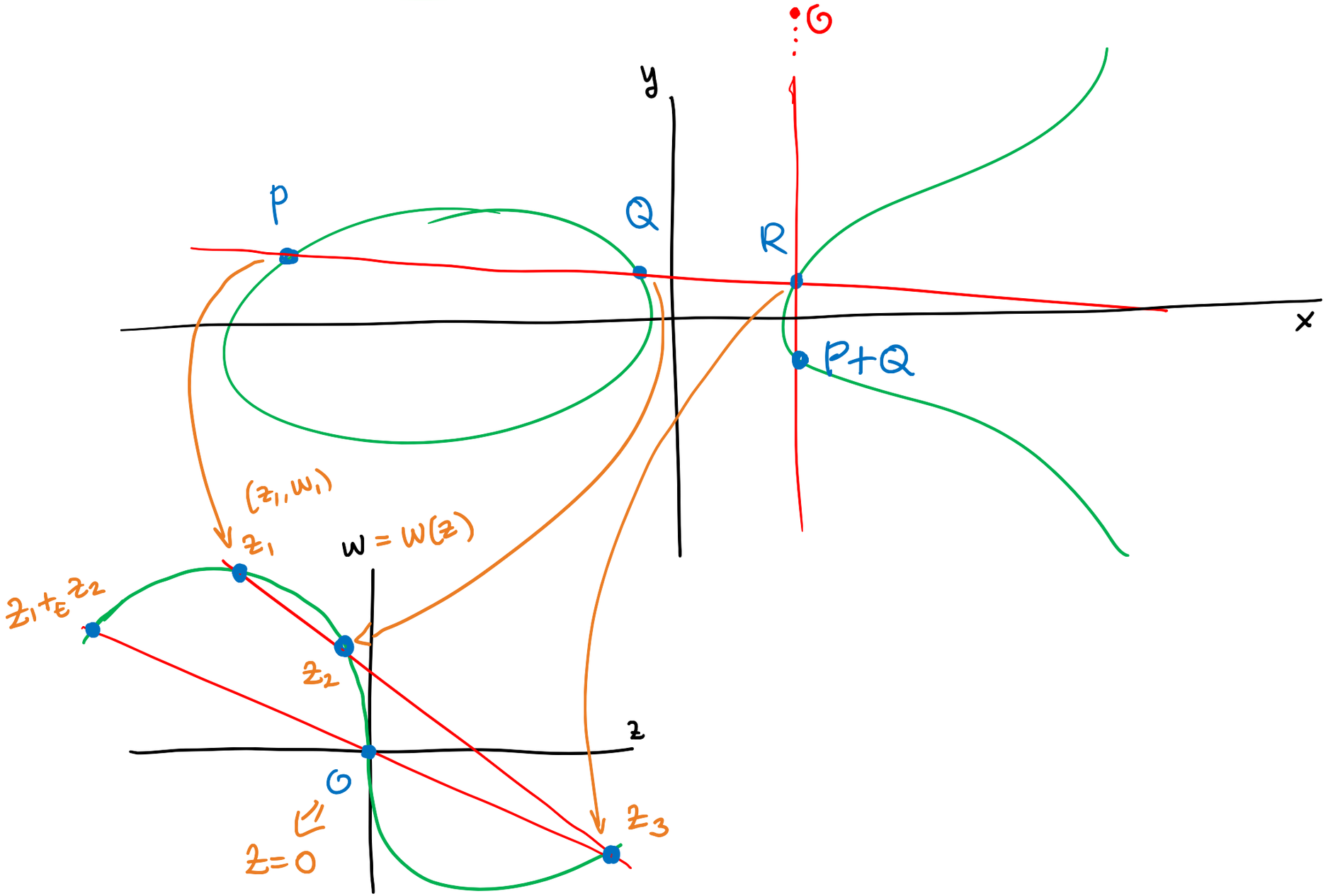
Last time: Intro. to Formal Groups



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

$$w = z^3 + a_1zw + a_2z^2w + a_3w^2 + a_4zw^2 + a_6w^3 = f(z,w)$$

Recursively solve $w = f(z,w)$:

