Elliptic Curves Example Sheet 2

Isaac Martin

Last compiled February 17, 2022

EXERCISE 1.

EXERCISE 2. Let A be an abelian group and let $q : A \to \mathbb{Z}$ be a map satisfying

$$q(x+y)-q(x-y) = 2q(x)+2q(y).$$

Prove that A is a quadratic form.

> *Proof:* Recall that to be a quadratic form, q must satisfy
>
> (i) $q(nx) = n^2 q(x)$ for all $x \in A$ and $n \in \mathbb{Z}$
>
> (ii) $\langle x,y\rangle = q(x+y)-q(x)-q(y)$ is a $\mathbb{Z}$-bilinear pairing.
>
> We prove these properties by induction.
>
> *(i)* Notice that $q(1\cdot x) = 1^2 q(x)$ trivially, $q(0+0)+q(0-0) = 2q(0)+2q(0)$ so $q(0) = 0$, and $q(2x) = 2q(x)+2q(x)-q(x-x) = 4q(x)$ for all $x \in A$; hence, (i) holds for $n = 0, 1$ and 2. Now suppose that (i) holds for all positive values k with $n > k > 2$. By induction,
>
> $$\begin{aligned} q(nx) &= 2q((n-1)x)+2q(x)-q((n-2)x) \\ &= 2(n-1)^2 q(x)+2q(x)-(n-2)^2 q(x) \\ &= (2n^2-4n+2+2-n^2+4n-4)q(x) = n^2 q(x), \end{aligned}$$
>
> so (i) holds for all values $n \geq 0$.
>
> Finally, if $n \geq 0$ then
>
> $$\begin{aligned} q(-nx) = q(x-(n+1)x) &= 2q(x)+2q((n+1)x)-q(x+(n+1)x) \\ &= 2q(x)+2(n+1)^2 q(x)-(n+2)^2 q(x) \\ &= (2+2n^2+4n+2-n^2-4n-4)q(x) = n^2 q(x). \end{aligned}$$
>
> This means $q(nx) = n^2 q(x)$ for all $n \in \mathbb{Z}$ and $x \in A$.
>
> *(ii)* Since the pairing $\langle x,y\rangle$ is invariant under the permutation $x \mapsto y$ and $y \mapsto x$, it suffices to prove that $\langle -,-\rangle$ is $\mathbb{Z}$ linear in the first coordinate, i.e. that $\langle nx,y\rangle n\langle x,y\rangle$ for all $n \in \mathbb{Z}$ and $x,y \in A$. We first treat the case that $n \geq 0$. This induction argument requires that the statement hold true for $n-1, n-2$ and $n-3$, so we need the cases that $n = 0, 1$ and 2 before proceeding to the induction step.
>
> $\underline{n=0}$: $\langle 0\cdot x,y\rangle = q(0\cdot x+y)-q(0\cdot x)-q(y) = q(y)-q(y) = 0 = 0\cdot\langle x,y\rangle$.
>
> $\underline{n=1}$: This is trivially satisfied.

$\underline{n=2}$: We invoke the equality $q(2x) = 4q(x)$ provided by (i) here.

$$\begin{aligned}\langle 2x,y\rangle &= q(2x+y) - q(2x) - q(y)\\ &= q(x+(x+y)) - q(2x) - q(y)\\ &= 2q(x) + 2q(x+y) - q(x-(x+y)) - 4q(x) - q(y)\\ &= 2q(x+y) - 2q(x) - q(-y) - q(y)\\ &= 2\big(q(x+y) - q(x) - q(y)\big) = 2\langle x,y\rangle.\end{aligned}$$

Assume now that $n > 2$ and that $\langle kx,y\rangle = k\langle x,y\rangle$ holds for $n > k \geq 0$. This means

$$\langle kx,y\rangle = q(kx+y) - q(kx) - q(y) = k\big(q(x+y) - q(x) - q(y)\big)$$

for $0 \leq k < n$ and so

$$\begin{aligned}q(kx+y) &= k\big(q(x+y) - q(x) - q(y)\big) + k^2 q(x) + q(y) \\ &= kq(x+y) + (k^2-k)q(x) - (k-1)q(y).\end{aligned} \tag{$*$}$$

We can now prove the desired statement:

$$\begin{aligned}\langle nx,y\rangle &= q(nx+y) - q(nx) - q(y)\\ &= 2q(x) + 2q\big((n-1)x+y\big) - q\big((n-2)x+y\big) - q(nx) - q(y)\\ &= 2q(x) + \overbrace{2(n-1)(q(x+y) + 2(n-1)(n-2)q(x) - 2(n-2)q(y))}^{2q\left((n-1)x+y\right) \text{ by } (*)}\\ &\quad - \overbrace{(n-2)q(x+y) - (n-2)(n-3)q(x) + (n-3)q(y)}^{-q\left((n-2)x+y\right) \text{ by } (*)} - n^2 q(x) - q(y)\\ &= \big(2(n-1) - (n-2)\big)q(x+y) + \big(2 + 2(n-1)(n-2) - (n-2)(n-3) - n^2\big)q(x)\\ &\quad + \big(-2(n-2) + (n+3) - 1\big)q(y)\\ &= nq(x+y) - nq(x) - nq(y)\\ &= n\langle x,y\rangle.\end{aligned}$$

We now must treat the case that $n < 0$. If $n = -1$ we get

$$\begin{aligned}\langle -x,y\rangle &= q(-x+y) - q(-x) - q(y)\\ &= 2q(x) + 2q(y) - q(x+y) - q(x) - q(y) = -\langle x,y\rangle\end{aligned}$$

without too much trouble. Using this together with the $n \geq 0$ case gives us

$$\langle -nx,y\rangle = -\langle nx,y\rangle$$

for $n \geq 0$, so we conclude that $\langle nx,y\rangle = n\langle x,y\rangle$ for all $n \in \mathbb{Z}$ and are done. $\square$

EXERCISE 3. Find a translation-invariant differential ω on the multiplicative group $\mathbb{G}_m$. Show that if $[n] : \mathbb{G}_m \to \mathbb{G}_m$ is the endomorphism $x \mapsto x^n$ then $[n]^*\omega = n\omega$.

Proof: An invariant differential of a formal group law $F \in R[\![X,Y]\!]$ is a differential form

$$\omega = P(T)dT \in R[\![T]\!]dT$$

which satisfies

$$\omega \circ F(T,S) = \omega(T)$$
$$\iff$$
$$P(F(T,S))F_X(T,S) = P(T)$$

where $F_X(T,S)$ is the partial derivative of F in the first variable. The formal group law of $\mathbb{G}_m$ is $F(X,Y) = X+Y+XY = (1+X)(1+Y)-1$, and its partial derivative in X is $F_X(X,Y) = 1+Y$. We are therefore looking for some $P(T) \in R[\![T]\!]$ such that

$$P((1+T)(1+S)-1)\cdot(1+S) = P(T).$$

It is fortunate that we discussed the element $\frac{1}{1-X} = 1+x+x^2+\ldots \in R[\![T]\!]$ in class – a slight modification, the power series $P(T) = \frac{1}{1+T} = 1-T+T^2-T^3+\ldots \in R[\![T]\!]$, will do the trick:

$$P((1+T)(1+S)-1)\cdot(1+S) = \frac{1}{(1+T)(1+S)-1+1}\cdot(1+S) = \frac{1}{1+T} = P(T).$$

Hence the differential form $\omega = \frac{1}{1+T}$ is an invariant differential of the multiplicative formal group law. $\square$