x + \rho y)(x + \rho^2 y) = -z^3$ etc.

We see that the nine flexes we have exhibited will lie on xyz but because of the enhanced symmetries of the Fermat cubic, all the four triplets are equivalent. The nine flexed tangents of a Fermat cubic will hence meet three and three in twelve points. This is the dual of the configuration of flexes.

The fix-points of E are the orbits of $\mu = 1 + \pm\sqrt{3}$ which will make up six-oints. This cubic will have an extra involution in its automorphism group induced projectively.

Those are the only exceptions.

In general we can write down an explicit function j of μ which is constant on the orbits of $PSL(2, \mathbb{F}_3)$ namely

$$\frac{\mu^3(\mu^3 + 8)^3)}{(\mu^3 - 1)^3}$$

Note that for the critical values ∞, ρ^i it will have poles of order three and thus correspond to $j = \infty$. Note that the special value $\mu = 0, -2\rho^i$ corresponds

to $j(\mu) = 0$

Group structure

A cubic curve is topologically a torus. A torus can be obtained by glueing opposites sides of a rectangle, thus making all the four corners go to one point. More elegantlys, we can think of it as $\mathbb{R}^2$ divided out by a lattice Λ. A lattice is a module over $\mathbb{Z}$ generated by two linearly independent vectors ω_1, ω_2. They span a parallelogram, which is called the period parallelogram, which is the so called fundamental region of the action of $\mathbb{Z}^2$ on $\mathbb{R}^2$ given by $(\lambda_1, \lambda_2)z = z + \lambda_1\omega_1 + \lambda_2\omega_2$. The orbits of this action intersect the parallelogram in exactly one point (if we take care which edges to include) and taking the quotient is the same thing as identifying opposite edges. Topologically we can reduce to $\omega_1 = (1, 0)$ and $\omega_2 = (0, 1)$ and thus the canonical inclusion of $\mathbb{Z}^2$ into $\mathbb{R}^2$. The quotient can be thought of as $\mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z} = S^1 \times S^1$. Now as $\mathbb{R}^2$ is a group under addition and $\mathbb{Z}^2$ a subgroup, the quotient is also a group. Thus a natural question is whether there is a group structure on a cubic.

In fact there will be. And there is a natural way of defining it. We say that three points add up to zero iff they are collinear. By this assumption the zero has to be a flex.

Thus let us fix a flex O as zero. We now get to define $P \oplus Q$ in the following way. Join P and Q by a line and let R be the residual intersection. Then $R = -(P \oplus Q)$ To get $P \oplus Q$ we take the line joining R with O and the residual intersection will be $-R$ hence our desired $P \oplus Q$. That this operation is commutative is obvious, also that it has a neutral element. The inverse is also easy to find by 'inversion' in O so to speak. What about associativity? This is a pain, but it is possible to prove geometrically. We will leave this aside.

Now the group structure on the torus has lots of so called torsion points. Those are points p such that $nP = 0$. One finds easily n^2 of such as given by $\Lambda/n\Lambda$. The torsion points of order n form a subgroup of the torus, and the structure of that group is $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Torsion groups on a torus are analogues of torsion points on a circle, which are simoly the roots of unity. (In fact if we classically divide the circle into 360^o those will be the points associated to a rational degree. The denominator of the rational number gives a clue to its order.)

The simplest torsion elements are the 2-torsion. They will form the Klein Viergruppe $\mathbb{Z}_2^2$. There will be O of course, and three primitive 2-torsion points. Geometrically we are looking at points P such that the tangent to P pass through O. That means $2P + 0$ lie on a line. We know that there are four such points, of which one is O itself, as it is a flex point. The other three are the primitive. As the sum of the primitive is zero, then those must lie on a line. That we already knew, as the polar at a clex point splits up into two line, one the flexed tangent and the other the line joining the three primitive 2-torsion points.