$$w(z) = w = z^3(1 + A_1z + A_2z^2 + \dots) \in \mathbb{Z}[a_1,\dots,a_6][[z]]$$

- $$x(z) = \frac{z}{w(z)} = \frac{1}{z^2} - \frac{a_1}{z} - a_2 - a_3z - (a_4 + a_1a_3)z^2 + \dots$$
- $$y(z) = -\frac{1}{w(z)} = -\frac{1}{z^3} + \frac{a_1}{z^2} + \frac{a_2}{z} + a_3 + (a_4 + a_1a_3)z + \dots$$
- $$\omega(z) = (1 + a_1z + (a_1^2 + a_2)z^2 + \dots)\,dz$$
- $$\text{“}z_1 +_E z_2\text{”} = F(z_1,z_2) = z_1 + z_2 - a_1z_1z_2 - a_2(z_1^2z_2 + z_1z_2^2) + \dots$$

is commutative, associative, there is additive inverses, 0 is neutral.

Formal Groups

Let R be a ring.

Def. A (one-parameter, commutative) formal group $\mathcal{F}$ defined over R is a power series $F(X,Y) \in R[\![X,Y]\!]$ satisfying:

(a) $F(X,Y) = X + Y + (\text{terms of deg} \geq 2)$

(b) $F(X, F(Y,Z)) = F(F(X,Y), Z)$ (associativity)

(c) $F(X,Y) = F(Y,X)$ (commutativity)

(d) $\exists!\, i(T) \in R[\![T]\!]$ s.t. $F(T, i(T)) = 0$ (existence of inverses)

(e) $F(X,0) = X$, $F(0,Y) = Y$. (existence of neutral elt.)

$X +_F Y := F(X,Y)$

$X +_F (Y +_F Z) = (X +_F Y) +_F Z$

We call F the formal gp. law of $\mathcal{F}$. $(\mathcal{F}, F)$

Rmk (a) + (b) $\Rightarrow$ (d) + (e), if R has no torsion nilpotents, then (a+b) $\Rightarrow$ (c,d,e).

Def. Let $(\mathcal{F}, F), (\mathcal{G}, G)$ be formal gps over R.

Then, a homomorphism $f: (\mathcal{F}, F) \to (\mathcal{G}, G)$ is

a power series $f(T) \in R[\![T]\!]$ s.t.

$$f(F(X,Y)) = G(f(X), f(Y))$$

"$f(X +_F Y) = f(X) +_G f(Y)$."

$(\mathcal{F}, F)$ and $(\mathcal{G}, G)$ are isomorphic if there are homs. $f: \mathcal{F} \to \mathcal{G}$, $g: \mathcal{G} \to \mathcal{F}$

s.t. $f(g(T)) = g(f(T)) = T$.

exercise: Find $i(T)$ for $\hat{\mathbb{G}}_m$

ex Formal additive group $\hat{\mathbb{G}}_a$ w/ $F(X,Y) = X + Y$.

ex Formal multiplicative group $\hat{\mathbb{G}}_m$ w/ $F(X,Y) = X + Y + XY$

$= (1+X)(1+Y) - 1$.

ex E/R, $\hat{E}$ w/ $F(z_1, z_2)$, the add. law we saw last time.

ex $(\mathcal{F}, F)$ $[m]: \mathcal{F} \to \mathcal{F}$ inductively: $[0](T) = 0$, $[m+1](T) = F([m]T, T)$

$m \in \mathbb{Z}$ $[m-1](T) = F([m]T, i(T))$.

Prop Let $(\mathcal{F}, F)$ be a formal gp / R. → Hot

(a) $[m](T) = m \cdot T + (\text{higher order terms})$

(b) If $m \in R^\times$, then $[m] : \mathcal{F} \to \mathcal{F}$ is an isomorphism.

(ex $R = \mathbb{Z}_p$, $R^\times = \mathbb{Z}_p - p\mathbb{Z}_p$ "$\{u \in \mathbb{Z}_p : u \not\equiv 0 \bmod p\}$")

Pf.

