10/22/04.

$$\alpha : \Gamma \longrightarrow \frac{\mathbb{Q}^*}{\mathbb{Q}^{*2}}$$

$$\alpha(\mathcal{O}) = 1 \pmod{\mathbb{Q}^{*2}}$$
$$\alpha(T) \equiv b \pmod{\mathbb{Q}^{*2}}$$
$$\alpha(x,y) \equiv x \pmod{\mathbb{Q}^{*2}}$$

Proposition

(a) The map α is a homomorphism

(b) The kernel of α is the image of $\psi(\bar{\Gamma})$. Hence α induces a 1-1 homomorphism $\frac{\Gamma}{\psi(\bar{\Gamma})} \longrightarrow \frac{\mathbb{Q}^*}{\mathbb{Q}^{*2}}$

(c) Let $p_1, \ldots, p_t$ be the distinct prime factors of b. Then the image of α is contained in the subgroup of $\mathbb{Q}^*/\mathbb{Q}^{*2}$ consisting of the elements

$$S = \{ \pm p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_t^{\varepsilon_t} : \text{each } \varepsilon_i = 0, 1 \}.$$

(d) The ~~image~~ index $(\Gamma : \psi(\bar{\Gamma}))$ is at most 2^{t+1}.

Proof of (c). $x = \frac{m}{e^2}, \; y = \frac{n}{e^3}$ $\quad (m, e) = (n, e) = 1$

m, n, e integers.

$$\left(\frac{n}{e^3}\right)^2 = y^2 = x^3 + ax^2 + bx = \left(\frac{m}{e^2}\right)^3 + a\left(\frac{m}{e^2}\right)^2 + b\left(\frac{m}{e^2}\right)$$
$$n^2 = m(m^2 + ame^2 + be^4).$$

Set $d = \gcd(m, m^2 + ame^2 + be^4)$.
$$= \gcd(m, be^4) = \gcd(m, b).$$

$d \mid b$.

$$m = \pm m_0^2 p_1^{\varepsilon_1} \cdots p_t^{\varepsilon_t}$$
$$x = \frac{m}{e^2} = \pm \left(\frac{m_0}{e}\right)^2 p_1^{\varepsilon_1} \cdots p_t^{\varepsilon_t} \equiv \pm p_1^{\varepsilon_1} \cdots p_t^{\varepsilon_t} \bmod \mathbb{Q}^{*2}$$

$x = 0 \Rightarrow m = 0 \qquad \alpha(P) = \alpha(T) \equiv b \mod \mathbb{Q}^{*2}$ ✓

Proof of (d) : $|S| = 2^{t+1}$, $(\Gamma : \psi(\bar{\Gamma})) \leq 2^{t+1}$.

$\phi : \Gamma \longrightarrow \bar{\Gamma}$, $\psi : \bar{\Gamma} \longrightarrow \Gamma$

$\phi \circ \psi$ and $\psi \circ \phi$ result in multiplying by 2.

and $(\Gamma : \psi(\bar{\Gamma}))$ and $(\bar{\Gamma} : \phi(\Gamma))$ are both finite.

$(\Gamma : 2\Gamma)$ is finite.

Lemma. Let A, B be abelian groups and consider two homomorphisms $\phi : A \longrightarrow B$ and $\psi : B \longrightarrow A$.

Suppose the following 3 conditions are satisfied.

(1) $\psi \circ \phi(a) = 2a \quad \forall a \in A$

(2) $\phi \circ \psi(b) = 2b \quad \forall b \in B$.

(3) $\phi(A)$ has finite index in B, and $\psi(B)$ has finite index in A.

Then $(A : 2A)$ is finite and satisfies

$$(A : 2A) \leq (B : \phi(A)) \cdot (A : \psi(B)).$$

$\psi(B)$ has finite index in $A \Rightarrow$ a set of representatives $a_1, a_2, \dots, a_n$ for the cosets of $\psi(B)$ in A.

