

Def. An abelian group is a set G with an operation

$$+: G \times G \rightarrow G \quad (g_1, g_2) \mapsto g_1 + g_2$$

such that

- 1) Associativity: $g_1 + (g_2 + g_3) = (g_1 + g_2) + g_3$
- 2) Commutativity: $g_1 + g_2 = g_2 + g_1$
- 3) Identity: $\exists 0 \in G$ s.t. $0 + g = g, \forall g \in G$.
- 4) Inverse: $\forall g \in G, \exists g' \in G$ s.t. $g + g' = 0$ ($g' = -g$)

Ex: $(\mathbb{Z}, +)$

Ex: (congruence classes mod $n, +$) $(\mathbb{Z}/(n), +)$

Ex: If G, H abelian groups, then $G \oplus H = \{(g, h) \mid g \in G, h \in H\}$
abelian grp:

$$(g, h) + (g', h') = (g + g', h + h')$$

Map (Homomorphism) between abelian groups:

$$(G, +_G) \xrightarrow{f} (H, +_H)$$

A map f is a set map $f: G \rightarrow H$ s.t. $f(g_1 + g_2) = f(g_1) + f(g_2)$

Ex: $E: y^2 = x^3 - 4x$

$$E(\mathbb{Q}) = \{(2, 0), (0, 0), (-2, 0), 0\}$$

	0	A	B	C
A	0	A	B	C
B	A	0	C	B
C	B <td>C</td> <td>0</td> <td>A</td>	C	0	A
0	C	B	A	0

Define a map $f: E(\mathbb{Q}) \rightarrow \mathbb{Z}/(2) \times \mathbb{Z}/(2)$

by $A \mapsto (1, 0)$ $B \mapsto (0, 1)$ $C \mapsto (1, 1)$, $0 \mapsto (0, 0)$ bijection.

Preserves $+$: $A+B=C$

$$f(A+B) = f(C) = (1, 1) = (1, 0) + (0, 1) = f(A) + f(B)$$

Isomorphism.

Goal: Say something about classification of $E(\mathbb{Q})$ as an abelian group.

Ex: $E: y^2 = x^3 - x + \frac{1}{4}$ ($y^2 - y = x^3 - x$, w/ completing square)

$$P = (0, \frac{1}{2})$$

Compute multiples of P :

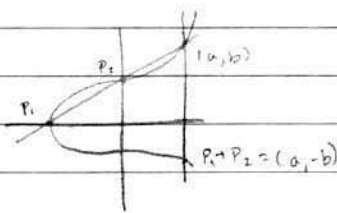
$$nP = \overbrace{P + \dots + P}^{n \text{ times}}$$

$$2P = (1, \frac{1}{2})$$

$$F = y^2 - x^3 + xz^2 - \frac{1}{4}z^2 = 0$$

$$\frac{\partial F}{\partial x}(P)x + \frac{\partial F}{\partial y}(P)y + \frac{\partial F}{\partial z}(P)z = 0 \Rightarrow 1 \cdot x + 1 \cdot y + (\frac{1}{2} - \frac{3}{4})z = 0 \Rightarrow x + y - \frac{1}{4}z = 0$$

$$\text{in } x+y \text{ plane: } x+y - \frac{1}{2}z = 0$$



$x^2 - x + \frac{1}{4} = x^3 - x + \frac{1}{4}$ (note we knew $x=0$ const. term drop out since $(0, \frac{1}{2})$ double root)

$$x^2 = x^3 \Rightarrow x = 0, 0, 1$$

$$x = 1 \Rightarrow y = -\frac{1}{2}, \text{ so } 2P = (1, \frac{1}{2})$$

$P = (a, b), a \neq 0$

$$y = \frac{b-\frac{1}{2}}{2} x + \frac{1}{2}$$

$$(mx + \frac{1}{2})^2 = x^3 - x + \frac{1}{4} \quad m^2 x^2 + mx + \frac{1}{4} = x^3 - x + \frac{1}{4}$$

$$m^2 x + m = x^2 - 1 \quad (\text{looking for sol'n with } x \neq 0)$$

This should be $(x-a)(x-x)$, x root we want:

$$x^2 - (a+x)x + ax = x^2 - m^2 x - (m+1)$$

$$\text{so } a+x = -m^2, \text{ so } P_3 = (m^2 - a, m^3 - am + \frac{1}{2})$$

$$P + (a, b) = (m^2 - a, -(m^3 - am + \frac{1}{2}))$$

n	1	2	3	4	5	6	7	8
nP	$(0, \frac{1}{2})$	$(1, \frac{1}{2})$	$(-1, -\frac{1}{2})$	$(2, -\frac{5}{2})$	$(\frac{1}{4}, -\frac{5}{4} + \frac{1}{2})$	$(6, 14 + \frac{1}{2})$	$(-\frac{5}{9}, \frac{7}{27} + \frac{1}{2})$	$(\frac{21}{5}, \frac{7}{125} - \frac{1}{2})$

Define $f: \mathbb{Z} \rightarrow E(\mathbb{Q})$ by $n \mapsto nP$.

$$f(n+m) = (n+m)P = \underbrace{P + \dots + P}_{n+m \text{ times}} \quad f(n) + f(m) = nP + mP = \underbrace{P + \dots + P}_{n \text{ times}} + \underbrace{P + \dots + P}_{m \text{ times}}$$

In fact, this is an isomorphism.

$$E(\mathbb{Q}) \supset E(\mathbb{Q})_{\text{torsion}} = \{P \in E(\mathbb{Q}) \mid \exists n > 0 \text{ s.t. } nP = 0\}$$

Lemma: $P, Q \in E(\mathbb{Q})_{\text{torsion}}$ then $P+Q, -P, -Q \in E(\mathbb{Q})_{\text{torsion}}$.

Proof: Say $n, m > 0$ s.t. $nP = 0$ and $mQ = 0$.

$$nm(P+Q) = m(nP) + n(mQ) = 0 + 0 = 0$$

$$P + -P = 0, \quad n(P + -P) = n \cdot 0 = 0 \Rightarrow nP + n(-P) = 0 \Rightarrow 0 + n(-P) = 0 \Rightarrow n(-P) = 0$$

Mazur's Thm: As an abel. group, $E(\mathbb{Q})_{\text{torsion}}$ is isomorphic to one of the following

$$\mathbb{Z}/(n), \quad n=1, 2, \dots, 10, 12 \quad \text{or} \quad \mathbb{Z}/(2) \times \mathbb{Z}/(n), \quad n=2, 4, 6, 8$$