LECTURE 8, MONDAY MARCH 08, 2004

FRANZ LEMMERMEYER

1. Projective Transformations

In affine geometry, affine transformations (translations, rotations, ...) play a central role; they can be described by $(x, y) \longmapsto (x', y')$, where $x' = ax + by + c$, $y' = dx + ey + f$, where $ad - bc \neq 0$. Note that affine transformations form a group under composition of maps.

Proposition 1.1. *Let P_1, P_2, P_3 be non-collinear points in the affine plane. Then there is a unique affine transformation that sends P_1 to $(0, 0)$, P_2 to $(1, 0)$, and P_3 to $(0, 1)$.*

Proof. We only sketch the proof. Write $P_i = (x_i, y_i)$; then we get a linear system of 6 equations in 6 unknowns, and since the P_i are not collinear, the corresponding system has nonzero determinant and thus a unique solution. □

Now let us define projective transformations. An invertible 3×3-matrix $A = (a_{ij}) \in M_3(K)$ acts on the projective plane $\mathbb{P}^2K$ via $A([x : y : z]) = [x' : y' : z']$, where

$$(x', y', z') = (x, y, z) \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}.$$

This is well defined, since $A([\lambda x : \lambda y : \lambda z]) = [\lambda x' : \lambda y' : \lambda z']$, so rescaling is harmless.

There are, however, matrices in $\mathrm{GL}_3(K)$ that have no effect on points in the projective plane: the diagonal matrix $\mathrm{diag}(\lambda, \lambda, \lambda)$ (this is the matrix with $a_{ij} = 0$ except for $a_{11} = a_{22} = a_{33} = \lambda$) for nonzero $\lambda \in K$ fixes every $[x : y : z] \in \mathbb{P}^2K$. The group of all diagonal matrices with entry $\lambda \in K^\times$ is isomorphic to $K^\times$, and we can make the projective general linear group $\mathrm{PGL}_3(K) = \mathrm{GL}_3(K)/K^\times$ act on the projective plane. Its elements are 3×3-matrices with nonzero determinant, and two such matrices are considered to be equal if they differ by a nonzero factor $\lambda \in K^\times$.

Some Abstract Nonsense. This is a very special case of some fairly general observation. Assume that a group G acts on a set X (this means that there is a map $G \times X \longrightarrow X : (g, x) \longmapsto gx$ such that $1x = x$ and $g(g'x) = (gg')x$). For any $x \in X$, there is a group $\mathrm{Stab}(x) = \{g \in G : gx = x\}$, the stabilizer. Now consider the intersection H of all these stabilizers. Then H is normal in G: in fact, for $h \in H$ and $g \in G$ we have $(g^{-1}hg)x = g^{-1}h(gx) = g^{-1}gx = x$, since h fixes everything (in particular gx), and therefore $g^{-1}hg \in H$.

Back to Projective Transformation.

Lemma 1.2. *Let A be a projective transformation represented by a a nonsingular 3×3-matrix $A=(a_{ij})$. Then the following assertions are equivalent:*

1. *The restriction of A to $\mathbb{A}^2=\{(x:y:1)\in\mathbb{P}^2\}$ is an affine transformation;*
2. *$a_{13}=a_{23}=0$;*
3. *A fixes the line $z=0$ at infinity.*

Proof. 1 $\iff$ 2: We have $[x:y:1]A=[x':y':z']$ with $z'=a_{13}x+a_{23}y+a_{33}$. If A induces an affine transformation, then we must have $z'\ne 0$ for all $x,y\in K$, and this implies $a_{13}=a_{23}=0$. Note that we automatically have $a_{33}\ne 0$, since $\det A\ne 0$. Thus we can rescale A to get $a_{33}=1$.

Conversely, if $a_{13}=a_{23}=0$ and $a_{33}=1$, then $A([x:y:1])=[x':y':1]$, where $x'=a_{11}x+a_{21}y+a_{31}$ and $y'=a_{12}x+a_{22}y+a_{32}$. This is an affine transformation.
2 $\iff$ 3: If $a_{31}=a_{32}=0$, then $A([x:y:0])=[x':y':0]$, hence the line $z=0$ is preserved. Conversely, if $A([x:y:0])=[x':y':0]$ for all $x,y\in K$, then $a_{31}=a_{32}=0$. □

This result shows that we have a lot more choice in the projective world; as an example, we have

Proposition 1.3. *Let $P_i=[x_i:y_i:z_i]$ $(i=1,2,3,4)$ be four points in the projective plane, no three of which are collinear. Then there is a unique projective transformation sending the standard frame, namely $[1:0:0]$, $[0:1:0]$, $[0:0:1]$ and $[1:1:1]$, to P_1, P_2, P_3 and P_4, respectively.*

