LECTURE 2, THURSDAY FEB. 12, 2004

FRANZ LEMMERMEYER

1. And now for something completely different ...

For the homework you need to know how to work with the finite field $\mathbb{F}_4$ with 4 elements. It is constructed as follows: start with $\mathbb{F}_2 = \{0, 1\}$ and pick a quadratic irreducible polynomial in $\mathbb{F}_2[X]$; there is only one: $f(X) = X^2 + X + 1$. Now form the ring $\mathbb{F}_2[X]/(f)$; since (f) is maximal, this is a field.

We can show this by hand as follows: the elements of $\mathbb{F}_2[X]/(f)$ are represented by polynomials of degree ≤ 1, since every X^2 occurring can be replaced by $X + 1$ in view of $X^2 \equiv -X - 1 = X + 1 \bmod f$. In general, two polynomials in $\mathbb{F}_2[X]$ give the same element in $\mathbb{F}_4$ if and only if their difference is divisible by f.

Thus we can write $\mathbb{F}_4 = \{0, 1, x, x + 1\}$, where $x = X + (f)$ is the residue class of X mod f. We find $x^2 = x + 1$ and $(x + 1)^2 = x^2 + 1 = x$. In this way, you can construct a multiplication table.

If you want to construct a field with 8 elements, pick a cubic irreducible polynomial in $\mathbb{F}_2[X]$, say $g(X) = X^3 + X + 1$, and set $\mathbb{F}_8 = \mathbb{F}_2[X]/(g)$. It has the elements $\{ax^2 + bx + c : a, b, c \in \mathbb{F}_2\}$.

2. Group Law

We will now present three different descriptions of the group law on the unit circle $\mathcal{C} : x^2 + y^2 = 1$; an algebraic, analytic and a geometric method.

The Algebraic Version. The algebraic group law is the one that can be described most easily: the sum of two points $P = (x, y)$ and $Q = (u, v)$ is simply defined to be

$$P + Q = (ux - vy, xv + yu). \tag{1}$$

It is then a trivial if tedious exercise to verify the group axioms. As usual, checking associativity is the hardest part; let us now describe a little pari program that does the trick.

Let us define three points $P_j = (x_j, y_j)$ $(j = 1, 2, 3)$; we then compute $P_1 + P_2 = (u, v)$ and $(P_1 + P_2) + P_3 = (w, z)$:

```
u=x1*x2-y1*y2:v=x1*y2+x2*y1:w=u*x3-v*y3:z=u*y3+v*x3
```

computes what we want; since pari only gives the last result as an output, you will have to type in `w` to see

$$\mathtt{w} = (\mathtt{x3} * \mathtt{y1} - \mathtt{y3} * \mathtt{y2}) * \mathtt{x1} + (-\mathtt{y3} * \mathtt{x2} * \mathtt{y1} - \mathtt{x3} * \mathtt{y2} * \mathtt{x2}),$$
$$\mathtt{z} = (\mathtt{x3} * \mathtt{y1} - \mathtt{y3} * \mathtt{y2}) * \mathtt{x1} + (-\mathtt{y3} * \mathtt{x2} * \mathtt{y1} - \mathtt{x3} * \mathtt{y2} * \mathtt{x2})$$

Now we compute $P_1 + (P_2 + P_3) = (w_1, z_1)$: set $P_2 + P_3 = (u_1, v_1)$; then

```
u1=x2*x3-y2*y3:v1=x2*y3+x3*y2:w1=u1*x1-v1*y1:z1=u1*y1+v1*x1
```

computes w_1 and z_1, and finally the commands `w-w1` and `z-z1` both produce 0, and associativity is proved.

