제 5 장 해 설

§5.1.1 벡터공간의 기저와 차원

§5.1.2 가 군

§5.5 Fermat 素數

§5.7 완전체

§5.9.1 타원곡선

§ 5.9.2 타원곡선을 이용한 암호체계

§5.1.1 벡터공간의 기저와 차원

여기서는, §5.1 에서 논한 정리에 대한 증명을 소개한다.
아래 정리의 번호는 [6] 에서의 번호를 그대로 옮긴 것이다.

정리 2.3.3 체 F 위의 벡터공간 V 에서 벡터 $v_1, v_2, \cdots, v_n, v \in V$ 에 대하여 다음이 성립한다.

(1) $v \neq \mathbf{0}$ 일 때 그리고 이때에만 v 는 일차독립이다.

(2) $v_1, v_2, \cdots, v_n$ 중에서 한 벡터가 영벡터이거나 또는 두 벡터가 서로 같으면, $v_1, v_2, \cdots, v_n$ 은 일차종속이다.

(3) $v \in \langle v_1, \cdots, v_n \rangle$ 이면, $v_1, \cdots, v_n, v$ 는 일차종속이다.

증 명 (1) 먼저 $v \neq \mathbf{0}$ 일 때, 적당한 $a \in F$ 에 대하여 $av = \mathbf{0}$ 이라고 가정하면 $a = 0$ 이므로 v 는 일차독립이다.

한편, $v = \mathbf{0}$ 이면, $1v = v = \mathbf{0}$, $1 \neq 0$ 이므로 v 는 일차종속이다.

(2) 예를 들어, $v_1 = \mathbf{0}$ 이면

$$1v_1 + 0v_2 + \cdots + 0v_n = \mathbf{0}, \qquad 1 \neq 0$$

이므로 $v_1, v_2, \cdots, v_n$은 일차종속이다. 그리고, 예를 들어 $v_1 = v_2$ 이면,

$$1v_1 + (-1)v_2 + \cdots + 0v_n = \mathbf{0}, \quad 1 \neq 0$$

이므로 $v_1, v_2, \cdots, v_n$ 은 일차종속이다.

(3) $v \in \langle v_1, \cdots, v_n \rangle$ 이면, 적당한 $a_1, \cdots, a_n \in F$ 에 대하여

$$v = a_1v_1 + \cdots + a_nv_n \quad \text{즉} \quad a_1v_1 + \cdots + a_nv_n + (-1)v = \mathbf{0}$$

이므로 $v_1, \cdots, v_n, v$ 는 일차종속이다.

정리 2.3.4 체 F 위의 벡터공간 V 에서 벡터 $v_1, v_2, \cdots, v_n, v \in V$ 에 대하여 다음이 성립한다.

(1) 벡터 $v_1, \cdots, v_n, v$ 가 일차독립이면, 벡터 $v_1, \cdots, v_n$ 은 일차독립이다.

(2) 벡터 $v_1, \cdots, v_n$ 이 일차독립이면, 모든 정수 $k\ (1 \leq k \leq n)$ 에 대하여 $v_1, \cdots, v_k$ 는 일차독립이다.

증 명 (1) 벡터 $v_1, \cdots, v_n, v$가 일차독립이라고 하자. 이 때,

$$a_1v_1 + \cdots + a_nv_n = \mathbf{0} \qquad (a_1, \cdots, a_n \in F)$$

이라고 가정하면, $a_1v_1 + \cdots + a_nv_n + 0v = \mathbf{0}$ 이고 또 $v_1, \cdots, v_n, v$는 일차독립이므로 $a_1 = \cdots = a_n = 0$ 이다. 따라서 $v_1, \cdots, v_n$은 일차독립이다.

(2) 위의 (1) 에 의하여 (2) 가 성립한다.

위의 정리에 의하여 다음 정리가 성립한다.

정리 2.3.5 체 F 위의 벡터공간 V 에서 벡터 $v_1, v_2, \cdots, v_n, v \in V$ 에 대하여 다음이 성립한다.

(1) 벡터 $v_1, \cdots, v_n$이 일차종속이면, 벡터 $v_1, \cdots, v_n, v$는 일차종속이다.

(2) 적당한 정수 k $(1 \leq k \leq n)$에 대하여 벡터 $v_1, \cdots, v_k$ 가 일차종속이면, $v_1, \cdots, v_n$은 일차종속이다.

정리 2.3.6 체 F 위의 벡터공간 V에서 벡터 $v_1, \cdots, v_n$이 일차종속이기 위한 필요충분조건은 $v_1 = \mathbf{0}$ 이거나 또는 적당한 j $(2 \leq j \leq n)$에 대하여 $v_j \in \langle v_1, \cdots, v_{j-1} \rangle$ 인 것이다.

증 명 먼저 벡터 $v_1, \cdots, v_n$이 일차종속이라고 하자. 이 때, 적어도 하나는 0이 아닌 $a_1, \cdots, a_n \in F$ 에 대하여 $a_1v_1 + \cdots + a_nv_n = \mathbf{0}$ 이다.

여기서 $j = \max\{k \mid a_k \neq 0,\ 1 \leq k \leq n\}$ 이라고 하면 다음이 성립한다.

$$a_1v_1 + \cdots + a_jv_j = 0, \quad a_j \neq 0,\ 1 \leq j \leq n$$

그런데 $j = 1$ 이면, $a_1v_1 = \mathbf{0}$, $a_1 \neq 0$ 이므로 $v_1 = \mathbf{0}$ 이다(정리 2.1.2), 또 $2 \leq j \leq n$ 이면, $v_j = a_j^{-1}a_1v_1 + \cdots + a_j^{-1}a_{j-1}v_{j-1} \in \langle v_1, \cdots, v_{j-1} \rangle$ 이다.

역으로, $v_1 = \mathbf{0}$ 이면, $v_1, \cdots, v_n$ 은 일차종속이다(정리 2.3.3). 또, 적당한 j $(2 \leq j \leq n)$에 대하여 $v_j \in \langle v_1, \cdots, v_{j-1} \rangle$ 이면, $v_1, \cdots, v_{j-1}, v_j$는 일차종속이므로 $v_1, \cdots, v_j, \cdots, v_n$은 일차종속이다.

앞의 정리에 의하여 다음 정리가 성립한다.

정리 2.3.7 체 F 위의 벡터공간 V에서 벡터 $v_1, \cdots, v_n$ 이 일차독립이기 위한 필요충분조건은 다음이 성립하는 것이다.

$$v_1 \neq \mathbf{0}, \quad v_j \notin \langle v_1, \cdots, v_{j-1} \rangle \quad (2 \leq j \leq n)$$

정리 2.3.7 과 정리 2.3.5 (3) 에 의하여 다음 정리가 성립한다.

정리 2.3.8 체 F 위의 벡터공간 V 에서 벡터 $v_1, \cdots, v_n \in V$이 일차독립일 때, 벡터 $v \in V$에 대하여 다음이 성립한다.

(1) $v \notin \langle v_1, \cdots, v_n \rangle$ 일 때 그리고 이때에만 $v_1, \cdots, v_n, v$ 는 일차독립이다.

(2) $v \in \langle v_1, \cdots, v_n \rangle$ 일 때 그리고 이때에만 $v_1, \cdots, v_n, v$ 는 일차종속이다.

정리 2.4.3 체 F 위의 벡터공간 V 에서 벡터 $v_1, \cdots, v_n, v$ 에 대하여 다음이 성립한다.

