LECTURE 6, MONDAY 23.02.04

FRANZ LEMMERMEYER

Today we will discuss some 'simple' algebraic groups. In order to explain what they are, consider the category of differentiable manifolds whose morphisms are differentiable maps. A Lie group is a differentiable manifold that carries a group structure for which composition and forming the inverse are morphisms, i.e., differentiable maps (examples are the matrix groups GL $_n(\mathbb{R})$). Now algebraic groups are to algebraic varieties what Lie groups are to differentiable manifolds: algebraic varieties carrying a group structure for which composition and forming the inverse are morphisms, i.e. given by rational maps. There are two different types of algebraic groups: affine algebraic groups (linear algebraic groups) and projective algebraic groups (abelian varieties); we will see examples of both types here.

The above can be made precise using the language of categories. We will not need any of this; consider the following as a free contribution to your mathematical education.

Let C be a category with direct products (such as the category of sets (cartesian product), abelian groups (direct product), topological spaces (product space); the category of fields does not have a direct product, since the direct product of two fields is not a field) and a final object (objects p such that every object G has exactly one morphism $G \longrightarrow p$ (any set with one element is final in the category of sets; the final object in the category of groups is "the" group with one element, the zero group [there are of course a lot of such zero groups, but they are all isomorphic]; finally, the space consisting of one point and the discrete topology is a final object in the category of topological spaces. The category of fields with ring homomorphisms is an example for a category without final objects).

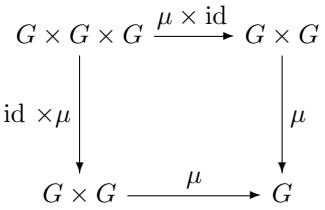
When generalizing concrete notions (like kernel, image, direct product, limits etc.) to categories, one has to find definitions that do not rely on elements (such as the definition of kernel as a set of elements that get mapped to 0) but only on morphisms. This may look strange at first, but after a while it actually becomes fun. Let us do this now for the concept of a group; the problem is to express the notion of composition, neutral element, inverse, and associativity in a language that avoids elements.

A group in C is an object G together with three morphisms

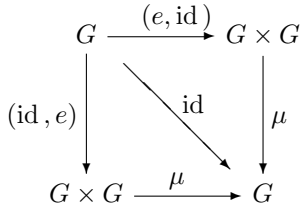
$$\begin{aligned} \mu &: G \times G \longrightarrow G, \\ \varepsilon &: p \longrightarrow G \\ \iota &: G \longrightarrow G \end{aligned}$$

such that the following diagrams commute:

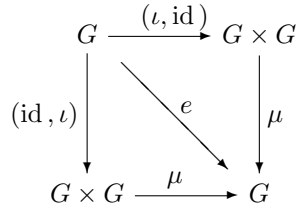
- associativity:



- neutral element:



- inverse:



Here $e : G \longrightarrow G$ is the composition of the unique morphism $G \longrightarrow p$ with ε.

Let us now work out what this means in a few categories. First consider the category of sets and let G be a group in the above sense. We claim that such groups are just the usual groups. In fact, we make the set G into an additive group $(G, +)$ by defining

- $a + b = \mu(a, b)$,
- $0 = \mathrm{im}\ \varepsilon$, and
- $-a = \iota(a)$.

Now we compute the maps in the diagrams. Associativity demands that $\mu \circ (\mu \times \mathrm{id})(a, b, c) = \mu \circ (\mathrm{id} \times \mu)(a, b, c)$, and in fact we get $\mu \circ (\mu \times \mathrm{id})(a, b, c) = \mu(a+b, c) = (a+b)+c$, as well as $\mu \circ (\mathrm{id} \times \mu)(a, b, c) = \mu(a, b+c) = a+(b+c)$. Both expressions agree for all $a, b, c \in G$ if and only if $+$ is associative. As usual when dealing with abstract nonsense, it is more fun to work these things out for yourself: just verify that the other two diagrams correspond to the existence of a neutral element and of inverses.

