Formulae for the group law

We have described the gp. law on $E(K)$ for all K. In homework, you will compute some examples. However, it is rather time consuming. To make things more efficient (& also for proving some things) it is useful to have 'formulae' for the group law, as follows.

Throughout, we fix ~~an~~ a field k and an elliptic curve (E, O) over k.

Prop: Let $K \supseteq k$ and $p = [(x_p, y_p, 1)] \in E(K)$. Then $-p = [(x_p, -y_p, 1)]$.

Pf: From pf of Thm, have $-p = p * (O * O)$. Let's compute $O * O$:

We need a line L in $\mathbb{P}^2_{\bar{k}}$ such that $L \cdot E = 2[O] + [q]$ for some q.

Let L be given by $z = 0$ (so $L = V^p_{(z)}$). We find the naive intersection $L \cdot E$ is exactly the point O. Then Bezoult tells us

$$L \cdot E = 3 \cdot [O] \quad \text{(can also check 'by hand')},$$

So $O * O = O$.

Next, compute $p * (O * O) = p * O$. Let M be the line $x - x_p \cdot z = 0$.

Then the naive intersection $M \cdot E$ is either:

1) $O \cup p \cup (x_p, -y_p, 1)$ if $y_p \neq 0$.

2) $O \cup p$ if $y_p = 0$.

In case (1), Bezoult implies $M \cdot E = [O] + [p] + [(x_p, -y_p, 1)]$, done

In case (2), need to compute something. Let's do $i_p(E, M)$. Find

$$i_p(E, M) = \dim_{\bar{k}} \frac{\bar{k}[x,y]_{(y, x-x_p)}}{(y^2 - (x^3 + ax^2 + bx + c), x - x_p)} = \dim_{\bar{k}} \frac{\bar{k}[x,y]_{(y, x-x_p)}}{(y^2, x - x_p)} = \dim_{\bar{k}} \bar{k}[y]/y^2$$

$$= 2.$$

(18) So Bezout tells us $M.E = 2[P]+[O]$, so again $-P = [(x_P, -y_P, 1)]$. □

What about adding points? Notation $[(x_P, y, z)] =: (x:y:z)$.

Again, E/k, now $P_1 = (x_1 : y_1 : 1)$

$$P_2 = (x_2 : y_2 : 1)$$

$$P_1 * P_2 = (x_3 : y_3 : 1) \quad \{\text{Say } P_1 \neq -P_2, \text{ so makes sense}\}$$

$$P_1 + P_2 = (x_3 : -y_3 : 1)$$

Say $P_1 \neq P_2$.

Line L joining P_1 & P_2 can be given by:

$$(y_2 - y_1)x + (x_1 - x_2)y + [y_1(x_2 - x_1) - x_1(y_2 - y_1)]z = 0$$

Set $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$, $\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$,

so L given by $y = \lambda x + \nu z$.

Set $z = 1$ to simplify, & substitute into $y^2 = x^3 + ax^2 + bx + c$;

get
$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + (c - \nu^2) = 0.$$

This has roots x_1, x_2 & x_3. Hence $x_1 + x_2 + x_3 = \lambda^2 - a$,

so
$$x_3 = \lambda^2 - a - x_1 - x_2, \quad y_3 = \lambda x_3 + \nu.$$

What if $P_1 = P_2$? Similar arguments, omitted. Result:
(if $2P_1 \neq 0$):

$$x_3 = \frac{x_1^4 - 2bx_1^2 - 8cx_1 + b^2 - 4ac}{4x_1^3 + 4ax_1^2 + 4bx_1 + 4c.}$$ 'duplication formula'

$= 0$ iff ~~$f(x_1) = 0$~~ $x_1^3 + ax^2 + \dots = 0$, since char $k \neq 2$.

$y_3 = \dots$ ~~an~~ mess...

In theory, could prove associativity using these formulae... Not fun! Also not illuminating.

Points of order 2 ~~& 4~~ ~~& ...~~ & 3.

To get more used to working with ECs, & to see a few basic things abt. gp law, let's look at ~~pts~~ some pts of small order.

Order 2: Say $2 \cdot p = 0$. Then $p = -p$, so ~~if $P \neq 0$~~ $p = (x_p : 0 : 1)$.