(1) $\langle v_1, \cdots, v_n \rangle \subseteq \langle v_1, \cdots, v_n, v \rangle$

(2) $\langle v_1, \cdots, v_n, v \rangle = \langle v_1, \cdots, v_n \rangle \Leftrightarrow v \in \langle v_1, \cdots, v_n \rangle$

증 명 (1) 부분공간 $\langle v_1, \cdots, v_n, v \rangle$는 벡터 $v_1, \cdots, v_n$을 포함하고, 따라서 $\langle v_1, \cdots, v_n \rangle \subseteq \langle v_1, \cdots, v_n, v \rangle$이다(정리 2.2.5).

(2) 먼저 $\langle v_1, \cdots, v_n, v \rangle = \langle v_1, \cdots, v_n \rangle$ 이면, $v \in \langle v_1, \cdots, v_n \rangle$ 이다. 이제 $v \in \langle v_1, \cdots, v_n \rangle$ 이라고 하자. 이 때,

$$v = a_1 v_1 + \cdots + a_n v_n \qquad (a_1, \cdots, a_n \in F)$$

이라고 하면, 임의의 $b_1, \cdots, b_n, b \in F$에 대하여

$$\begin{aligned} & b_1 v_1 + \cdots + b_n v_n + bv \\ &= b_1 v_1 + \cdots + b_n v_n + ba_1 v_1 + \cdots + ba_n v_n \\ &= (b_1 + ba_1) v_1 + \cdots + (b_n + ba_n) v_n \in \langle v_1, \cdots, v_n \rangle \end{aligned}$$

이고 따라서 $\langle v_1, \cdots, v_n, v \rangle \subseteq \langle v_1, \cdots, v_n \rangle$ 이다.

그러므로 (1) 에 의하여 $\langle v_1, \cdots, v_n, v \rangle = \langle v_1, \cdots, v_n \rangle$ 이다.

정리 2.4.4 체 F 위의 벡터공간 $V\ (\neq\{\mathbf{0}\})$에서 벡터 $v_1, \cdots, v_n$에 대하여 $V=\langle v_1, \cdots, v_n\rangle$ 일 때, 다음이 성립한다.

(1) 적당한 정수 $k\ (1\leq k\leq n)$에 대하여 벡터 $v_1, \cdots, v_k$가 일차독립이면,

$$\{v_1, \cdots, v_k\}\subseteq \mathscr{B}\subseteq\{v_1, \cdots, v_n\}$$

인 V의 기저 $\mathscr{B}$가 존재한다.

(2) $\mathscr{B}\subseteq\{v_1, \cdots, v_n\}$인 V의 기저 $\mathscr{B}$가 존재한다.

증 명 (1) 먼저 $V=\langle v_1, \cdots, v_k\rangle$이면, $\mathscr{B}=\{v_1, \cdots, v_k\}$는 V의 기저이다.

이제 $\langle v_1, \cdots, v_k\rangle\subsetneq V=\langle v_1, \cdots, v_n\rangle$이라고 하자. 이 때, $k<n$이다. 그리고, $v_{k+1}, \cdots, v_n\in\langle v_1, \cdots, v_k\rangle$이라고 가정하면, 정리 2.4.3에 의하여

$$V=\langle v_1, \cdots, v_k, v_{k+1}, \cdots, v_n\rangle=\langle v_1, \cdots, v_k\rangle$$

로 되어 모순이 생긴다. 따라서 $v_{k+1}, \cdots, v_n$ 중에는 $\langle v_1, \cdots, v_k\rangle$에 속하지 않는 벡터가 적어도 하나 존재한다.

한편, $v_1, \cdots, v_k$는 일차독립이므로, 각 정수 $i\ (k+1\leq i\leq n)$에 대하여 $v_i\notin\langle v_1, \cdots, v_k\rangle$일 때 그리고 이때에만 $v_1, \cdots, v_k, v_i$는 일차독립이다(정리 2.3.8). 따라서 $v_{k+1}, \cdots, v_n$ 중에서 다음 두 조건을 만족시키는 벡터 $u_1, \cdots, u_r$가 존재한다.

(i) $v_1, \cdots, v_k, u_1, \cdots, u_r$는 일차독립이다.

(ii) $v_{k+1}, \cdots, v_n\in\langle v_1, \cdots, v_k, u_1, \cdots, u_r\rangle$

이 때, 조건 (ii)와 정리 2.4.3에 의하여

$$V=\langle v_1, \cdots, v_k, v_{k+1}, \cdots, v_n\rangle=\langle v_1, \cdots, v_k, u_1, \cdots, u_r\rangle$$

이고, 또 조건 (i)에 의하여 $\mathscr{B}=\{v_1, \cdots, v_k, u_1, \cdots, u_r\}$는 V의 기저이다.

(2) 가정에 의하여 $\langle v_1, \cdots, v_n\rangle=V\neq\{\mathbf{0}\}$ 이므로 $v_1, \cdots, v_n$ 중에는 영벡터가 아닌 벡터가 존재한다. 이제 필요하다면 첨자의 번호를 재조정하여 $v_1\neq\mathbf{0}$이라고 하자. 이 때, v_1은 일차독립이고(정리 2.3.3), 따라서 위의 (1)에 의하여 $\{v_1\}\subseteq\mathscr{B}\subseteq\{v_1, \cdots, v_n\}$ 인 기저 $\mathscr{B}$가 존재한다.

정리 2.4.5 체 F 위의 벡터공간 $V(\neq\{\mathbf{0}\})$에서 $V=\langle v_1, \cdots, v_n\rangle$ 일 때, V 의 m개의 벡터 $w_1, \cdots, w_m$이 일차독립이면 $m \leq n$ 이고 따라서 V 의 $n+1$ 개 이상의 벡터는 일차종속이다.

증 명 V 의 m개의 벡터 $w_1, \cdots, w_m$이 일차독립이라고 하자.

이 때, $w_1 \in V=\langle v_1, \cdots, v_n\rangle$ 이므로, 정리 2.3.8에 의하여 $w_1, v_1, \cdots, v_n$ 은 일차종속이고 또 정리 2.4.3 에 의하여

$$V=\langle v_1, \cdots, v_n\rangle \subseteq \langle w_1, v_1, \cdots, v_n\rangle \subseteq V$$

이므로 $\langle w_1, v_1, \cdots, v_n\rangle = \langle v_1, \cdots, v_n\rangle = V$ 이다.

그리고, $w_1, \cdots, w_m$은 일차독립이므로 w_1은 일차독립이다(정리 2.3.4). 따라서 정리 2.4.4 에 의하여 다음과 같은 꼴의 V 의 기저 S_1 이 존재한다.

$$S_1=\{w_1, v_{i_1}, \cdots, v_{i_s}\} \subseteq \{w_1, v_1, \cdots, v_n\}$$

여기서 $s+1$ 개의 벡터 $w_1, v_{i_1}, \cdots, v_{i_s}$ 는 일차독립이고 $w_1, v_1, \cdots, v_n$ 은 일차종속이므로 $s < n$ 즉 $s \leq n-1$ 이다.

다음에 $m \geq 2$ 이라고 하자.