Next let C be the category of topological spaces. Then a group in C is a *topological group*: in addition to $(G, +)$ being a group, the conditions demand that μ and ι be continuous (note ε is automatically continuous since every subset of p is open).

category	group
sets	(usual) group
topological spaces	topological groups
differentiable manifolds	Lie groups
schemes over Spec R	group schemes

Algebraic groups as the groups in the category of geometrically reduced schemes of finite type over some field k. Whatever that means. For us, an algebraic group will be an affine or a projective variety with a group law for which composition and forming inverses are "polynomial" maps.

1. Group Laws on Lines

The Additive Group. The simplest way of defining a group law on a subset of the projective line $\mathbb{P}^1K$ is to take the affine part $K = \mathbb{P}^1K \setminus \{\infty\}$ and add points in K using the group structure of the additive group of K.

Note that $K = \mathbb{A}^1K$ is an affine algebraic variety, namely the affine zero set of the zero polynomial (or, if you don't like that, the zero set of $y = 0$ in $\mathbb{A}^2K$). Adding and forming the inverse are given by rational maps. The set K is usually denoted in three different ways: just K if we consider K as a field, $\mathbb{A}^1K$ if we consider it to be an algebraic variety, and $\mathbb{G}_a$ or $G_a(K)$ (for *additive* group) if we think of it as an algebraic group.

Note that the additive group law is defined not only over fields, but more generally over arbitrary (commutative) rings. Moreover, it has a simple geometric interpretation:

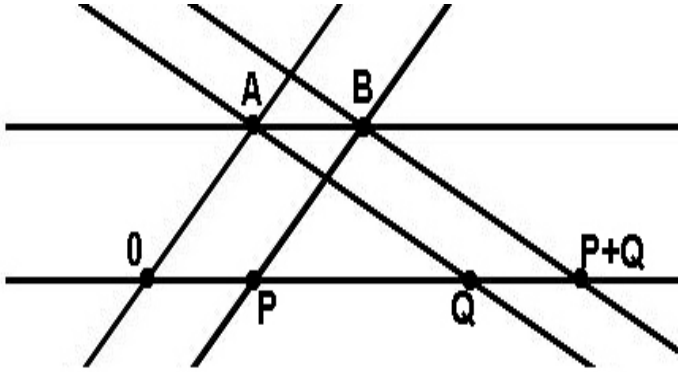


Figure 1. Group Law on the Unit Circle

Given a line with a fixed point 0, draw a parallel and pick any A on it; draw a parallel to $0A$ through P and call the second point of intersection B. Draw a parallel to AQ through B; the second point of intersection is $P + Q$.

The Multiplicative Group. The next simple thing to do is to take $K^\times = \mathbb{P}^1K \setminus \{\infty, 0\}$ and 'add' points using the multiplicative group $K^\times$.

Note that $K^\times$ is an algebraic variety, as it can be identified with the hyperbola $\mathcal{H} : XY = 1$ via the isomorphism $x \longmapsto (x, \frac{1}{x})$. Finally, if we want to view $K^\times$ as an algebraic group, we write $\mathbb{G}_m$ or $\mathbb{G}_m(K)$ instead of $K^\times$.

As above, the group law on $R^\times$ can be defined for arbitrary rings R. Again, there is a simple geometric interpretation of this group law:

On a line with fixed points 0 and 1, draw a line through 0 and choose some point A on it. Draw a parallel to $1A$ through Q and call the second point of intersection B. Draw a parallel to AP through B; the second point of intersection is PQ

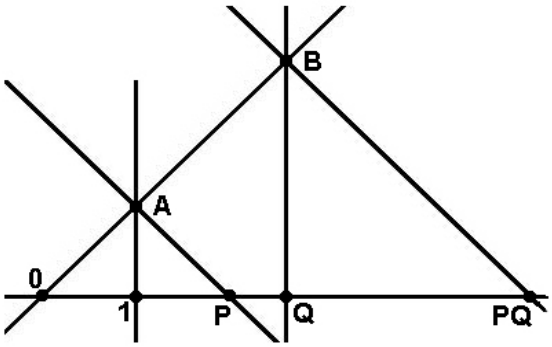


FIGURE 2. Group Law on the Unit Circle

The Twisted Multiplicative Group. Finally we claim that, for any nonsquare $a \in K$, the formula

$$[r:s] \oplus [t:u] = [rt + asu : ru + st] \tag{1}$$

defines an abelian group law on the projective line $\mathbb{P}^1K$ with neutral element $[1:0]$. That this definition is a 'natural' one will become clear only after we have made the connection to the group law on nonsingular conics and singular cubics.