Proof. The transformation defined by $A=(a_{ij})\in\mathrm{PGL}_3(K)$ will map $[1:0:0]$ to P_1 if and only if there is some $\alpha_1\in K^\times$ with

$$\alpha_1(x_1,y_1,z_1)=(1,0,0)A=(a_{11},a_{21},a_{31}).$$

This determines the first column of A up to some nonzero factor. Similarly, the second and the third columns are determined up to nonzero factors $\alpha_2,\alpha_3\in K^\times$ by the second and third condition. Thus the columns of A are given by α_1p_1, α_2p_2 and α_3p_3, where the p_i are vectors corresponding to the P_i. Now P_4 will be the image of $[1:1:1]$ if and only if $\alpha_4p_4=\alpha_1p_1+\alpha_2p_2+\alpha_3p_3$ (rescaling allows us to assume that $\alpha_4=1$). Now this is a linear system of three equations in three unknowns; since the vectors p_1, p_2, p_3 are linearly independent, there is a unique solution $(\alpha_1,\alpha_2,\alpha_3)$. Since p_4 is independent of any two out of p_1, p_2, p_3, the numbers α_i are all nonzero; this implies that the matrix A with columns α_ip_i $(i=1,2,3)$ is invertible, hence A defines a projective transformation. Finally, A is unique except for the rescaling $\alpha_4=1$, hence is unique as an element of $\mathrm{PGL}_3(K)$. □

This result has a number of important corollaries:

Corollary 1.4. *Let P_i and Q_i $(i=1,2,3,4)$ denote two sets of four points in the projective plane such that no three P_i and no three Q_i are collinear. Then there is a projective transformation sending P_i to Q_i for $i=1,2,3,4$.*

Proof. Let A denote the projective transformation that sends the standard frame to the P_i; let B denote the transformation that does the same with the Q_i. Then $A\circ B^{-1}$ is the projective transformation we are looking for. □

Projective transformations A act on projective planes and therefore on plane algebraic curves $\mathcal{C}_F : F(X,Y,Z) = 0$; the image of $\mathcal{C}$ under A is some curve $\mathcal{C}_G : G(U,V,W) = 0$. How can we compute G from F? Let us first look at a simple example. Take $F(X,Y,Z) = YZ - X^2$ and the transformation $[u : v : w] = [x : y : z]A = [x + y : y : z]$. For getting G, we solve for x, y, z, that is, put $[x : y : z] = [u : v : w]A^{-1}$ and then plug the result into F: $[x : y : z] = [u-v : y : z]$, hence $G(U,V,W) = F(U-V,V,W) = VW-(U-V)^2$. Thus we get G by evaluating F at $(X,Y,Z)A^{-1}$, that is, $G = F \circ A^{-1}$. This ensures that a point $[x : y : z]$ on $\mathcal{C}_F$ will get mapped by A to a point $[u : v : w] = [x : y : z]A$ on $\mathcal{C}_G$.

Proposition 1.5. *Projective transformations preserve the degree of curves.*

Proof. Projective transformations map a monomial $X^iY^iZ^k$ of degree $m = i+j+k$ either to 0 or to another homogeneous polynomial of degree m. If $f(X,Y,Z)$ is transformed by some transformation T into the zero polynomial, then the inverse transformation maps the zero polynomial into f, which is nonsense. □

Finally, let us talk a little bit about singular points. We have $F = G \circ A$, hence the chain rule implies that the derivative of F is the derivative of G with respect to the new variables multiplied by the derivative of the linear map $(u,v,w) = (x,y,z)A$, which is the matrix A itself. In symbols:

$$\Big(\frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}, \frac{\partial F}{\partial Z}\Big) = \Big(\frac{\partial G}{\partial U}, \frac{\partial G}{\partial V}, \frac{\partial G}{\partial W}\Big) \cdot A.$$

Now a point on $\mathcal{C}_F$ is singular if and only if all three derivatives vanish at some point $P = [x : y : z]$. Since the matrix A is nonsingular, this happens if and only if the point $[u : v : w] = [x : y : z]A$ is singular.

Proposition 1.6. *Projective transformations preserve singularities.*

With some more work it can also be shown that projective transformations also preserve multiplicities, tangents, flexes etc.