(a) $m \geq 0$ induction using $F(X,Y) = X + Y + \cdots$

$m < 0$ use $0 = F(T, i(T)) = T + i(T) + \cdots \to i(T) = -T + \cdots$

(b) Use:

[**Lemma** Let $a \in R^\times$, and $f \in R[[T]]$, s.t. $f(T) = aT + \cdots$
Then $\exists!\ g \in R[[T]]$ s.t. $f(g(T)) = T$ (and $g(f(T)) = T$).]

Since $m \in R^\times$, $[m]T = mT + \cdots = f(T) \overset{\text{Lemma}}{\Longrightarrow} \exists!\ g(T)$ s.t. $f(g(T)) = g(f(T)) = T$.

NEED! $g(F(X,Y)) = F(g(X), g(Y))$

$f(T) = [m](T)$ is a hom $\Longrightarrow$ $f(F(X,Y)) = F(f(X), f(Y))$

$\Longrightarrow$ $f(F(g(X), g(Y))) = F(\underbrace{f(g(X))}_{\text{id}}, \underbrace{f(g(Y))}_{\text{id}})$

$\Longrightarrow$ $f(F(g(x), g(x)) = F(x, y)$

$\Longrightarrow$ $\underbrace{g}_{\text{id}}(f(F(g(x), g(y)))) = g(F(x,y))$

$\longrightarrow$ $\boxed{F(g(x), g(y)) = g(F(x,y)).}$

$\Longrightarrow g$ is a hom. $\Longrightarrow [m]$ is an iso.

Groups Assoc. to Formal groups.

R a complete local ring wrt the maximal ideal $\mathfrak{m} \subseteq R$.

$k = R/\mathfrak{m}$ residue field

$\mathcal{F}$ a formal gp over R, w/ law $F(X,Y)$

$R = \mathbb{Z}_p$
$\mathfrak{m} = p\mathbb{Z}_p$
$k \cong \mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$.

Def The group associated to $(\mathcal{F}, F)$, denoted $\mathcal{F}(\mathfrak{m})$, is the set $\mathfrak{m}$ with operations

$x \oplus y = F(x,y)$ for any $x, y \in \mathfrak{m}$

$\ominus x = i(x)$ for $x \in \mathfrak{m}$.

ex Formal add. gp $\hat{\mathbb{G}}_a$

$\hat{\mathbb{G}}_a(\mathfrak{m}) = (\mathfrak{m}, +)$

NOTE: Fits in an exact sequence

$$0 \to \hat{\mathbb{G}}_a(\mathfrak{m}) \to R \longrightarrow k \to 0$$

ex Formal mult. gp $\widehat{\mathbb{G}}_m$

$$\widehat{\mathbb{G}}_m(\mathfrak{m}) \cong (1+\mathfrak{m}, \times)$$

NOTE: Fits in $0 \to \widehat{\mathbb{G}}_m(\mathfrak{m}) \to R^\times \to k^* \to 0$

ex $R = \mathbb{Z}_p$ $\quad 0 \to 1+p\mathbb{Z}_p \to \mathbb{Z}_p^\times \to \mathbb{F}_p^* \to 0$

ex $E/R \rightsquigarrow \hat{E}(\mathfrak{m})$ $\quad$ Recall: $\mathfrak{m} \hookrightarrow E(K)$

K = fract. fld of R $\quad \hat{E}(\mathfrak{m}) \xrightarrow[\text{hom}]{} E(k)$

(Also! $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ $\quad E(\mathbb{Q}) \subseteq E(\mathbb{Q}_p)$)

OFTEN!

$$0 \to \hat{E}(\mathfrak{m}) \to \underbrace{E(k)}_{E/K} \to \underbrace{\tilde{E}(k)}_{\tilde{E}/k} \to 0 \quad ??$$

exact??

ell. curve??

More on Formal Groups.

Prop (a) For each $n \geq 1$ the map $\mathcal{F}(\mathfrak{m}^n)/\mathcal{F}(\mathfrak{m}^{n+1}) \xrightarrow{\psi} \mathfrak{m}^n/\mathfrak{m}^{n+1}$ induced by the identity map on sets is an isom. of groups.