이 때, $w_2 \in V=\langle w_1, v_{i_1}, \cdots, v_{i_s}\rangle$ 이므로, 앞에서 논한 바와 마찬가지로 $w_2, w_1, v_{i_1}, \cdots, v_{i_s}$ 는 일차 종속이고 또 다음이 성립함을 알 수 있다.

$$\langle w_1, w_2, v_{i_1}, \cdots, v_{i_s}\rangle = \langle w_1, v_{i_1}, \cdots, v_{i_s}\rangle = V$$

한편, 벡터 $w_1, \cdots, w_m$은 일차독립이므로 두 벡터 w_1, w_2 는 일차독립이다(정리 2.3.4). 따라서 다음과 같은 꼴의 기저 S_2 가 존재한다(정리 2.4.4).

$$S_2=\{w_1, w_2, v_{j_1}, \cdots, v_{j_t}\} \subseteq \{w_1, w_2, v_{i_1}, \cdots, v_{i_s}\}$$

여기서 $t+2$ 개의 벡터 $w_1, w_2, v_{j_1}, \cdots, v_{j_t}$ 는 일차독립이지만 $s+2$ 개의 벡터 $w_1, w_2, v_{i_1}, \cdots, v_{i_s}$ 는 일차종속이므로 $t < s$ 즉 $t \leq s-1 \leq n-2$ 이다.

이와 같은 과정을 되풀이하면, 다음과 같은 꼴의 V 의 기저를 얻는다.

$$S_{m-1}=\{w_1, w_2, \cdots, w_{n-1}, v_{k_1}, \cdots, v_{k_r}\}, \quad r \leq n-(m-1)$$

한편, 가정에 의하여 $w_1, w_2, \cdots, w_m$ 은 일차독립이므로 정리 2.3.8에 의하여

$w_m \notin \langle w_1, w_2, \cdots, w_{m-1} \rangle$이고 따라서 $\langle w_1, w_2, \cdots, w_{m-1} \rangle \subsetneq V$ 이다. 그런데, 이 사실은 $S_{m-1} \neq \{w_1, w_2, \cdots, w_{m-1}\}$ 임을 뜻한다.

그러므로 $r \geq 1$ 이고, 따라서 $n-(m-1) \geq r \geq 1$ 즉 $m \leq n$ 이다.

정리 2.4.6 체 F 위의 벡터공간 $V\ (\neq \{\mathbf{0}\})$ 가 유한 개의 벡터에 의하여 생성될 때, V 는 유한 기저를 가진다. 더욱이, 이 경우에 V 의 기저에 속해 있는 벡터의 개수는 그 기저에 관계없이 일정하다. 즉,

$$\mathscr{B} = \{v_1, \cdots, v_n\}, \qquad \mathscr{C} = \{w_1, \cdots, w_m\}$$

가 V 의 기저이면 $n = m$ 이다.

증 명 먼저 정리 2.4.4 에 의하여 V 는 유한 기저를 가진다.

다음에 $\mathscr{B} = \{v_1, \cdots, v_n\}$, $\mathscr{C} = \{w_1, \cdots, w_m\}$ 가 V 의 기저라고 하자. 이 때, $V = \langle v_1, \cdots, v_n \rangle$ 이고 $w_1, \cdots, w_m$ 은 일차독립이므로 정리 2.4.5 에 의하여 $m \leq n$ 이다. 마찬가지로, $V = \langle w_1, \cdots, w_m \rangle$ 이고 $v_1, \cdots, v_n$ 은 일차독립이므로 $n \leq m$ 이고, 따라서 $n = m$ 이다.

정리 2.4.9 체 F 위의 벡터공간 $V\ (\neq \{\mathbf{0}\})$ 가 n 차원 벡터공간일 때 다음이 성립한다.

(1) V 의 m 개의 벡터 $w_1, \cdots, w_m$ 이 일차독립이면 $m \leq n$ 이다.

따라서 $n < m$ 이면, V 의 임의의 m 개의 벡터는 일차종속이다.

(2) V 의 n 개의 벡터 $w_1, \cdots, w_n$ 이 일차독립이면, $\mathscr{C} = \{w_1, \cdots, w_n\}$ 는 V 의 기저이다.

(3) $V = \langle w_1, \cdots, w_m \rangle$ 이면, $n \leq m$ 이다.

특히, $V = \langle w_1, \cdots, w_n \rangle$ 이면, $\mathscr{C} = \{w_1, \cdots, w_n\}$ 는 V 의 기저이다.

(4) V 의 m 개의 벡터 $w_1, \cdots, w_m$ 이 일차독립일 때, $m < n$ 이면 이들 m 개의 벡터에 적당한 $r\ (= n-m)$ 개의 적당한 벡터 $u_1, \cdots, u_r$ 를 첨가하여 V 의 기저 $\mathscr{C} = \{w_1, \cdots, w_m, u_1, \cdots, u_r\}$ 를 얻을 수 있다.

증 명 (1) 가정에 따라 벡터공간 V에는 n 개의 벡터로 이루어진 기저

$\mathscr{B}=\{v_1, \cdots, v_n\}$ 가 존재하고 이때 $V=\langle v_1, \cdots, v_n\rangle$ 이므로 정리 2.4.5에 의하여 (1) 이 성립한다.

(2) V 의 n 개의 벡터 $w_1, \cdots, w_n$ 이 일차독립이라고 하자.

이 때, v 를 V 의 임의의 벡터라고 하면, (1) 에 의하여 $n+1$ 개의 벡터 $v, w_1, \cdots, w_n$ 은 일차종속이고 또 $w_1, \cdots, w_n$ 은 일차독립이므로 정리 2.3.8에 의하여 $v \in \langle w_1, \cdots, w_n\rangle$ 이다.

따라서 $V=\langle w_1, \cdots, w_n\rangle$ 이므로 $\mathscr{C}=\{w_1, \cdots, w_n\}$ 는 V 의 기저이다.

(3) $V=\langle w_1, \cdots, w_m\rangle$ 이면, 정리 2.4.4 에 의하여 $\mathscr{C} \subseteq \{w_1, \cdots, w_m\}$ 인 V 의 기저 $\mathscr{C}$ 가 존재하고 또 $|\mathscr{C}| = n$ 이므로 $n \leq m$ 이다.

특히, $m = n$ 이면, $\mathscr{C} = \{w_1, \cdots, w_n\}$ 이다.

(4) V 의 m 개의 벡터 $w_1, \cdots, w_m$ 이 일차독립이고 $m < n$ 이라고 하자. 이 때, $\mathscr{B}=\{v_1, \cdots, v_n\}$ 를 V 의 기저라고 하면,

$$V=\langle v_1, \cdots, v_n\rangle \subseteq \langle w_1, \cdots, w_m, v_1, \cdots, v_n\rangle \subseteq V$$

이므로 $V=\langle w_1, \cdots, w_m, v_1, \cdots, v_n\rangle$ 이고 따라서 정리 2.4.4 에 의하여

$$\{w_1, \cdots, w_m\} \subseteq \mathscr{C} \subseteq \{w_1, \cdots, w_m, v_1, \cdots, v_n\}$$

인 V 의 기저 $\mathscr{C}$ 가 존재한다. 한편, 정리 2.4.6에 의하여 $|\mathscr{C}| = n > m$ 이므로, 적당한 r $(=n-m)$ 개의 벡터 $u_1, \cdots, u_r \in \{v_1, \cdots, v_n\}$ 에 대하여 $\mathscr{C}=\{w_1, \cdots, w_m, u_1, \cdots, u_r\}$ 이다.

정리 2.5.1 체 F 위의 벡터공간 V $(\neq \{\mathbf{0}\})$ 가 유한차원 벡터공간일 때, V 의 부분공간 W 는 유한차원 벡터공간이고 또 다음이 성립한다.