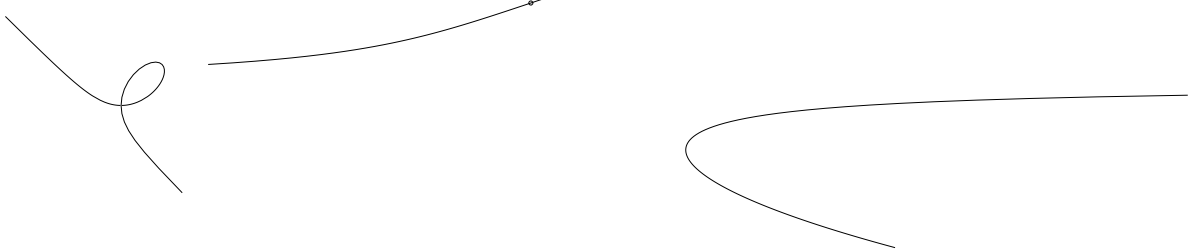
Elements of order 3 are given by the flexes. They form a subgroup isomorphic to $\mathbb{Z}_3^2$ which explains a lot of what we have already studied. Translations by 3-

torsion points can be induced by projective transformations. And also the map $z \mapsto -z$. Two cubic curves have extra symmetries, and hence also those operate on the sub-groups of torsion points. We have already established non-general isomorphisms on the group of flexes in those cases.

What about group-structures on singular cubics? The definition works fine as long as we stay away from singular points. Note that if we take a line through two non-singular points, it cannot hit the singular locus, unless the line is a component of the cubic, as a line can only hit in three points.

Now a nodal cubic is P^1 minus two points. This is the same thing as $\mathbb{C}^*$ (or more generally k^*) which is a group under multiplication. While the cuspidal cubic is simply $\mathbb{C}$ (k) which is a group under addition. So what you need to do is to give appropriate parametrizations by nets of binary cubics letting the identity be mapped onto a flex and such that the three solutions to any polynomial in the net multiply to one or add to zero, depending on whether we are dealing with nodal or cuspidal cubics.

In the case of the nodal cubic, we are looking for a polynomials such that the contant term is -1 as that means that the product of the roots multiply to one. One may remark that such polynomials are not closed under addition, but this can easily be remedied. We are simply looking at cubics $at^3 + \ldots - as^3$. Those make up a net and a basis can easily be found by $t^3 - s^3, t^2s, ts^2$. Call them X, Y, Z respectively. Among the ten monomials $X^3, Y^3, \ldots$ we are looking for a linear relation. It is easy to find the one, namely $Y^3 - Z^3 - XYZ = 0$ (By replacing Y with $-Y$ we may put it in the more appealing form $Y^3 + Z^3 = XYZ$ parametrized by $(t^3 - 1, -t^2, t)$. The singular point is $(1, 0, 0)$ the common image of $t = 0, \infty$. The lines $AY + BZ = 0$ are the lines going through the nodes and are not interesting. The other lines are of form $X = AY + BZ$ and correspond to $t^3 + At^2 - Bt - 1$ with the solutions t_1, t_2, t_3 satisfying $t_1t_2t_3 = 1$. In particular we have the flex $(t-1)^3 = t^3 - 3t^2 + 3t - 1$ which correspond to the line $X + 3Y - 3Z = 0$ flexed to the cubic at the point $(0, -1, 1)$. Note that the other two flexes correspond to primtive cube roots of unity and are hence not real.



In the picture above on the left, the flex is at infinity, and the flexed tangent ought to be obvious. While on the right we have changed the perspective and the flex is pointed out. The two branches of the curve correspond to $t > 0$ and $t, 0$ respectively and they will asymptotically become horizontal corresponding to the nodal tangent $Y = 0$, the other being the line at infinity ($Z = 0$).

The case of the flex is much simpler. A natural parametrization (t, t^3) buts the cusp at infinity, and a lex at the origin with flexed tangent $y = 0$ and clearly

the roots of $AX + BY + CZ = 0$ are given by $Bt^3 + At + C = 0$ and clearly their sum is zero.