(b) Let $p = \mathrm{char}(k)$. Then every torsion elt. of $\mathcal{F}(\mathfrak{m})$ has order a power of p.

Pf. (a) Underlying sets of elts. are the same, suffices to prove hom:

$$x \oplus y = F(x,y) = x + y + \text{HOT} \equiv x + y \bmod \mathfrak{m}^{2n}.$$

($x, y \in \mathfrak{m}^n$)

$$\psi(x \oplus y) \equiv x + y \bmod \mathfrak{m}^{n+1}.$$

$R = \mathbb{Z}_p$, $\mathfrak{m} = p\mathbb{Z}_p$; $R/\mathfrak{m} = k$; $R \to R/\mathfrak{m}$, $m \to m \bmod \mathfrak{m}$, $m \neq 0$ in k

(b) It suffices to show there are no elts. of order m prime to p. ($\gcd(m,p)=1$)

Suppose $x \in \mathcal{F}(\mathfrak{m})[m]$ so $[m](x) = 0$. Since $(m,p)=1 \Rightarrow m \notin \mathfrak{m}$

$\Rightarrow [m]: \mathcal{F} \to \mathcal{F}$ iso! $\Rightarrow$ induces $[m]: \mathcal{F}(\mathfrak{m}) \to \mathcal{F}(\mathfrak{m})$ iso!

$\Rightarrow$ kernel $[m]$ is trivial $\to x = 0$. ▨

Def Let $(\mathcal{F}, F)$ a formal gp over R.

An invariant differential of $\mathcal{F}/R$ is a diff. form:

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

s.t. $\omega(F(T,S)) = \omega(T)$ (invariant)

i.e., $P(F(T,S))\,\frac{d}{dx}F(T,S) = P(T)$

We say $\omega(T)$ is normalized if $P(0) = 1$.

ex $(\hat{\mathbb{G}}_a, F(X,Y) = X+Y)$ $\omega = dT$

ex $(\hat{\mathbb{G}}_m, F(X,Y) = X+Y+XY)$ $\omega = \frac{1}{1+T}\,dT = (1 - T + T^2 - \dots)\,dT$

Cor 4.4. Let $\mathcal{F}/R$ be a f.g., p prime.

There exist $f(T), g(T) \in R[[T]]$ w/ $f(0) = g(0) = 0$ s.t.

$$[p](T) = p \cdot f(T) + g(T^p).$$

ex $\hat{E}$ $\quad [3](T) = 3 \cdot \left(T - a_1 T^2 + (4a_1 a_2 - 13 a_3) T^4 + \dots \right)$

$$+ \left((a_1^2 - 8a_2) T^3 + (\dots) T^6 + \dots \right)$$

Def R of char $=0$, $K = R \otimes \mathbb{Q}$, $\mathcal{F}/R$ formal gp.

$$\omega(T) = (1 + c_1 T + c_2 T^2 + \dots)\, dT$$

The formal logarithm of $\mathcal{F}/R$ is

$$\log_{\mathcal{F}}(T) = \int \omega(T) = T + \frac{c_1}{2} T^2 + \frac{c_2}{3} T^3 + \dots \in K[[T]]$$

$1 \cdot T + \dots$

The formal exponential of $\mathcal{F}/R$ is the unique power series $\exp_{\mathcal{F}}(T) \in K[\![T]\!]$

$$\text{s.t. } \log_{\mathcal{F}} \circ \exp_{\mathcal{F}}(T) = \exp_{\mathcal{F}} \circ \log_{\mathcal{F}}(T) = T.$$

ex $\widehat{\mathbb{G}}_m \qquad \omega_{\mathcal{F}} = \frac{1}{1+T}\,dT$

$$\text{so } \log_{\mathcal{F}}(T) = \int \frac{1}{1+T}\,dT = \sum_{n=1}^{\infty} (-1)^n \frac{T^n}{n} \quad \left(= \log(1+T)\right)$$

$$\exp_{\mathcal{F}}(T) = \sum_{n=1}^{\infty} \frac{T^n}{n!} \quad \left(= e^T - 1\right)$$