(1) $0 \leq \dim_F W \leq \dim_F V$

(2) $\dim_F W = 0 \iff W=\{\mathbf{0}\}$, $\dim_F W = \dim_F V \iff W = V$

증 명 분명히 $W=\{\mathbf{0}\} \iff \dim_F W = 0$ 이다.

다음에 $\{\mathbf{0}\} \subsetneq W \subseteq V$ 이라고 하자. 이 때, W 에는 벡터 $w_1 \neq \mathbf{0}$ 이 존재하고 벡터 w_1 은 일차독립이다(정리 2.3.3).

이 사실을 이용하면, 다음 두 조건을 만족시키는 벡터 $w_1, \cdots, w_m \in W$ 이 존재함을 알 수 있다(정리 2.4.9).

(i) $w_1, \cdots, w_m$ 은 일차독립이다.

(ii) 모든 벡터 $w \in W$ 에 대하여 $w_1, \cdots, w_m, w$ 는 일차종속이다.

이 때, 정리 2.3.8 에 의하여 모든 $w \in W$ 에 대하여 $w \in \langle w_1, \cdots, w_m \rangle$ 이므로 $W = \langle w_1, \cdots, w_m \rangle$ 이고, 따라서 $\mathscr{C} = \{w_1, \cdots, w_m\}$ 는 W 의 기저이므로 $\dim_F W = m$ 이다.

한편, 정리 2.4.9 에 의하여 $\dim_F W = m \leq \dim_F V$ 이다.

특히, $\dim_F W = \dim_F V = n$ 이면, W는 n 개의 벡터로 이루어진 기저 $\{w_1, \cdots, w_n\}$ 을 가지므로 $W = \langle w_1, \cdots, w_n \rangle = V$ 이다(정리 2.4.9).

따름정리 2.5.2 체 F 위의 유한차원 벡터공간 $V\,(\neq \{\mathbf{0}\})$ 에서 V의 두 부분공간 W_1, W_2 에 대하여 다음이 성립한다.

(1) $W_1 \subseteq W_2$ 이면, $\dim_F W_1 \leq \dim_F W_2$ 이다.

(2) $W_1 \subseteq W_2$ 일 때, $\dim_F W_1 = \dim_F W_2$ 이면 $W_1 = W_2$ 이다.

증 명 정리 2.5.1 에 의하여 V의 부분공간 W_1, W_2는 유한차원 벡터공간이다. 그리고, $W_1 \subseteq W_2$ 이면, W_1 은 벡터공간 W_2 의 부분공간이기도 하므로 정리 2.5.1 에 의하여 (1), (2) 가 성립한다.

§5.1.2 가 군

벡터공간의 개념은 다음과 같이 일반화할 수 있다.

정의 1 환 R가 단위원 1을 가진 환일 때, 집합 M이 다음 두 조건을 만족시킬 때, M를 R 위의 **좌 가군**(左 加群 left module) 또는 **좌 R-가군**이라고 한다.

(1) M 위에 덧셈이 정의되어 있고 $(M,+)$는 덧셈군이다.

(2) 사상

$$R\times M \longrightarrow M,\quad (r,a)\longmapsto r\cdot a$$

가 정의되어 있고 임의의 $r,s\in R$와 $a,b\in V$ 와 에 대하여 다음이 성립한다.

(i) $r\cdot(a+b)=r\cdot a+r\cdot b$

(ii) $(r+s)\cdot a=r\cdot a+s\cdot a$

(iii) $(rs)\cdot a=r\cdot(s\cdot a)$

(iv) $1\cdot a=a$

정의 2 환 R가 단위원 1을 가진 환일 때, 집합 M이 다음 두 조건을 만족시킬 때, M를 R 위의 **우 가군**(右 加群(right module) 또는 **우 R-가군**이라고 한다.

(1) M 위에 덧셈이 정의되어 있고 $(M,+)$는 덧셈군이다.

(2) 사상

$$M\times R \longrightarrow M,\quad (a,r)\longmapsto a\cdot r$$

가 정의되어 있고 임의의 $a,b\in M$ 과 $r,s\in R$에 대하여 다음이 성립한다.

(i) $(a+b)\cdot r=a\cdot r+b\cdot r$

(ii) $a\cdot(r+s)=a\cdot r+a\cdot s$

(iii) $a\cdot(rs)=(a\cdot r)\cdot s$

(iv) $a\cdot 1=a$

정의 3 환 D가 나눗셈환일 때, D 위의 左 가군을 D 위의 **左 벡터공간** 또는 **左 D-벡터공간**이라 하고 또 D 위의 右 가군을 D위의 **右벡터공간** 또는 **右 D-벡터공간**이라고 한다.

환 R가 단위원 1을 가진 가환환일 때, M이 左 R-가군이면 M을 右 R-가군으로 볼 수 있다. 실제로, 임의의 $r\in R$와 $a\in M$에 대하여 $a\cdot r$를 $r\cdot a$로 정하면, 정의 2의 네 조건이 성립한다.

마찬가지로, 환 R가 단위원 1을 가진 가환환일 때, M이 右 R-가군이면 M을 左 R-가군으로 볼 수 있다. 실제로, 임의의 $a\in M$와 $r\in R$에 대하여 $r\cdot a$를 $a\cdot r$로 정하면, 정의 1 의 네 조건이 성립한다. 이러한 의미에서 이 경우에 M을 R 위의 **가군** 또는 **R-가군**이라고 한다.

특히, 체 F 위의 左 벡터공간 [右 벡터공간] V는 체 F 위의 右벡터공간 [左 벡터공간] 으로 볼 수 있다. 이러한 의미에서 V를 체 F 위의 **벡터공간**이라고 한다.

덧셈군 A에서, 임의의 원소 $a, b\in A$와 임의의 정수 m, n에 대하여 다음이 성립한다(정리 2.1.13).

(i) $n\cdot(a+b) = n\cdot a + n\cdot b$ (iii) $(mn)\cdot a = m\cdot(n\cdot a)$

(ii) $(m+n)\cdot a = m\cdot a + n\cdot a$ (iv) $1\cdot a = a$

이러한 의미에서 모든 덧셈군은 $\mathbb{Z}$-가군이다.

§5.5 Fermat 素數

일반적으로, 두 실수 x, y 에 대하여 다음 등식이 성립한다.

(1) n 이 양의 정수일 때,

$$x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1})$$

(2) k 가 양의 홀수일 때,

$$x^k + y^k = (x+y)(x^{k-1} - x^{k-2}y + \cdots - xy^{k-2} + y^{k-1})$$

정리 1 양의 정수 m 에 대하여 정수 $2^m + 1$ 이 素數이면, 적당한 정수 $n\ (\geq 0)$ 에 대하여 $m = 2^n$ 이다.

증 명 양의 정수 m 은 다음과 같은 꼴로 나타낼 수 있다.

$$m = 2^n k \qquad (n \geq 0,\ k\text{는 홀수})$$

이 때, k 는 홀수이므로 다음이 성립한다.

$$2^m + 1 = (2^{2^n} + 1)\{2^{2^n(k-1)} - 2^{2^n(k-2)} + \cdots - 2^{2^n} + 1\},$$

$$2^{2^n} + 1 \geq 2^{2^0} + 1 = 3$$

따라서 $2^m + 1$ 이 素數이면, $2^m + 1 = 2^{2^n} + 1$ 이므로 $m = 2^n$ 이다.