2. Projective Conics

Observe that this means that projective transformations map lines into lines and conics into conics. Affine transformations preserve the line at infinity, hence cannot map a (real) circle (no point at infinity) into a hyperbola (two points at infinity). Projective transformations can do this: the projective circle has equation $X^2 + Y^2 - Z^2 = 0$; the projective transformation $X = Y'$, $Y = Z'$, $Z = X'$ transforms this into $Y'^2 - X'^2 + Z'^2 = 0$, which, after dehomogenizing with respect to Z', is just the hyperbola $x^2 - y^2 = 1$. What happened here is that $Y = Z'$ has moved the two points with $Y = 0$ to infinity.

Similarly, the hyperbola $XY - Z^2 = 1$ can be transformed into a parabola via $X = Y'$, $Y = Z'$, $Z = X'$: after dehomogenizing we get $y = x^2$. The hyperbola had two points $[1 : 0 : 0]$ and $[0 : 1 : 0]$ at infinity; the first one was moved to the point $[0 : 1 : 0]$ at infinty, the second one to $[0 : 0 : 1]$, which is the origin in the affine plane. As a matter of fact it can easily be proved that, over the complex numbers (or any algebraically closed field of characteristic $\neq 2$), there is only one nondegenerate conic up to projective transformations.

Note that $f(X,Y,Z) = XYZ - XY^2$ is transformed into the zero polynomial by the singular transformation $X = X'$, $Y = X'$, $Z = X'$.

Let us call two conics projectively equivalent if there is a projective transformation mapping one to the other.

Proposition 2.1. *Any nondegenerate projective conic defined over some field K with at least one K-rational point is projectively equivalent to the conic*

$$XY + YZ + ZX = 0. \tag{1}$$

More exactly, given a nondegenerate conic $\mathcal{C}$ and three points on $\mathcal{C}$, there is a unique projective transformation mapping $\mathcal{C}$ to (1) and the three points to $[1:0:0]$, $[0:1:0]$ and $[0:0:1]$, respectively.

Proof. Take any three points on a conic (it has one K-rational point, hence a parametrization gives all of them; there are infinitely many over infinite fields and exactly $q+1$ over finite fields with q elements. Now observe that $q+1 \ge 3$). Then there is a projective transformation mapping them into $[1:0:0]$, $[0:1:0]$ and $[0:0:1]$, respectively (note that the three points on the conic are not collinear since the conic is degenerate). If the transformed conic has the equation

$$aX^2 + bXY + cY^2 + dYZ + eZX + fZ^2 = 0,$$

then we immediately see that $a = c = f = 0$. Moreover, $bde \ne 0$ since otherwise the conic is degenerate. Using the transformation $X' = dX$, $Y' = eY$, $Z = bZ'$, this becomes (1).

If there are two such maps A, B, then $B \circ A^{-1}$ maps the standard conic onto itself and preserves the three points of the standard frame. It is then easily seen that $B \circ A^{-1}$ must be the identity map in $\mathrm{PGL}(K)$. □

This result allows us to simplify computational proofs of a number of theorems in projective geometry. As an example, we prove Pascal's Theorem (1640); its analog for degenerate conics is due to Pappus of Alexandria (ca. 320). For its proof, we use a little

Lemma 2.2. *A point $P \in \mathbb{P}^2K$ different from $[0:0:1]$ is on the conic (1) if and only if there is some $r \in K$ such that $P = [r : 1-r : r(r-1)]$.*

Proof. The equation of the conic is $(x+y)z = -xy$. If $x+y = 0$, then $x = y = 0$ and thus $P = [0:0:1]$. Therefore we can rescale the coordinates such that $x + y = 1$. Write $x = r$; then $y = 1 - r$ and $z = -xy/(x+y) = r(r-1)$. Conversely, every point $[r : 1-r : r(r-1)]$ is easily seen to be on the conic. □

Theorem 2.3 (Pascal's Theorem)**.** *Let $ABCDEF$ be a hexagon inscribed in a nondegenerate conic. Then the points of intersection $X = AE \cap BF$, $Y = BD \cap CE$ and $Z = AD \cap CF$ are collinear.*

Proof. Since projective transformations preserve lines, conics, and points of intersection, we may assume that the conic has the form (1) and that $A = [1:0:0]$, $B = [0:1:0]$ and $C = [0:0:1]$. Now let $D = [d : 1-d : d(d-1)$, $E = [e : 1-e : e(e-1)]$ and $F = [f : 1-f : f(f-1)]$ and observe that $def \ne 0$.