If we want to view $\mathbb{P}^1K$ as an algebraic group, we usually denote it by $\mathbb{G}_m[1]$ and call it a twisted multiplicative group.

2. The Group Law on Pell Conics

Let $d \in \mathbb{Z}$ be a squarefree integer $\neq 1$, and put

$$\Delta = \begin{cases} d & \text{if } d \equiv 1 \bmod 4, \\ 4d & \text{if } d \equiv 2, 3 \bmod 4. \end{cases}$$

Then the affine curve $\mathcal{C} : X^2 - \Delta Y^2 = 4$ is called a Pell conic. Each Pell conic has integral points, namely $N = (2, 0)$ as well as $(-2, 0)$. We define a group law on the set of all rational points by saying $P + Q = R$ if the parallel to PQ through N intersects the conic in N and R.

Proposition 1. *The sum of the two points $P = (r, s)$ and $Q = (t, u)$ in $\mathcal{C}(\mathbb{Q})$ is*

$$P + Q = \begin{cases} \left(\frac{r^2+\Delta s^2}{2}, rs\right) = (r^2 - 2, rs) & \text{if } P = Q, \\ \left(2\frac{\Delta(s-u)^2+(r-t)^2}{\Delta(s-u)^2-(r-t)^2}\ ,\ 4\frac{(r-t)(s-u)}{\Delta(s-u)^2-(r-t)^2}\right) & \text{if } P \neq Q. \end{cases} \tag{2}$$

Observe that these formulas work in any field in which Δ is not a square; this condition guarantees that the denominator $\Delta(s-u)^2-(r-t)^2$ is nonzero whenever $P \neq Q$.

Proof. For adding the points $P = (r, s)$ and $Q = (t, u)$, we have to draw a parallel to the line PQ through N and compute its second point of intersection with $\mathcal{C}$. Lines through $N = (2, 0)$ have the equation $Y = m(X - 1)$.

If $P = Q$, then the slope m of the the tangent at P can be computed by taking the derivative of the curve equation and solving for Y'; we find $Y' = \frac{x}{\Delta y}$, hence

$m = \frac{r}{\Delta s}$ in $P = (r, s)$. A simple calculation yields $X = \frac{1}{2}(r^2 + \Delta s^2) = r^2 - 2$ and $Y = rs$.

Now assume that $P \neq Q$; if $r = t$, then $P = (r, s)$ and $Q = (r, -s)$, and the line through N parallel to PQ is tangent to N, that is, we have $P + Q = N$; this agrees with the formulas above.

Thus we may assume that $r \neq t$; the line through PQ has slope $m = \frac{s-u}{r-t}$. Intersecting this line with $\mathcal{C}$ leads to

$$(X - 2)\big[X + 2 - \Delta m^2(X - 2)\big] = 0;$$

since $X = 2$ gives the point N, the X-coordinate of the second point of intersection is given by

$$X = 2\frac{\Delta m^2 + 1}{\Delta m^2 - 1}.$$

Plugging in $m = \frac{s-u}{r-t}$, we find

$$P + Q = \Big(2\frac{\Delta(s-u)^2 + (r-t)^2}{\Delta(s-u)^2 - (r-t)^2}\ ,\ \frac{s-u}{r-t}(X-2)\Big).$$

Now observe that $\frac{s-u}{r-t}(X-2) = 4\frac{(r-t)(s-u)}{\Delta(s-u)^2-(r-t)^2}$. □

Since we are interested in the integral and not the rational solutions of Pell equations, the geometric group law does not seem to be very helpful. Fortunately, all is not lost:

Proposition 2. *The addition formula (2) is valid over $\mathbb{Z}$: we have*

$$2\frac{\Delta(s-u)^2 + (r-t)^2}{\Delta(s-u)^2 - (r-t)^2} = \frac{rt + \Delta su}{2}, \quad 4\frac{(r-t)(s-u)}{\Delta(s-u)^2 - (r-t)^2} = \frac{ru + st}{2},$$

hence $P + Q = (\frac{rt+\Delta su}{2}, \frac{ru+st}{2}) \in \mathcal{C}(\mathbb{Z})$ for points $P = (r, s)$ and $Q = (t, u)$ in $\mathcal{C}(\mathbb{Z})$.