The algebraic version has a complex interpretation: to a point (x, y) on the real unit circle, associate the complex number $\phi(x, y) = x+iy$ with absolute value 1; this is clearly a bijection with inverse map $\psi(x+iy) = (x, y)$. Since the set S^1 of complex numbers with absolute value 1 form a group with respect to multiplication, the bijection can be used to transport the group structure from S^1 to the points on the real unit circle. In fact, given two points $P = (x, y)$ and $Q = (u, v)$ on the unit circle, we can define their sum by mapping them to S^1, taking the product there, and mapping the product back to the unit circle, that is, we put $P+Q = \psi(\phi(P)\phi(Q))$. Using coordinates we find $\phi(P)\phi(Q) = (x + iy)(u + iv) = ux - vy + (xv + yu)i$, hence $P + Q$ is given by (1). Note that if P and Q are rational points, then so is $P + Q$. The neutral element of this operation is $N = (1, 0) = \phi(1)$.

The Analytic Version. We have seen above that the real points on the unit circle are parametrized by trigonometric functions: there is a bijection between the real interval $[0, 2\pi)$ and the unit circle S^1 via the map $\alpha \longmapsto (\cos\alpha, \sin\alpha)$. In more fancy terms, this map can be described as a bijective function $\mathbb{R}/2\pi\mathbb{Z} \longrightarrow S^1$; since $R/2\pi\mathbb{Z}$ is an abelian group under addition, we can make S^1 into a group by transport of structure: given two points $(x_j, y_j) \in S^1$ $(j = 1, 2)$, write $x_j = \cos\alpha_j$, $y_j = \sin\alpha_j$ and put $(x_1, x_2) + (x_2, y_2) = (x_3, y_3)$ with $x_3 = \cos(\alpha_1 + \alpha_2)$, $y_3 = \sin(\alpha_1 + \alpha_2)$.

The addition formulas for sine and cosine then imply that we can write $x_3 = x_1x_2 - y_1y_2$, $y_3 = x_1y_2 + x_2y_1$. Since $\mathbb{R}/2\pi\mathbb{Z}$ is a group, so is the unit circle by transport of structure.

The Geometric Version. The first thing to do when defining the geometric group law is choosing a neutral element. Any rational point on the unit circle will do, but in order to get the same group law as above we better pick $N = (1, 0)$. Given two points $P = (x, y)$ and $Q = (u, v)$, consider the parallel to PQ through N; it will intersect the unit circle in N and a second point (possibly coinciding with N) that we call $P + Q$.

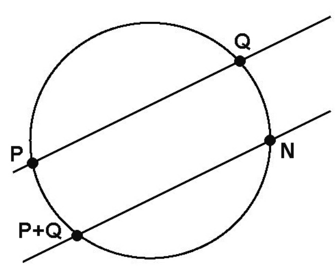

FIGURE 1. Group Law on the Unit Circle

It is easy to verify all group axioms with the exception of associativity: this requires a special case of Pascal's theorem in the general case. For circles, a simple geometric argument shows that the addition law just defined corresponds to adding angles: $\angle NO(P + Q) = \angle NOP + \angle NOQ$. It is also clear that the sum of two rational points has to be rational again, so we also get a group law on the set of rational points on $\mathcal{C}$.

Let us compute explicit formulas. First assume that P and Q have different x-coordinates. Then the slope of the line PQ is $m = \frac{y-v}{x-u}$. The line through $N = (1,0)$ with this slope is $Y = m(X-1)$, and intersecting it with $\mathcal{C}$ gives $0 = X^2 - 1 + m^2(X-1)^2 = (X-1)[X+1+m^2(X-1)]$. Thus the x-coordinate of $P+Q$ satisfies $X+1+m^2(X-1) = 0$, that is, $X = \frac{m^2-1}{m^2+1}$. Plugging in m we find

$$P + Q = \Big(\frac{(y-v)^2 - (x-u)^2}{(y-v)^2 + (x-u)^2}, -2\,\frac{(y-v)(x-u)}{(y-v)^2 + (x-u)^2}\Big). \tag{2}$$

This does not at all look like the addition formulas we computed from the algebraic definition – yet they are the same, as a simple calculation shows. We will later prove more generally that algebraic and geometric group laws on arbitrary non-degenerate conics coincide.