Now we see

$$\begin{array}{lll} AE : ey + z = 0, & BF : (1-f)x + z = 0, & X = [e : 1-f : e(f-1)] \\ BD : (1-d)x + z = 0, & CE : (e-1)x + ey = 0, & Y = [e : 1-e : e(d-1)], \\ CF : (f-1)x + fy = 0, & AD : dy + z = 0, & Z = [f : 1-f : d(f-1)]. \end{array}$$

Now three points are collinear in $\mathbb{P}^2K$ if and only if the determinant whose columns are the coordinates of these points is 0. A standard calculation shows that this is the case. □

3. Conics over Finite Fields

Note that the conic $X^2 + Y^2 = 3Z^2$ does not have a point defined over $\mathbb{Q}$. Over finite fields, the situation is different:

Proposition 3.1. *Let $\mathcal{C}$ be a nondegenerate conic defined over a finite field $\mathbb{F}_p$. Then $\mathcal{C}(\mathbb{F}_p)$ contains an affine point defined over $\mathbb{F}_p$.*

In particular this implies that every nondegenerate conic over $\mathbb{F}_p$ is equivalent to the standard conic $XY + YZ + ZX = 0$.

Proof. The general conic is defined by an equation

$$ax^2 + bxy + cy^2 + dx + ey + f = 0. \tag{2}$$

Assume first that $p > 2$. If $c = 0$, the claim is clear (note that if $c = b = e = 0$, then the conic is degenerate). Assume therefore that $c \neq 0$. Multiplying through by a and completing the square shows that the substitution $x' = ax + \frac{b}{2}y$ leads to a new equation in which $b = 0$. Afterwards, we can get rid of the term aey by a similar trick. Finally, we can achieve that $c = 1$.

Thus we may assume that the conic has the form $y^2 = f(x)$ for some linear or quadratic polynomial f. If f is linear, it has a zero $x = r$, and $(r, 0)$ is a point on the affine conic.

If f is quadratic, it attains exactly $\frac{p+1}{2}$ different values (this is trivial for $f(x) = x^2$, to which the general case easily reduces). Since there are exactly $\frac{p-1}{2}$ nonsquares in $\mathbb{F}_p$, at least one of the values of f must be a square, say $f(r) = s^2$; then (r, s) is a point on the affine conic.

Now consider the case $p = 2$ and assume that the conic (2) defined over $\mathbb{F}_2$ does not have an affine point. Plugging in $x = 0$ we immediately see that we must have $c = e = f = 1$. Plugging in $y = 0$ we similarly get $a = d = 1$. Plugging in $x = 1$ finally gives $b = 0$. Thus the only conic without an affine point over $\mathbb{F}_2$ is $x^2 + y^2 + x + y + 1 = 0$. Its projective closure is $x^2 + y^2 + xz + yz + z^2$; it has three points at infinity, namely $[0 : 1 : 0]$, $[1 : 0 : 0]$ and $[1 : 1 : 0]$. Thus $\mathcal{C}$ contains the line at infinity and must be degenerate. In fact, the last point is singular. □

Thus there is essentially only one smooth conic with a K-rational point over K. Something similar does not hold for cubics: it can be shown that smooth cubics defined over K and with a K-rational point (such curves are called elliptic curves) can be transformed into cubics of Weierstrass form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

but the necessary transformations are in general not projective but birational. Thus the world of elliptic curves is much richer than that of conics.

4. Group Laws on Nonsingular Conics

Let $\mathcal{C}$ be a nondegenerate conic defined over some field K, and assume that $\mathcal{C}$ has a K-rational point, which we will denote by N. We then can define a group law on $\mathcal{C}(K)$ as follows: given $P, Q \in \mathcal{C}(K)$, let $P + Q$ be the second point of intersection

with $\mathcal{C}$ of the line through N parallel to PQ; if $P = Q$, the line PQ is taken to be the tangent at P.

This addition law is clearly abelian; the neutral element is N, and the inverse of a point P is the second point of intersection with $\mathcal{C}$ of the line through P parallel to the tangent at N.

It remains to show that the addition is associative. Assume that we are given points P, Q, R on the conic; let $A = P + Q$ and $B = Q + R$. Then $PQRANB$ is a hexagon on the conic. Moreover, we know that

- $PQ \parallel AN$ since $P + Q = A$, and
- $QR \parallel BN$ since $Q + R = B$.

Now associativity is equivalent to $A + R = P + B$, i.e. to $AR \parallel PB$. But since the points of intersection $PQ \cap AN$ and $QR \cap BN$ lie on the line at infinity, by Pascal's theorem the same must be true of $AR \cap PB$.

Note that this proof is only valid if no two of the six points P, Q, R, A, B, N coincide. The other cases must be handled one by one.