정의 2 다음과 같은 꼴의 정수를 **페르마 수**(Fermat number)라고 한다.

$$F_n = 2^{2^n} + 1 \qquad (n \geq 0)$$

특히, F_n 이 素數일 때 F_n 을 **페르마 素數**(Fermat prime)라고 한다.

Fermat 素數는 2019 년 현재 다음의 5 개만이 알려져 있다.

$$F_0 = 2^1 + 1 = 3, \quad F_1 = 2^2 + 1 = 5, \quad F_2 = 2^4 + 1 = 17,$$

$$F_3 = 2^8 + 1 = 257, \quad F_4 = 2^{16} + 1 = 65537$$

한편, 아래에서 보는 바와 같이 F_5, F_6 는 素數가 아니다.

$$F_5 = 2^{32}+1 = 4294967297 = 641 \cdot 6700417, \qquad 641 = 2^7 \cdot 5 + 1,$$
$$F_6 = 2^{64}+1 = 274177 \cdot 67280421310721, \quad 2742177 = 2^8 \cdot 1071 + 1$$

정리 3 Fermat 수 $F_n = 2^{2^n}+1$ 에 대하여 다음이 성립한다.

(1) $F_0 F_1 \cdots F_{n-1} = F_n - 2$ $\qquad (n \geq 1)$

(2) $(F_m, F_n) = 1$ $\qquad (m, n \geq 1,\ m \neq n)$

증 명 (1) 먼저 $n = 1$ 일 때, $F_0 = 3 = 5-2 = F_1 - 2$ 이다.

다음에 $n = k \geq 1$ 일 때 (1) 이 성립한다고 가정하면,

$$\begin{aligned} F_0 F_1 \cdots F_{k-1} F_k &= (F_k - 2) F_k \\ &= (2^{2^k}-1)(2^{2^k}+1) \\ &= 2^{2^{k+1}} - 1 = F_{k+1} - 2 \end{aligned}$$

이므로 $n = k+1$ 일 때에도 (1) 이 성립한다.

그러므로, 수학적 귀납법에 의하여 모든 양의 정수 n 에 대하여 (1) 이 성립한다.

(2) 이제 $1 \leq m < n$ 일 때, $d = (F_m, F_n)$ 이라고 하자.

위의 (1) 에 의하여

$$F_0 F_1 \cdots F_m \cdots F_{n-1} = F_n - 2$$

이고 또 $d \mid F_m$, $d \mid F_n$ 이므로 $d \mid 2$ 이다. 그런데, F_m 과 F_n 은 모두 홀수이므로 $d = 1$ 이다.

보기 1 Fermat 수를 이용하여 素數가 무한히 많음을 밝힐 수 있다.

실제로, 각 정수 $n\ (\geq 0)$ 에 대하여 Ferma 수 $F_n = 2^{2^n}+1$ 에는 적어도 한 소인수 p_n 이 존재한다. 그런데, 서로 다른 양의 정수 m, n 에 대하여 $(F_m, F_n) = 1$ 이므로(정리 2.3.3), p_m 과 p_n 은 서로 다른 素數이다. 그러므로 $p_0, p_1, \cdots, p_n, \cdots$ 은 모두 서로 다른 素數이다.

§5.7 완전체

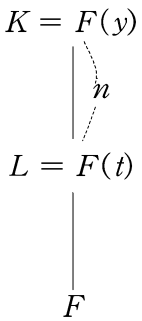
체 F 위의 기약다항식이 모두 F 위의 분리다항식일 때, F를 **완전체** (perfect field)라고 한다.

이제 표수 p인 무한체 중에 완전체가 아닌 체가 존재함을 증명하기로 한다.

정리 1 체 F 위의 부정원 y에 관한 유리식체

$$K = F(y) = \{ \frac{f(y)}{g(y)} \mid f(x), g(x) \in F[y],\ g(y) \neq 0 \}$$

에서 임의의 정수 $n\ (\geq 2)$에 대하여 $t = y^n \in K$이라 하고 $L = F(t)$ 이라고 할 때 다음이 성립한다.



(1) $K = L(y)$ 이고 원소 $y \in K$는 L 위에서 대수적이다.

(2) $\mathscr{B} = \{1, y, \cdots, y^{n-1}\}$는 K의 L-기저이고

$\mathrm{irr}\,(y, L) = x^n - t \in L[x]$, $\quad [K : F] = n$이다.

증명 (1) $K = F(y)$ 이고 $F \subseteq L \subseteq K$이므로

$$K = F(y) \subseteq L(y) \subseteq K$$

이고 따라서 $K = L(y)$ 이다. 또, $y \in K$는 L 위의 다항식 $f(x) = x^n - t$의 근이므로 t는 L 위에서 대수적이다.

(2) 이제 $p(x) = \mathrm{irr}\,(y, L)$ 이라고 하면, y는

$$f(x) = x^n - t \in L[x]$$

의 근이므로 $L[x]$ 에서 $p(x) \mid f(x)$ 이고 따라서 다음이 성립한다.

$$\deg p(x) \leq \deg f(x) = n$$

또, $K = L(y)$ 이므로 K는 L의 유한 확대체이고 다음이 성립한다.

$$[K : L] = \deg p(x) \leq n$$

한편, $t \in K$ 는 F 위에서 초월적이므로 다음이 성립한다..

$$L = F(t) = \{ \frac{f(t)}{g(t)} \mid f(t), g(t) \in F[t],\ g(t) \neq 0 \} \cong F(x)$$

이제 체 K의 원소 $1, y, \cdots, y^{n-1}$가 L-일차독립임을 증명하기 위하여 L의 원소

$$\frac{f_0(t)}{g_0(t)}, \frac{f_1(t)}{g_1(t)}, \frac{f_2(t)}{g_2(t)}, \cdots, \frac{f_{n-1}(t)}{g_{n-1}(t)}$$

에 대하여 다음이 성립한다고 하자.

$$\frac{f_0(t)}{g_0(t)} + \frac{f_1(t)}{g_1(t)} y + , \frac{f_2(t)}{g_2(t)} y^2 + \cdots + \frac{f_{p-1}(t)}{g_{n-1}(t)} y^{n-1} = 0$$

이 때,

$$g(t) = g_0(t)\, g_1(t)\, g_2(t) \cdots g_{p-1}(t)$$

이라 하고

$$g(t) = g_i(t)\, h_i(t), \quad k_i(t) = f_i(t)\, h_i(t) \quad (0 \le i \le n-1)$$

이라고 하면, $h_i(t)$는 영다항식이 아니고 다음 등식이 성립한다.

$$k_0(t) + k_1(t)\, y + k_2(t)\, y^2 + \cdots + k_{n-1}(t)\, y^{n-1} = 0$$

즉

$$k_0(y^n) + k_1(y^n)\, y + k_2(y^n) y^2 + \cdots + k_{n-1}(y^n) y^{n-1} = 0$$

그런데, 각 i $(0 \le i \le n-1)$에 대하여 $k_i(y^n)\, y^i$의 항은

$$b_s y^{ns+i} \qquad (b_s \in F)$$

와 같은 꼴이므로, $0 \le i \ne j \le n-1$일 때 $k_i(y^n)\, y^i$의 각 항과 $k_j(y^n)\, y^j$의 각항은 어느 둘도 그 차수가 같지 않다.

그러므로 각 i $(0 \le i \le n-1)$에 대하여 $k_i(t)$는 영다항식이고 또

$$k_i(t) = f_i(t)\, h_i(t),$$

이므로 $f_i(t)$는 영다항식이다. 따라서 $1, y, y^2, \cdots, y^{n-1}$은 L-일차독립이다.

