INTRODUCTION

We now want to study elliptic curves. A full treatment would require algebraic geometry, which is beyond the scope of this course; however, we can get a basic understanding using analytic and projective geometry. I will discuss this geometric foundation before Zach applies it to elliptic curves.

CUBICS AND ELLIPTIC CURVES

Define $\boxed{\mathbb{P}_2(\mathbb{C})}$ as the complex projective plane, namely

$$\{(X, Y, Z) \in \mathbb{C}^3 \setminus \{(0,0,0)\} : (X, Y, Z) \equiv (\lambda X, \lambda Y, \lambda Z),\ \lambda \in \mathbb{C} \setminus \{0\}\}$$

Define a $\boxed{\text{curve } F}$ given by $F(x, y, z) = 0$ as an element of $\mathbb{P}(k[X, Y, Z]_d)$, the projective space of the (k-vector) space of homogeneous polynomials of degree d in X, Y, Z.

Define a $\boxed{\text{line}}$ as a curve with $d=1$, $\boxed{\text{conic}}$ as $d=2$, and $\boxed{\text{cubic}}$ as $d=3$.

Define a $\boxed{\text{decomposition}}$ of a curve as a factoring into unions of lower-degree curves.

Define F $\boxed{\text{absolutely irreducible}}$ to mean $F \in k[X,Y,Z]$ is irreducible in the algebraic closure $\bar{k}[X,Y,Z]$.

Define $P=(a,b,c) \in F(\bar{k})$ as $\boxed{\text{singular}}$ to mean $\frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial F}{\partial Z}(P) = 0$.

Define a $\boxed{\text{simple}}$ P to mean nonsingular, and a $\boxed{\text{smooth}}$ curve to mean P simple $\forall P \in \mathbb{P}_2(\bar{k})$.

→ If $P \in F \cap G$ for plane curves F, G then P is singular in the curve FG.

(Proof: $\forall u \in \{X, Y, Z\}$ have
$$\frac{\partial (FG)}{\partial u}(P) = \frac{\partial F}{\partial u}(P)\, G(P) + F(P)\frac{\partial G}{\partial u}(P),$$
and by defn of singular, RHS $= 0+0=0$.)

→ If $F(\bar{k})$ is smooth then F is absolutely irreducible.

Define an $\boxed{\text{elliptic curve}}$ over k as a smooth cubic F s.t. $F(k) \neq \emptyset$.

(Example: for what fields is $Y^2Z - X^3$ an elliptic curve?)

→ If $F \in k[X,Y,Z]_d$, $F = GH \neq 0$, $G \in k[X,Y,Z] \setminus k$, and $H \in k[X,Y,Z] \setminus k$, then G and H are homogenous.

(Proof: set $F = GH$, consider indeterminate T s.t. $(X,Y,Z) \to (TX, TY, TZ)$. Exercise (answer p. 176).)

→ If $F = \prod_{i=1}^{r} F_i^{e_i}$, the decomposition into a product of irreducible ~~factors~~ components in $\bar{k}[X, Y, Z]$, then F_i homogeneous $\forall i$, and $F(\bar{k}) = \bigcup_{i=1}^{r} F_i(\bar{k})$.

Define the $\boxed{\text{dehomogenization}}$ of F in Z as $F_b(x, y) := F(x, y, 1)$.

Define the order of multiplicity $\boxed{m_P(F)}$ of P on F as the smallest index i s.t. $F_i(X, Y) \not\equiv 0$.

Define a rational map $\boxed{F \dashrightarrow G}$ as $\varphi(P) = (A(P), B(P), C(P))$ for all but finitely many $P \in F(\bar{k}) \to G(\bar{k})$, where A, B, C are homogeneous polynomials of the same degree in $k[X, Y, Z]$.

(Example: $F = Z$, $G = Y^2 - XZ$, $\varphi(x, y, z) = (x^2, xy, y^2)$)

→ If F is smooth then φ is defined $\forall P \in F(\bar{k})$.

→ If F is singular then φ is defined $\forall P \in F(\bar{k})$ s.t. P is ~~nonsingular~~ simple.

Define rational $\varphi : F \dashrightarrow G$ as $\boxed{\text{birational}}$ if $\exists \psi : G \dashrightarrow F$ rational map s.t. $\psi \circ \varphi = \varphi \circ \psi = id$.

Define $\boxed{\text{elliptic curve equivalence}}$ as the existence of such a birational map.

BÉZOUT'S THEOREM

Define $\boxed{\mathcal{O}_P}$ as the local ring of P in $\overline{K}^2$, i.e.

$\{U(x,y)/V(x,y) : U,V \in \overline{K}[X,Y],\ V(0,0) \neq 0\}$.

Define $\boxed{(F_b, G_b)}$ as the ideal generated by F_b and G_b in $\mathcal{O}_P$.

Define the intersection multiplicity of F and G at P as the integer $\boxed{\mu_P(F,G)} = \dim_{\overline{K}} \mathcal{O}_P/(F_b, G_b)$.

→ $\boxed{\text{Bézout's Theorem}}$: if F and G are two algebraic plane curves in $\mathbb{P}_2(\overline{K})$ of degree m and n with no common component, then $\sum_{P \in \mathbb{P}_2(\overline{K})} \mu_P(F,G) = mn$.

→ $\mu_P(F,G)$ has the following 7 properties:

1) $\mu_P \in \mathbb{N} \cup \{\infty\}$, $\mu_P < \infty$ iff F, G have no common component containing P.

2) $\mu_P = 0$ iff $P \notin F \cap G$. μ_P is independent of the F, G components containing P.