There are exactly 3 such pts over $\bar{k}$, the roots of $x^3 + ax^2 + bx + c$ (note E non-sing $\Rightarrow$ these roots are distinct). They all have order 2, since none are O.

Def: let $n \in \mathbb{Z}_{>0}$, let $E/_k$ and $K \supseteq k$. ~~th~~ We write

$E(K)[n]$ for the points ~~of order~~ in $E(K)$ killed by multiplication by n.

Ex: $E(K)[n]$ is a subgroup of $E(K)$.

We see $\# E(\bar{k})[2] = 4$. Moreover, all pts except O have order 2, so

$$E(\bar{k})[2] \cong \mathbb{Z}/_{2\mathbb{Z}} \times \mathbb{Z}/_{2\mathbb{Z}}.$$ Note char $k \neq 2$.

Similarly (using that p of order 3 $\Rightarrow x(p) = x(2p)$), we find that

$$E(\bar{k})[3] \cong \mathbb{Z}/_{3\mathbb{Z}} \times \mathbb{Z}/_{3\mathbb{Z}}$$ if char $k \neq 3$.

~~Thm: k a field, (E,O) $EC/_k$, $n \in \mathbb{Z}_{>0}$, $K \supseteq k$. Then $E(K)[n]$ is finite.~~

~~Pf: Wlog $K = k = \overline{k}$.~~

~~Claim: Let $r>0$. Then there is at least one point of order 2^r.~~

~~Proof: Substitute the 'duplication polynomial' into itself r times, yielding a rat fctn $\psi \in k(x)$ such that~~

~~$$\psi(x_p) = x(2^n \cdot p).$$~~

Order 3:

- If $3p=0$ then $2p=-p$, so $x(2p)=x(-p)=x(p)$.

- If $x(2p)=x(p)$, then $2p=\pm p$. If $2p=p$ then $p=0$.

Hence if $p \neq 0$ then $3p=0 \iff x(2p)=x(p)$.

Using formula for $x(2p)$, we find that $3p=0$ iff $\psi_3(x(p))=0$, where

$$\psi_3(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + (4ac-b^2).$$

I claim this has distinct roots if char $k \neq 3$. Indeed, if $E: y^2 = f(x)$, we can write

$$\psi_3(x) = 2f(x)f''(x) - f'(x)^2, \text{ so}$$

$$\psi_3'(x) = 2f(x)f'''(x) = 12f(x),$$

so a common root of $\psi_3(x)$ & $\psi_3'(x)$ would be a common root of $2f(x)f''(x) - f'(x)^2$ & $12f(x)$, so would be a common root of $f(x)$ & $f'(x)$ (here use char $k \neq 3$) contradicting smoothness of E.

So there are $2 \cdot 4 = 8$ points of order 3 over $k = \bar{k}$, char $k \neq 3$, so

$$\# E(\bar{k})[3] = 8 + 1 = 9, \quad \& \text{ so } \quad E(\bar{k})[3] \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

In general:

Thm: $k = \bar{k}$ a field, $(E, O)/k$ elliptic, ~~[illegible]~~ p prime number, $r \geq 1$.

- If $p \in k^\times$ then $E(k)[p^r] \simeq \mathbb{Z}/p^r \times \mathbb{Z}/p^r$
- If $p = 0$ in k then $E(k)[p] \simeq \mathbb{Z}/p^r$ or 0.

Pf omitted. Not deep, but no super easy proofs I know of. $\boxtimes$

(22) Elliptic curves over finite fields

For this section, k is finite, & (E,O) an $EC/_k$.
$\#k = q$

- Note $E(k)$ finite, since $E(k) \subseteq \mathbb{P}^2(k)$, $\#\mathbb{P}^2(k) = q^2+q+1$.
- In fact, $E \setminus O \subseteq \mathbb{A}^2(k)$, so $\#E(k) \leq q^2+1$.
- $O \in E(k)$, so $\#E(k) \geq 1$.
- Apart from O, only q possible x-coords, & each with ≤ 2 y-coords,

  so $\quad \#E(k) \leq 2q+1$.

Can one do better?

Thm (Hasse, Weil): $\quad \left|\#E(k) - q - 1\right| \leq 2\sqrt{q}$.

Pf: Omitted, quite hard. Follows immediately from Weil conjectures [Deligne] $\square$