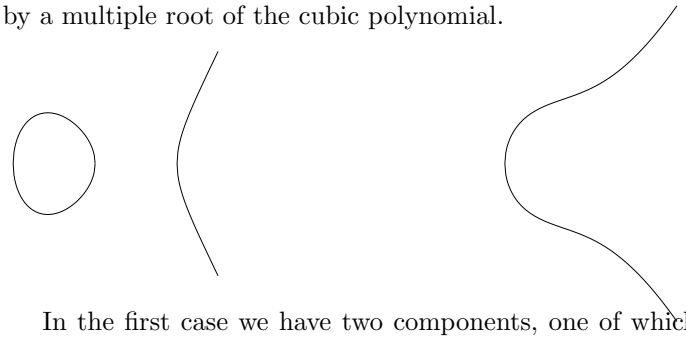
Weierstrass Normal form

The most common normal form is the Weierstrass normal form given by

$$y^2 = 4x^3 - g_2 x - g_3$$

(The significance of the 4 will become apparent later). The salient feature is $y^2 = p_3(x)$ where p_3 is a cubic polynomial in x. The curve is smooth iff p_3 has no multiple roots. We also see that the line at infinity will be the flexed tangent at the point $(0, 1, 0)$ which means that the pencil of lines through it will be given by the lines parallel to the y-axis. That flex will be the natural point to choose as a zero. The obvious symmetry of the curve given by reflection $(x, y) \mapsto (x - y)$ in the x-axis will then simply be the map $X \mapsto -X$ on the group level. The intersection of the curve with the x-axis will then correspond to the fix points of this involution, hence to the four torsion-points of order two, one of which is at infinity, and the remaining primitive ones in the finite part.

It is easy to draw the real picture, and we get two different ones, depending on whether the cubic has one or three real roots. The two cases are separated by a multiple root of the cubic polynomial.



In the first case we have two components, one of which is an oval (convex in fact why?) and subdivides the porjective plane in two parts and the other a curve that does not. Notice on the right two prominent flexes.

Now this normal form has two parameters instead of one. And in fact if we make the automorphism $(x, y) \mapsto (t^2 x, t^3 y)$ the cubic will be transformed to $y^2 = 4x^3 - t^2 g_2 - t^3 g_3$ and be isomorphic. We can now concoct an invariant which takes care of this, namely

$$J = \frac{g_2^3}{g_2^3 - 27 g_3^2}$$

where $\Delta = g_2^3 - 27 g_3^2$ is the discriminant of the binary cubic, and is non-zero iff the (ternary) cubic is non-singular. It will turn out that two cubics are isomorphic iff they have the same J-invariant.

Remark 2 The case for real cubics is a bit more complicated. To the same j invariant there may be two different cubics, non-isomorphic over the

reals, but isomoprhic over the complex numbers. To every cubic $y^2 = p_3(x)$ we may associate the dual cubic $y = -p_3(x)$ which will have the same J-invariant ($g_3 \mapsto -g_3$ while g_2 invariant), but which is different. The situation becomes even more complicated if we consider $k = \mathbb{Q}$ and ask for isomorphisms defined over the rationals.

The Explicit Group law

Give two points $P = (x_1, y_1), Q = (x_2, y_2)$ how do we compute the co-ordinates (x_3, y_3) of their sum? It is easy, just write down the equation of the line passing through P, Q and determine its residual intersection. If we work it out we get the following formulas in case $P \neg \pm Q$

$$\begin{aligned} x_3 &= (\tfrac{y_2-y_1}{x_2-x_1})^2 - (x_1 + x_2) \\ y_3 &= -\tfrac{y_2-y_1}{x_2-x_1} x_3 - \tfrac{y_1 x_2 - y_2 x_1}{x_2-x_1} \end{aligned}$$

while if $P = Q$ we have the duplication formula

$$\begin{aligned} x_3 &= (\tfrac{y_2-y_1}{x_2-x_1})^2 - (x_1 + x_2) \\ y_3 &= -\tfrac{y_2-y_1}{x_2-x_1} x_3 - \tfrac{y_1 x_2 - y_2 x_1}{x_2-x_1} \end{aligned}$$

Example 1 If g_2, g_3 are rational and we have a rational point, i.e. a rational solution to the diophantine equation we can generate new ones.

Example 2 This works on finite groups too, although special care needs to be taken for char $2, 3$ where the Weierstrass form need to be modified.

Cubic Curves over Finite fields

Elliptic curves and Elliptic functions

A curve X is called elliptic iff it is of the form $\mathbb{C}/\Lambda$ where Λ is a lattice of rank two over the reals. (That means $\Lambda \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{C}(= \mathbb{R}^2)$). A meromorphic function on X can be thought of as meromorphic function $E(z)$ on $\mathbb{C}$ which is doubly periodic. That means $E(z + \omega) = E(z) \quad \forall \omega \in \Lambda$, where ω is referred to as a period. Or more specifically $E(z + \omega_1) = E(z + \omega_2) = E(z)$ for a basis ω_1, ω_2 of Λ, which explains the classical terminology of doubly periodic functions.