3) μ_P is independent of change of coordinates

4) $\mu_P(F,G) = \mu_P(G,F)$

5) $\mu_P(F,G) \geq m_P(F) m_P(G)$ and $\mu_P(F,G) = m_P(F) m_P(G)$ iff F, G have no common tangents at P.

6) If $F=\prod F_i^{r_i}$ and $G=\prod G_j^{s_j}$ then

$$\mu_p(F,G)=\sum_{i,j} r_i s_j \mu_p(F_i,G_j)$$

7) $\forall A\in \bar{K}[x,y]$ have $\mu_p(F,G)=\mu_p(F,G+AF)$

NINE-POINT THEOREM

→ If F, G have no common component, all points of $F(\bar{K})\cap G(\bar{K})$ are simple over F, and H is a curve s.t. $HF \geq GF$, then $\exists A$ homogeneous polynomial s.t. $AF = HF-GF$.

→ $\boxed{\text{Nine-point Theorem}}$: If C, C', C'' are cubics, C is absolutely irreducible, $CC'=\sum_{i=1}^{9}\vec{P_i}$, P_i are simple and NN distinct, $CC''=\sum_{i=1}^{8}\vec{P_i}+\vec{Q}$, then $Q=P_9$.

GROUP LAWS ON AN ELLIPTIC CURVE

Recall from Shiv's lecture the group law that if $A=f(u)$ and $B=f(v)$ then $A\oplus B=f(u+v)=f(f^{-1}(A)+f^{-1}(B))$.

→ If C is a smooth cubic defined over K, A and B are in $C(K)$, and R is the third point of intersection of the line AB with C, then $A\oplus B$ relative to the origin is the third point of intersection of the line OR with C.

→ $(C(K), \oplus)$ is an Abelian group

Proof: By the previous, $C(K)$ is closed under $\oplus$, and by defn of the origin $A \oplus \mathcal{O} = A$, $A = B^{-1}$ iff AB intesects the origin tangent on C. The difficult part is associativity. WTS $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$. Define S to be the inverse of LHS and T of RHS. This requires the 9-point theorem, which he omits, it's just adding 6 points, making 6 collinearities, and a lot of arithmetic.

→ If $\mathcal{O}, \mathcal{O}'$ correspond to $(C(K), \oplus), (C(K), \oplus')$, then the two groups are isomorphic.

Proof: Want to define a birational isomorphism over K. Let $P, Q \in C(K)$ and define $*$ as the operation taking PQ line to its third intersection point with C, R, s.t. $P * Q = R$. Consider $\varphi : \oplus \dashrightarrow \oplus'$ such that $\varphi(P) = \mathcal{O} * (\mathcal{O}' * P)$. This is birational, considering $\psi(Q) = \mathcal{O}' * (\mathcal{O} * Q)$, and it maps origin to origin'. It remains to show $\varphi(P \oplus Q) = \varphi(P) \oplus' \varphi(Q)$. Expanding this gives

$O * (O' * (O * (P * Q))) = O' * ((O(O'P)) * (O(O'Q)))$.

This follows from the lemma that for any 4 points of $C(K)$, $L * (\Omega * (M * N)) = M * (\Omega * (L * N))$.

To prove this lemma, exercise. The answer is bottom of page 187: multiply LHS by Ω and use original associativity from above.

Define a $\boxed{\text{Weierstrass cubic}}$ as a smooth curve with $O = (0,1,0)$ of the form $W: y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6) = 0$.

REDUCTION MOD P

Define the reduction map $\boxed{\pi}: \mathbb{P}_2(\mathbb{Q}) \to \mathbb{P}_2(\mathbb{F}_p)$ such that $\pi((a,b,c)) = (\bar{a}, \bar{b}, \bar{c})$, the $\bar{\ }$ denoting reduction.

→ If C is a plane cubic defined over $\mathbb{Q}$, D a line of $\mathbb{P}_2(\mathbb{Q})$, $C(\mathbb{Q}) \cap D(\mathbb{Q}) = \{P_1, P_2, P_3\}$ for P_i repeated μ_p times, and $\bar{D}$ is not a component of $\bar{C}$, then $\bar{C}(\mathbb{F}_p) \cap \bar{D}(\mathbb{F}_p) = \{\bar{P}_1, \bar{P}_2, \bar{P}_3\}$ with same $\bar{P}_i$ multiplicity as P_i.

→ If cubic C is smooth in $\mathbb{P}_2(\mathbb{Q})$, $O \in C(\mathbb{Q})$, and $\bar{C}$ is smooth, then π is a homomorphism from $(C(\mathbb{Q}), \oplus)$ to $(\bar{C}(\mathbb{Q}), \bar{\oplus})$, $\bar{\oplus}$ denoting $\oplus$ wrt $\bar{O}$ instead of O.

→ If C the same except $\tilde{C}$ has a double point S in $\mathbb{P}_2(\overline{\mathbb{F}_p})$ and $O \in (C(\mathbb{Q}) \setminus \pi^{-1}(S))$, then $\{O\}$ is a subgroup of $C(\mathbb{Q})$ and π induces a homomorphism of this subgroup on the set of simple points of $\tilde{C}(\mathbb{F}_p)$ with addition law $\bar{\oplus}$.

Define W having a $\boxed{\text{good reduction}}$ at p when $\bar{W}$ smooth.

Define W having a $\boxed{\text{multiplicative reduction}}$ at p when $\bar{W}$ has a double point with distinct tangents in $\mathbb{P}_2(\overline{\mathbb{F}_p})$.

Define W having an additive reduction at p when $\bar{W}$ has a cusp in $\mathbb{P}_2(\overline{\mathbb{F}_p})$.