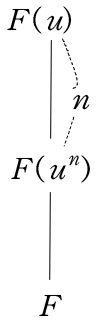
한편, (1)에 의하여 $[K : L] \le n$이므로 $\mathscr{B} = \{1, y, \cdots, y^{n-1}\}$는 K의 L-기저이고 따라서 $[K : F] = n$이다.

특히, $1, y, \cdots, y^{n-1}$는 모두 L에 속하지 않는다.

[참고] 체 F의 확대체 K의 원소 $u \in K$가 F 위에서 초월적이라고 하면, 부정원 x, y에 대하여

$$F[u] \cong F[x] \cong F[y], \quad F(u) \cong F(x) \cong F(y)$$

이고 또 임의의 정수 $n\ (\geq 2)$에 대하여 u^n은 F 위에서 초월적이지만, u는 $F(u^n)$ 위에서 대수적이고 $F(u)$는 $F(u^n)$의 유한 확대체이다.



그리고,

$$\mathscr{B} = \{1, u, \cdots, u^{n-1}\}$$

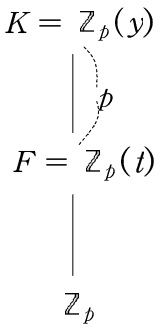
는 $F(u)$의 $F(u^n)$-기저이고 따라서 $[F(u) : F(u^n)] = n$이다.

특히, $1, u, \cdots, u^{n-1}$은 모두 $F(u^n)$에 속하지 않는다.

보기 素數 p에 대하여 체 $\mathbb{Z}_p$ 위의 부정원 y에 관한 유리식체 $K = \mathbb{Z}_p(y)$에서 $t = y^p$이라 하고 $L = \mathbb{Z}_p(t)$이라고 하면, 앞의 정리에 의하여

$$K = F(y)$$

이고, $p(x) = \mathrm{irr}(y, L)$이라고 하면 $p(x) = x^p - t$이고 $[K : L] = p$이다.



그런데, K의 표수는 p이므로 K위에서 $p(x)$는

$$p(x) = x^p - t = x^p - y^p = (x - t)^p$$

와 같이 인수분해된다.

따라서 $p(x)$는 체 L 위의 기약다항식이지만 분리다항식은 아니다.

§5.9.1 타원곡선

여기서는, [4] 의 §4.4 의 내용을 소개하기로 한다.

체 F 에 대하여 집합 $F^2 = \{(x, y) \mid x, y \in F\}$ 의 각 원소 (x, y)를 '**점**'이라 하고 체 F 에서의 일차방정식

$$ax + by + c = 0 \qquad (a \neq 0 \text{ 또는 } b \neq 0)$$

을 만족시키는 점 (x, y) 전체의 집합

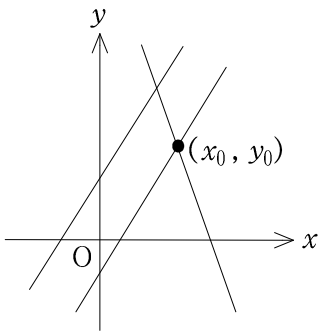
$$\{(x, y) \in F^2 \mid ax + by + c = 0\}$$

을 '**직선**'이라고 하자. 여기서, 방정식 $ax + by + c = 0$ 을 이 직선의 방정식이라 하고 이 직선을 간단히 '직선 $ax + by + c = 0$' 이라고 한다.

그리고 점 (x_0, y_0) 가 동시에 두 직선

$$ax + by + c = 0,$$
$$a'x + b'y + c' = 0$$

위에 있을 때 이 두 직선은 점 (x_0, y_0) 에서 만난다고 하고, 이 두 직선이 일치하거나 또는 만나지 않을 때 이 두 직선은 평행하다고 한다.



이와 같이 정의한 점 전체의 집합과 직선 전체의 집합으로 이루어진 평면을 체 F 위의 **아핀평면**(affine plane)이라 하고 이것을 $\mathrm{AG}(2, F)$ 로 나타낸다. 특히, 실수체 $\mathbb{R}$ 위의 아핀평면 $\mathrm{AG}(2, \mathbb{R})$ 를 **유클리드 평면**이라고 한다.

체 F 위의 아핀평면 $\mathrm{AG}(2, F)$ 에서 x, y 에 관한 방정식 $f(x, y) = 0$ 을 만족시키는 점 (x, y) 전체로 이루어진 집합

$$\{(x, y) \in F^2 \mid f(x, y) = 0\}$$

을 아핀평면 $\mathrm{AG}(2, F)$ 위의 **곡선**이라고 한다. 그리고, 방정식 $f(x, y) = 0$ 을 이 곡선의 방정식이라 하고 이 곡선을 간단히 '곡선 $f(x, y) = 0$' 이라고 한다. 특히, 아핀평면 $\mathrm{AG}(2, F)$ 에서 Weierstrass 의 방정식

$$E : \quad y^2 + dxy + ey = x^3 + ax^2 + bx + c$$

를 만족시키는 점 $(x, y) \in F^2$ 전체로 이루어진 집합

$$(*) \qquad \{(x, y) \in F^2 \mid y^2 + dxy + ey = x^3 + ax^2 + bx + c\}$$

를 체 F 위에서의 **타원곡선**(elliptic curve)이라고 한다.

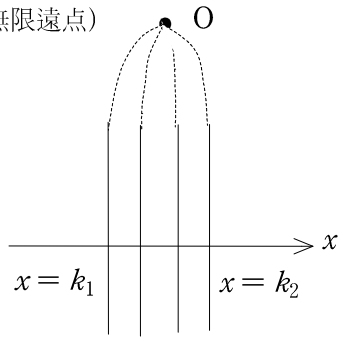
이제 아핀평면 $\mathrm{AG}(2, F)$ 에 **무한원점**(無限遠点) O 를 새로 도입하여 모든 직선

$$x = k \qquad (k \in F)$$

가 점 O 를 지난다고 생각하면, 임의의 서로 다른 $k_1, k_2 \in F$ 에 대하여 두 직선

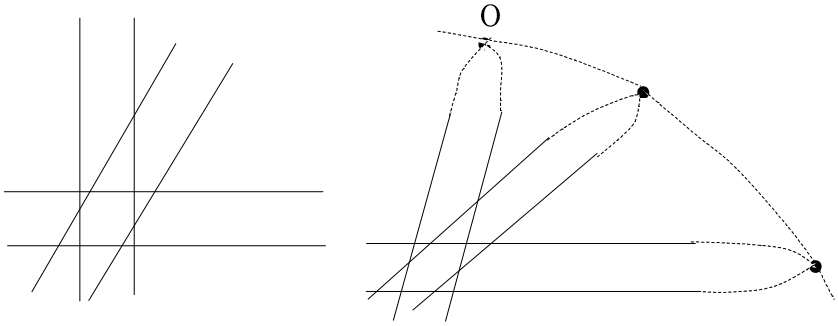
$$x = k_1, \quad x = k_2$$

은 단 한 점 O 에서 만난다. 집합 (*) 에 무한원점 O 를 추가한 집합을 $G(E, F)$ 로 나타내자. 즉,



$$G(E, F) = \{(x, y) \in F^2 \mid y^2 + dxy + ey = x^3 + ax^2 + bx + c\} \cup \{\mathrm{O}\}$$

사실 이는 아핀평면 $\mathrm{AF}(2, F)$ 를 **사영평면**(射影平面 projective plane) $\mathrm{PG}(2, F)$ 안에서 생각하고 있음을 의미한다([8] 의 §2.5, §2.6 참조).