Remark 3 A parallelogram spanned by ω_1, ω_2 is a fundamental region for the action of $\mathbb{Z}^2$ as explained above.

It is clear that the elliptic functions form a field, the function field oof the elliptic curve X.

We have three basic facts about Elliptic functions.

I) *An elliptic function without poles is constant.*

II *The sum of the residues of an elliptic function inside a fundamental parallelogram P (with no poles on its boundary ∂P) is zero.*

III *If an elliptic function has zeroes and poles of order m_i at a_i then* $\sum m_i = 0$

IV *If an elliptic functions have zeroes and poles at the points a_i with multiplicity m_i ($m_i > 0$ means a zero $m_i < 0$ means a pole) then $\sum m_i a_i = 0(|Lambda$, or $\sum m_i \overline{a_i} = 0$ in the group structure of X.*

For I) we simply note that such a function must be bounded (as it can be thought of as a function on a compact set X) and then appeal to Liouvilles theorem that a bounded entire function is constant. Or note that any holomoprhic function on a compact curve must be constant. (Its modulus will have global max and minima).

For I) II) and III) we consider the residue theorem applied to the functions $E, \frac{1}{2\pi}\frac{E'}{E}$ and $\frac{1}{2\pi}z\frac{E'}{E}$ respectively. The first functions are elliptic and thus the integral of them around ∂P must be zero because of periodicity. On the other hand those integrals are the sums of their residues. As to the third function, its integral around the perimeter will be $\sum m_i a_i$, while the integrals along opposite sides will differ my a period, hence the total integral will be an element of Λ. (This is also attributed to Liouville.)

II) Implies that an elliptic function cannot have a simple pole. Note that any meromorphic function with a simple pole on a compact curve X would give a birational function to $\mathbb{C}P^1$ and thus establish a 1-1- correspondence between the fields of meromoprhic functions on X and $\mathbb{C}P^1$.

IV) implies that the dimension of elliptic functions of degree d is at most d. By that I mean elliptic functions with a fixed pole of order d and holomoprhic everywhere else. Note that two elliptic functions with the same zeroes and poles (counted with multiplicities) differ my a multiplicative constant, as seen by taking their quotient, which will be holomorphic and hence constant. Later we will see that the dimension is in fact d. This will follow if we can show that the necessary condition given by III) is also sufficient.

In order to show that the theory is not empty, we need to exhibit an explicit non-constant elliptic function. A classical example is due to Weierstrass and referred to as the Weierstrass p-function and denoted by $\wp(z)$. Its definition is given by

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda^*} \left[(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right]$$

For this to make sense, we need to show that the sum converges uniformly on compact subsets away from the lattice of poles. This will follow easily from the fact that $\sum_{\omega \in \Lambda^*} \frac{1}{|\omega|^\lambda}$ converges if $\lambda > 2$.

It is clear that $\wp(z)$ is even, but it is not clear that it is periodic with respect to the lattice. However its derivative $\wp'(z)$ satisfies

$$\wp'(z) = -2 \sum_{\omega \in \Lambda^*} \frac{1}{(z-\omega)^3}$$

for which the convergence is easier to show and the form shows directly that $\wp'$ is odd and periodic. Thus we get that $\wp(z + \omega_i) = \wp(z) + C_i$ for some constant

C. Putting $z = -\frac{\omega_i}{2}$ and using that the function is even, we conclude that $C_i = 0$ and thus that the function is indeed periodic.

Let $E(z)$ be an even elliptic function, then it has even order (most likely zero) at the 2-torsion points. In fact if ω is a 2-torsion point then $E(z+\omega$ is still even (and elliptic) with a zero at 0. This zero has hence to be of even order. Now let the zeroes (poles) of E(z) be u_i (inside a period parallelogram) with multiplicities m_i. Consider $(\wp(z) - \wp(u_i))^{m_i'}$ where $m_i' = m_i$ unless $2u_i = 0$ in which case $m_i' = m_i/2$. This will have the same zeroes and poles as $E(z)$. Hence every even elliptic function is a rational faunction of $\wp(z)$. Now every function can in a unique way be written as a sum of an odd and even function, and those will be elliptic if the original function is

