9/24/04

Alya.

Def. A group elt P has order m iff m is the smallest pos. int. s.t. $\underbrace{P+P+\cdots+P}_{m} = \mathcal{O}$.

$m = 2, 3$

order 2.

Non-singular C

$C: y^2 = x^3 + ax^2 + bx + c = f(x) \qquad \mathcal{O}: [0,1,0]$.

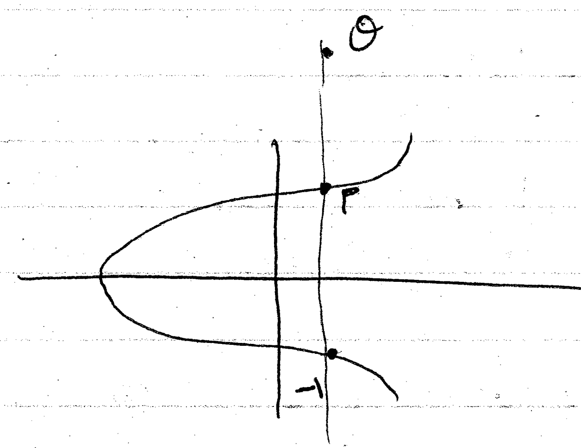
non-singular: $f(x)$ has no repeated roots.

$2P = \mathcal{O}, \quad P \neq \mathcal{O}$.

$P = -P$

Let $P = (x, y)$

$-P = (x, -y)$



$x = x$ ✓

$y = -y \Rightarrow 0$

$y^2 = 0$

$f(x) = 0$.

roots of $f(x)$: $\alpha_1, \alpha_2, \alpha_3$

Points of order 2: $P_1 = (\alpha_1, 0) \quad P_2 = (\alpha_2, 0), \quad P_3 = (\alpha_3, 0)$

$S = \{\mathcal{O}, P_1, P_2, P_3\}$ = set of points on C whose order $| 2$.

identity: $\mathcal{O}$ ✓

inverses: $P_i = -P_i$

closure: $2(P_1 + P_2) = 2P_1 + 2P_2 = \mathcal{O} + \mathcal{O} = \mathcal{O}$. ✓

S is a subgroup

$S = C_2 \times C_2$ els of S have order 1 or 2.
(in $\mathbb{C}$)

roots in $\mathbb{R}$

3 roots $\Rightarrow S = C_2 \times C_2$

1 root $\Rightarrow S = C_2$ ($\mathcal{O}$, P of ord 2).

roots in $\mathbb{Q}$

3 rat'l roots $\Rightarrow S = C_2 \times C_2$

1 rat'l root $\Rightarrow S = C_2$

0 rat'l roots $\Rightarrow S =$ trivial group. $\{\mathcal{O}\}$.

<u>pts of order 3</u>

$3P = \mathcal{O}$ $(2P \neq \mathcal{O})$

$2P = -P$

$x(P) =$ x-coord. of P.

$-P = (x, -y)$

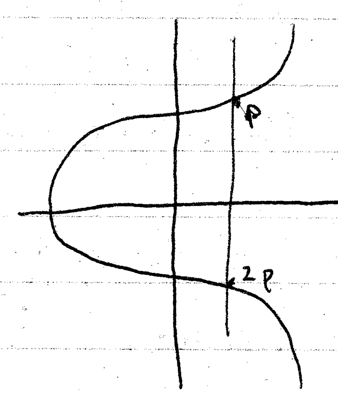
$2P = -P$

$x(2P) = x(-P) = x(P)$

Assume $P \neq \mathcal{O}$, $x(2P) = x(P)$

$2P = -P$.

$$x(2P) = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c} = x$$



x ~~so~~ solve this when x is a root of

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

To show: $\exists$ 9 pts of order dividing 3.

~~$\psi_3(x)$~~

$$x(2P) = \frac{f'(x)^2}{4f(x)} - a - 2x = x \quad \left\lfloor f(x) = x^3 + ax^2 + bx + c \right.$$

$$f'(x)^2 - 4a\,f(x) - 8x\,f(x) = 4x\,f(x).$$

$$f''(x) = 6x + 2a.$$

$$\psi_3(x) = 2f(x)f''(x) - f'(x)^2$$

orders of terms: $3+1=4$, $2\cdot 2 = 4$.

ψ_3 of x has order 4

ψ_3 has all 4 roots distinct. iff $\psi_3(x)$, $\psi_3'(x)$ have no common roots.

$$\psi_3'(x) = 2f'(x)f''(x) + 2f(x)f'''(x) - 2f'(x)f''(x)$$
$$= 2f(x)f'''(x)$$

$f'''(x) = 6$

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

Same roots as $f(x)$

$\psi_3(x)$, $\psi_3'(x)$ share roots ~~only~~ iff $f(x)$, $f'(x)$ do as well assumption $\Rightarrow$ f, f' share no roots.

$\Psi_3(x)$ has 4 distinct roots. ✓

Let thee roots be $\beta_1, \beta_2, \beta_3, \beta_4$

Let $\delta_1 = \sqrt{f(\beta_1)}$, ..., $\delta_i = \sqrt{f(\beta_i)}$

points $(\beta_i, \pm\delta_i) \in C$

$\delta_i = 0 \Rightarrow$ point has order 2. $\Rightarrow\!\Leftarrow$

$\delta_i \neq 0$.

look set $T = \{$ 8 points of order 3, $\mathcal{O} \}$.

orders $| 3$, $\Rightarrow C_3 \times C_3$. (over $\mathbb{C}$)

<u>Summary</u>.

Let C be a nonsingular cubic. $\mathcal{O}$ = pt at ∞.

Weierstrass form: $y^2 = x^3 + ax^2 + bx + c$

a) $P = (x, y)$ $(P \neq \mathcal{O})$ has order 2 iff $y = 0$.

b) C has exactly 4 pts of order dividing 2, forming $C_2 \times C_2$.

c) $P = (x, y)$ on C, $P \neq \mathcal{O}$, then P has order 3 iff x is a root of $\Psi_3(x) =$ ~~stuff~~

d) C contains exactly 9 pts of order dividing 3. and these form $C_3 \times C_3$.