이제 체 F 의 표수가 0 이거나 또는 홀수인 素數라 하고, 체 F 위에서 다음과 같은 꼴의 타원곡선을 생각해 보자.

$$E : \quad y^2 = x^3 + ax^2 + bx + c$$

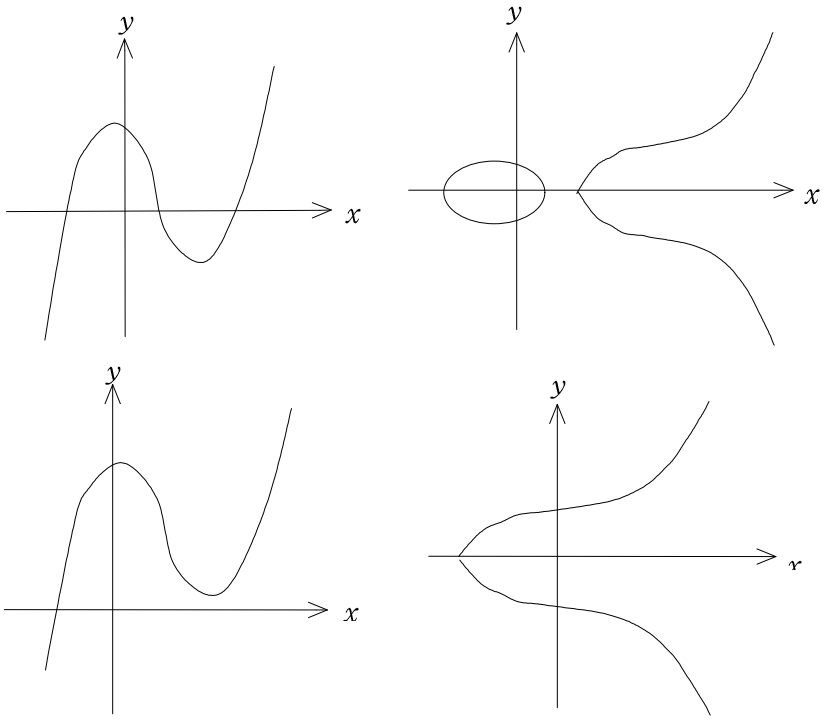
삼차방정식 $x^3 + ax^2 + bx + c = 0$ 은 체 F 의 적당한 확대체 안에서 중복을 허락하여 세 근 α, β, γ 를 가진다고 하자. 이 때,

$$D = \{(\alpha-\beta)(\alpha-\gamma)(\beta-\gamma)\}^2$$

를 삼차다항식 $f(x)\ x^3 + ax^2 + bx + c$ 과 타원곡선 E 의 **판별식**(判別式) 이라고 하며 D 는 다음과 같은 식으로 나타내어진다(정리 4.7.4).

$$D = -27\,c^2 - 4\,a^3c - 4\,b^3 + a^2b^2 + 18\,abc$$

특히, $F = \mathbb{R}$ 인 경우에 $D \neq 0$ 이면, 삼차방정식 $x^3 + ax^2 + bx + c = 0$ 은 서로 다른 세 실근을 갖거나 또는 한 실근과 두 허근을 가지며 이 경우에 $y = x^3 + ax^2 + bx + c$ 와 $y^2 = x^3 + ax^2 + bx + c$ 의 그래프는 다음과 같다.



타원곡선 위의 서로 다른 두 점 $\mathrm{P} = (x_1, y_1)$, $\mathrm{Q} = (x_2, y_2)$ 에 대하여 다음과 같이 정의하자.

$\phi(\mathrm{O}, \mathrm{P}) = \phi(\mathrm{P}, \mathrm{O}) =$ (사영평면 안에서 O, P 를 지나는 직선이 타원곡선과 새로 만나는 점)

$\phi(\mathrm{P}, \mathrm{Q}) = \phi(\mathrm{Q}, \mathrm{P}) =$ (사영평면 안에서 P, Q 를 지나는 직선이 타원곡선과 새로 만나는 점)

점 $\mathrm{P}=(x_1,y_1)$ 가 타원곡선 E 위의 점일 때, 이 점을 지나는 직선의 방정식 $x=x_1$ 을 방정식 $y^2=x^3+ax^2+bx+c$ 에 대입하면

$$y^2={x_1}^3+a{x_1}^2+bx_1+c={y_1}^2$$

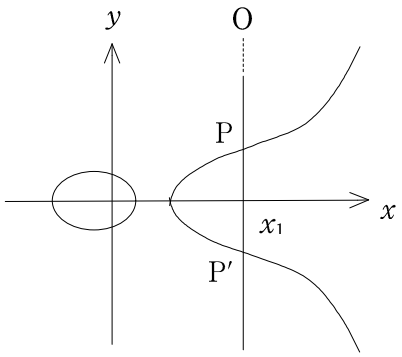
즉 $(y-y_1)(y+y_2)=0$

이므로 $y=y_1$ 또는 $y=-y_1$

이다. 따라서 직선 $x=x_1$ 과 타원곡선 E 와의 교점은

$$\mathrm{P}=(x_1,y_1),\ \mathrm{P}'=(x_1,-y_1)$$

뿐이고, 또 다음이 성립한다.



(1) $\phi(\mathrm{O},\mathrm{P})=\phi(\mathrm{P},\mathrm{O})=\mathrm{P}'$, $\quad\phi(\mathrm{O},\mathrm{P}')=\phi(\mathrm{P}',\mathrm{O})=\mathrm{P}$

$\mathrm{P}\neq\mathrm{P}'$ 이면, $\phi(\mathrm{P},\mathrm{P}')=\phi(\mathrm{P}',\mathrm{P})=\mathrm{O}$ 이다.

다음에 타원곡선 위의 서로 다른 두 점

$$\mathrm{P}=(x_1,y_1),\quad \mathrm{Q}=(x_2,y_2),\qquad x_2\neq x_1$$

에 대하여 $\mathrm{R}=\phi(\mathrm{P},\mathrm{Q})$, $\mathrm{R}'=\phi(\mathrm{O},\mathrm{R})=(x_3,y_3)$ 이라고 하자.

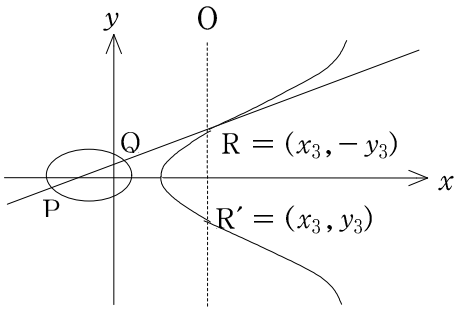
이 때, (1) 에 의하여

$$\mathrm{R}=(x_3,-y_3)$$

이고, 또 직선 PQ 의 기울기는

$k=\dfrac{y_2-y_1}{x_2-x_1}$ 이므로 이 직선의 방정식은 $y=k(x-x_1)+y_1$

이다.



방정식 $y=k(x-x_1)+y_1$ 을 $y^2=x^3+ax^2+bx+c$ 에 대입하여 정리하면, 삼차방정식

$$x^3+(a-k^2)x^2+(b+2k^2x_1-2ky_1)x$$
$$+c-k^2{x_1}^2+kx_1y_1-{y_1}^2=0$$

을 얻고 x_1, x_2, x_3 는 이 방정식의 근이므로 $x_1+x_2+x_3=-(a-k^2)$ 이고

$$k=\frac{y_1-(-y_3)}{x_1-x_3}=\frac{y_1+y_3}{x_1-x_3}$$

이므로 다음 결과를 얻는다.