$\phi(A)$ has finite index in $B \Rightarrow$ a set of representatives $b_1, b_2, \dots, b_m$ for the cosets of $\phi(A)$ in B.

Claim : $\{a_i + \psi(b_j) : 1 \leq i \leq n, 1 \leq j \leq m\}$ include a complete set of representatives for the cosets of $2A$ in A.

Proof of claim: Let $a \in A$. So $\exists$ a_i s.t.

$a = a_i + \psi(b)$ for some $b \in B$.

$b = b_j + \phi(a')$ for some $a' \in A$.

$$a = a_i + \psi(b_j) + \psi\phi(a')$$
$$= a_i + \psi(b_j) + 2a'$$

[Then restated Mordell's Theorem].

Γ abelian and finitely generated.

$$\Gamma = \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r} \oplus \mathbb{Z}_{p_1^{\nu_1}} \oplus \mathbb{Z}_{p_2^{\nu_2}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{\nu_s}}$$

$$r = \text{rank}(\Gamma)$$

$$P_1, P_2, \ldots, P_r, Q_1, \ldots, Q_s.$$

$$P = n_1 P_1 + n_2 P_2 \cdots + n_r P_r + m_1 Q_1 + \cdots + m_s Q_s.$$

if Γ is finite, $\Rightarrow \prod_{i=1}^{s} p_i^{\nu_i}$

$$2\Gamma = \underbrace{2\mathbb{Z} \oplus 2\mathbb{Z} \oplus \cdots \oplus 2\mathbb{Z}}_{r} \oplus 2\mathbb{Z}_{p_1^{\nu_1}} \oplus \cdots \oplus 2\mathbb{Z}_{p_s^{\nu_s}}$$

$$\frac{\Gamma}{2\Gamma} = \mathbb{Z}/2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/2\mathbb{Z} \oplus \frac{\mathbb{Z}_{p_1^{\nu_1}}}{2\mathbb{Z}_{p_1^{\nu_1}}} \oplus \cdots \oplus \frac{\mathbb{Z}_{p_s^{\nu_s}}}{2\mathbb{Z}_{p_s^{\nu_s}}}$$

$$\mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2$$

$$\frac{\mathbb{Z}_{p_i^{\nu_i}}}{2\mathbb{Z}_{p_i^{\nu_i}}} = \begin{cases} \mathbb{Z}_2 & p_i = 2 \\ 0 & \end{cases}$$

$$\#\left(\frac{\Gamma}{2\Gamma}\right) = 2^{r + \{i \mid 1 \le i \le s,\ p_i = 2\}}.$$

$\Gamma[2] \subset \Gamma$ consisting of the elements $Q \in \Gamma$ such that $2Q = 0$.

$$Q = n_1 P_1 + \cdots + n_r P_r + m_1 Q_1 + \cdots + m_s Q_s.$$

$2n_i P_i = 0$ for $1 \le i \le r$.

$\Rightarrow n_i = 0.$ for $1 \le i \le r$.

$2m_j Q_j \equiv 0 \mod p_j^{\nu_j}$

if p_j is odd $\Rightarrow m_j \equiv 0 \mod p_j^{\nu_j}$

if p_j is even $(=2)$ $\Rightarrow m_j \equiv 0 \ (p_j^{\nu_j})$

$\equiv p_j^{\nu_j - 1} \ (p_j^{\nu_j})$

$$\Gamma[2] \cong \mathbb{Z}_2^{\#\{i:\ 1 \le i \le s,\ p_i = 2\}}$$

$$(\Gamma : 2\Gamma) = 2^{r + \#\{i\ 1 \le i \le s\ p_s = 2\}}$$

<u>Proposition</u>: If Γ is a finitely generated abelian group, then $(\Gamma : 2\Gamma) = 2^{\mathrm{rank}(\Gamma)} \cdot \#\Gamma[2]$.