Remark 4 This follows from the standard decomposition $f(t) = \frac{f(t)+f(-t)}{2} + \frac{f(t)-f(-t)}{2}$

From this follows that every elliptic function can be written as rational function of $\wp(z)$ and $\wp'(z)$ as every odd function becomes even when divided by $\wp'(z)$. Now there must be a relation between $\wp(z)$ and $\wp'(z)$. In fact $\wp'(z)^2$ is an even function. It must vanish at the primitive 2-torsion points ω_i ($\omega_3 = \frac{1}{2}(\omega_1 + \omega_2)$ as $\wp'(z+e_i)$ are odd functions. Set $e_1 = \wp(\omega_1/2), e_2 = \wp(\omega_2/2), e_3 = \wp((\omega_1+\omega_2)/2)$ Hence we get that $\wp'(z)^2$ is a multiple of $(\wp(z)-e_1)(\wp(z)-e_2)(\wp(z)-e_3)$ and looking at the pole at zero, the constant must be 4.

This relation can also be realized as follows. The Laurent expansion of $\wp(z)$ follows from the identity

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \sum_{n\geq 0} \frac{1}{\omega^2}((n+1)\frac{z^n}{\omega^n} - 1)$$

giving

$$\wp(z) = \frac{1}{z^2} + \sum_{n>0}(2n+1)(\sum_{\omega\in\Lambda^*}\frac{1}{\omega^{2n}})z^{2n}$$

Let us define $s_n(\Lambda) = \sum_{\omega\in\Lambda^*}\frac{1}{\omega^{2n}}$ and write

$$\wp(z) = \frac{1}{z^2} + \sum_{n>0}(2n+1)s_n(\Lambda)z^{2n}$$

and then

$$\wp'(z) = -2\frac{1}{z^3} + \sum_{n>0}(4n^2+2n)s_n(\Lambda)z^{2n-1}$$

In particular the initial expansion of $\wp^3(z)$ is given by

$$\frac{1}{z^6} + \frac{9s_1}{z^2} + 15s_2 + \dots$$

while that of $(\wp')^2(z)$ is provided by

$$\frac{4}{z^6} - \frac{24s_1}{z^2} - 80s_2 + \dots$$

from which follows that

$$(\wp')^2(z) = 4\wp(z) - 60s_1\wp - 140s_2$$

because the difference is a holomorphic elliptic function which vanishes at 0.

Remark 5 If we expand the above identiy and identify coefficients we note that all the s_k with $k > 2$ can be written as polynomials in s_1, s_2

Thus we see that given a cubic curve in Weierstrass normal form we can parametrize it by doubly periodic functions $(\wp(z), \wp'(z), 1)$ provided we can find a lattice Λ such that $g_2 = 60s_1$ and $g_3 = 140s_2$. This is in general not so easy.

Isomorphism classes of Elliptic curves

The functions $s_n(\Lambda)$ are functions on lattices. It is obvious that $s_n(\lambda\Lambda) = \lambda^{2n}s_n(\Lambda)$. Furthermore $\lambda\Lambda$ and Λ give rise to isomorphic curves. In particular we can chose a basis for Λ given by $1, \tau$ where τ is an element of the upper halfplane $\mathbf{H} = \{\mathbf{z} : \Im(\mathbf{z}) > \mathbf{0}\}$. However, τ is not uniquely determined. If γ is any element of the Modular group $\Gamma = PSL(2, \mathbb{Z})$ then τ and $\gamma\tau$ correspond to isomorphic elliptic curves. The reason is that if $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ has determinant ± 1 then $c\tau + d, a + b\tau$ is another basis. We can now divide by the first and get the action $\tau \to \frac{a\tau+b}{c\tau+d}$. To be sure that the quotient belongs to the upper halfplane we need that the determinant is one (a positively oriented basis).

Now the quotient $\mathbf{H}/\mathbf{\Gamma}$ parametrizes elliptic curves up to isomorphism. However the action of Γ on $\mathbf{H}$ is not properly discontinuous, there are points which are fixed for some of the elements. This actually complicates life.