Proof. There is nothing to show if $P = Q$ since, in this case, the coordinates of $P + Q$ are obviously integral.

Thus we only have to consider the case $P \neq Q$. We have to show that the denominator $\Delta(s-u)^2 - (r-t)^2$ divides the numerator. Now we can simplify this expression by observing

$$\Delta(s-u)^2 - (r-t)^2 = \Delta s^2 - r^2 + \Delta u^2 - t^2 + 2rt - 2\Delta su = 2(rt - \Delta su - 4).$$

Since $(rt - \Delta su - 4)(ru + st) = 4(r-t)(s-u)$, this gives

$$4\frac{(r-t)(s-u)}{\Delta(s-u)^2 - (r-t)^2} = 4\frac{(r-t)(s-u)}{2(rt - \Delta su - 4)} = \frac{(rt - \Delta su - 4)(ru + st)}{2(rt - \Delta su - 4)} = \frac{ru + st}{2}.$$

Observe that if $\Delta \equiv 1 \bmod 4$, then $r \equiv s, t \equiv u \bmod 2$, hence $ru + st \equiv 0 \bmod 2$.

Now let us look at the numerator of the x-coordinate; since

$$\begin{aligned} 4(r^2 + \Delta s^2 + t^2 + \Delta u^2) &= (t^2 - \Delta u^2)(r^2 + \Delta s^2) + (r^2 - \Delta s^2)(t^2 + \Delta u^2) \\ &= 2(r^2t^2 - \Delta^2 s^2 u^2) = 2(rt + \Delta su)(rt - \Delta su), \end{aligned}$$

we find

$$\begin{aligned} 2[\Delta(s-u)^2 + (r-t)^2] &= 2[r^2 + \Delta s^2 + t^2 + \Delta u^2 - 2(rt + \Delta su)] \\ &= (rt + \Delta su)(rt - \Delta su) - 4(rt + \Delta su)] \\ &= (rt + \Delta su)(rt - \Delta su - 4). \end{aligned}$$

This finally shows

$$2\frac{\Delta(s-u)^2+(r-t)^2}{\Delta(s-u)^2-(r-t)^2} = \frac{(rt+\Delta su)(rt-\Delta su-4)}{2(rt-\Delta su-4)} = \frac{rt+\Delta su}{2},$$

and now it follows as before that the x-coordinate of $P+Q$ is integral. □

These addition formulas also show that we have a group law over any ring in which 2 is a unit or a prime, such as $\mathbb{F}_q$ for odd prime powers q, the ring $\mathbb{Z}_p$ of p-adic integers and its quotient field $\mathbb{Q}_p$, or the rings $\mathbb{Z}_S$ of S-integers.

The group law on Pell conics has a well known algebraic interpretation: consider the maximal order $\mathcal{O}_K = \mathbb{Z}[\frac{1}{2}(\Delta+\sqrt{\Delta})]$ of the quadratic number field K with discriminant Δ; sending $(x,y) \in \mathcal{C}(\mathbb{Z})$ to the unit $\frac{1}{2}(x+y\sqrt{d}) \in \mathcal{O}_K^\times$ induces a bijection $\phi : \mathcal{C}(\mathbb{Z}) \longrightarrow \mathcal{O}_K^\times$.

Corollary 3. *The map ϕ defined above is an isomorphism of groups.*

Proof. Since ϕ is bijective, it is sufficient to show that it is a homomorphism; but this is clear from

$$\Big(\frac{r+s\sqrt{\Delta}}{2}\Big)\Big(\frac{t+u\sqrt{\Delta}}{2}\Big) = \frac{1}{2}\Big(\frac{rt+\Delta su}{2} + \frac{ru+st}{2}\sqrt{\Delta}\Big)$$

and Proposition 2. □