One can consider a subgroup $\Gamma(2)$ of the modular group Γ. This is given as the kernel of the reduction modulo two map onto $PSL(2, \mathbb{Z}/\not{=}Z)$. The elements that give rise to trouble do not occur in this subgroup and we can easily take the quotient. It turns out to be $\mathbb{C}P^1$ minus three points, which can be normalized to $0, 1, \infty$. We can think of it as elliptic curves with a labeling of the three primitive 2-torsion points. In other words we keep track of the points $\frac{1}{2}, \frac{\tau}{2}, \frac{1+\tau}{2}$. The group $PSL(2, \mathbb{Z}/\not{=}Z)$ is isomorphic with S_3 and acts as permutations on the three 2-torsion points. Furthermore if $\lambda \in \mathbf{H}/\Gamma(2)$ then the action of S_3 is generated by the involutions $1 - \lambda, 1/\lambda$

Example 3 If $y^2 = x(x-1)(x-\lambda)$ then we have an elliptic curve wich is a double cover of $\mathbb{C}P^1$ ramified at four points $0, 1, \lambda$ and ∞ and with the three primitive 2-torsion points given by $0, 1, \lambda$.

Special Lattices and Special Values

Theta functions

Rational functions are defined as quotients of polynomials. For those to be well-defined on the Riemann sphere they need to have the same degree, i.e. belong to the same linear system.

One may also define certain quasi-periodic entire functions which may be thought of as sections of line-bundles on elliptic curves and express elliptic functions as quotients of those, associated to the same quasi-periodic behaviour.

It turns out that it is very convenient to consider exponential factors and we make the following formal definition.

A function Θ is called a theta-function with respect to the multiplier $M = \begin{pmatrix} 2\pi i a_1 & b_1 \\ 2\pi i a_2 & b_2 \end{pmatrix}$ if it exhibits the following quasi-periodic behaviour with respect to a lattice Λ

$$\begin{aligned} \Theta(z+\omega_1) &= e^{2\pi i a_1 + b_1}\Theta(z) \\ \Theta(z+\omega_2) &= e^{2\pi i a_2 + b_2}\Theta(z) \end{aligned}$$

If Θ is associated to the multiplier M and Ψ is associated to N then $\Theta\Psi$ is also a thetafunction and associated to $M+N$. However the sum of two theta functions is not a thetafunction, unless the summands are associated to the same multiplier. Those form a vectorspace and can be thought of as the sections of a linebundles, their zeroes forming linearly equivalent divisors.

Now the numbers a_1, a_2 cannot be arbitrary but need to satisfy a condition. In fact if we consider the integral

$$\frac{1}{2\pi i}\int_{\partial P}\frac{\Theta'}{\Theta}$$

it becomes an integer, counting the number of zeroes of Θ in a fundamental parallelogram. On the other hand we have

$$\begin{aligned} \Theta'(z+\omega_1) &= 2\pi i e^{2\pi i a_1 + b_1}\Theta(z) + e^{2\pi i a_1 + b_1}\Theta'(z) \\ \Theta'(z+\omega_2) &= 2\pi i e^{2\pi i a 21 + b_2}\Theta(z) + e^{2\pi i a_2 + b_2}\Theta'(z) \end{aligned}$$

from which follows

$$\frac{\Theta'(z+\omega_1)}{\Theta(z+\omega_1)} = 2\pi i a_i + \frac{\Theta'(z)}{\Theta(z)}$$

and thus

$$N = \frac{1}{2\pi i}\int_{\partial P}\frac{\Theta'}{\Theta} = a_1\omega_2 + a_2\omega_1$$

The integer N is called the order of the theta-function and is simply the degree of the divisor of its zeroes.

Example 4 Theta-functions of degree zero are given by $e^{2\pi i Q(z)}$ where Q is a quadratic polynomial. They correspond to trivial line-bundles, and they will be referred to as trivial theta functions. One easily computes their multipliers. Those will have rows given by $(2\pi i(2a\omega_i)2\pi i(a\omega_i^2 + b_i\omega_i)$ and indeed $(2a\omega_1)\omega_2 - (2a\omega_2)\omega_1 = 0$.

Remark 6 By multiplying with a suitable trivial theta function we can always obtain periodicity with respect to one of the vectors. This is not always suitable, but sometimes convenient. By normalizing the lattice to $< 1, \tau >$ we can then achieve periodity with respect to $z \to z + 1$ and hence expand the theta-function in a Fourier series.

Riemann-Roch for Elliptic Curves