(2) $k=\frac{y_2-y_1}{x_2-x_1}$, $x_3=k^2-a-(x_1+x_2)$, $y_3=k(x_1-x_3)-y_1$

타원곡선 위의 점 $\mathrm{P}=(x_1, y_1)$에 대하여, 타원곡선 위의 점

$$\mathrm{Q}=(x_2, y_2), \qquad x_2\neq x_1,\ y_2\neq -y_1$$

를 택하여 Q가 타원곡선을 따라 P에 한없이 접근할 때 직선 PQ가 한없이 접근하는 직선을 점 P에서의 **접선**(接線)이라 하고 또 다음과 같이 정의하자.

$\phi(\mathrm{P}, \mathrm{P})=$ (사영평면 $\mathrm{PG}(2, F)$ 안에서 P에서의 접선이 타원곡선과 새로 만나는 점)

이 때, 직선 PQ의 기울기를 m이라고 하면, $m(x_2-x_1)=y_2-y_1$이고 이 직선의 방정식은 $y=m(x-x_1)+y_1$이다. 그런데,

$$m(x_2-x_1)(y_2+y_1)=y_2{}^2-y_1{}^2, \qquad y_2+y_1\neq 0$$

$$y_2{}^2-y_1{}^2=x_2{}^3-x_1{}^3+a(x_2{}^2-x_1{}^2)+b(x_2-x_1)$$

$$=(x_2-x_1)\{(x_2{}^2+x_1x_2+x_1{}^2)+a(x_2+x_1)+b\}$$

이므로 다음이 성립한다.

(3) $\qquad m(y_1+y_2)=x_2{}^2+x_1x_2+x_1{}^2+a(x_2+x_1)+b$

먼저 $y_1\neq 0$인 경우를 생각해 보자. 이 경우에 점 Q가 타원곡선을 따라 점 P에 한없이 접근할 때의 m의 값을 k라고 하면, (3)에서 x_2, y_2는 각각 x_1, y_1에 한없이 접근하므로 다음 결과를 얻는다.

(4) $2y_1k=3x_1{}^2+2ax_1+b$, $\quad k=\frac{3x_1{}^2+2ax_1+b}{2y_1}$

그러므로 $y_1\neq 0$일 때,

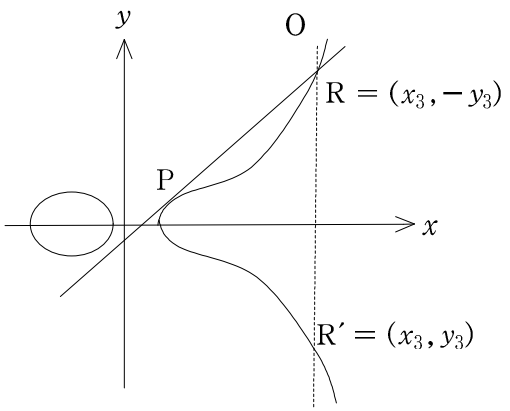
$$\mathrm{R}=\phi(\mathrm{P}, \mathrm{P}), \qquad \mathrm{R}'=\phi(\mathrm{O}, \mathrm{R})=(x_3, y_3)$$

이라고 하면, (1)에 의하여

$$\mathrm{R} = (x_3, -y_3)$$

이고 또 (2)에 의하여 다음이 성립한다.

$$(5)\quad \begin{aligned} x_3 &= k^2 - a - 2x_1, \\ y_3 &= k(x_1 - x_3) - y_1 \end{aligned}$$



다음에 $y_1 = 0$ 인 경우에 $3x_1^2 + 2ax_1 + b \neq 0$ 이다.

실제로, $3x_1^2 + 2ax_1 + b = 0$ 이라고 가정하면, $x_1^3 + ax_1^2 + bx_1 + c = 0$이므로

$$\begin{aligned} & x^3 + ax^2 + bx + c \\ &= (x - x_1)\{x^2 + (x_1 + a)x + x_1^2 + ax_1 + b\} \\ &= (x - x_1)^2(x + 2x_1 + a) \end{aligned}$$

이고, 이것은 삼차방정식 $x^3 + ax^2 + bx + c = 0$ 이 중근 $x = x_1$ 을 가진다는 것을 뜻하므로 $D \neq 0$ 에 모순된다. $3x_1^2 + 2ax_1 + b \neq 0$

따라서 점 Q가 타원곡선을 따라 점 P에 한없이 접근할 때, 등식

$$m(y_1 + y_2) = x_2^2 + x_1x_2 + x_1^2 + a(x_2 + x_1) + b$$

에서 좌변은 0에 접근하고 우변은 에 접근하므로 이 경우에 m의 값은 정해지지 않는다.

그러므로 이 경우에 점 P에서의 접선의 방정식은 $x = x_1$ 이고, 이 접선은 타원곡선과 점 P에서만 만나므로, 점 P에서의 접선이 타원곡선과 새로 만나는 점은 O이다. 즉, $\mathrm{P} = (x_1, 0)$ 일 때, $\phi(\mathrm{P}, \mathrm{P}) = \mathrm{O}$ 이다.

이제 타원곡선 위의 두 점 P, Q와 무한원점 O에 대하여

$$\mathrm{O} + \mathrm{O} = \mathrm{O}, \qquad \mathrm{O} + \mathrm{P} = \phi(\mathrm{O}, \phi(\mathrm{O}, \mathrm{P})),$$
$$\mathrm{P} + \mathrm{O} = \phi(\mathrm{O}, \phi(\mathrm{P}, \mathrm{O})), \quad \mathrm{P} + \mathrm{Q} = \phi(\mathrm{O}, \phi(\mathrm{P}, \mathrm{Q}))$$

이라고 정의하면, 이제까지 얻은 결과에 의하여 다음 정리가 성립함을 증명할 수 있다.

정리 1 체 F 의 표수가 0 이거나 또는 홀수인 素數일 때, 체 F 위에서의 타원곡선

$$E : \quad y^2 = x^3 + ax^2 + bx + c$$

에 대하여 $D = -27c^2 - 4a^3c - 4b^3 + a^2b^2 + 18abc$ 이라고 하자.

여기서 $D \neq 0$ 일 때, 집합

$$G(E, F) = \{(x, y) \in F^2 \mid y^2 = x^3 + ax^2 + bx + c\} \cup \{O\}$$

의 원소 O 와 $P = (x_1, y_1)$, $Q = (x_2, y_2)$ 에 대하여 다음과 같이 정의하면 이와 같이 정의된 덧셈에 관하여 $G(E, F)$ 는 덧셈군을 이룬다.

특히, 홀수인 素數 p 와 양의 정수 m 에 대하여 $q = p^m$ 이라고 할 때, 군 $G(E, \mathbb{F}_q)$ 는 유한 덧셈군이다.

(1) $O + O = O, \quad O + P = P + O = P$

(2) $x_2 = x_1$, $y_2 = -y_1$ 이면, $P + Q = Q + P = O$ 이다.

즉, $P = (x_1, y_1)$ 에 대하여 $-P = (x_1, -y_1)$ 이다.

(3) $x_2 \neq x_1$ 일 때, $P + Q = Q + P = (x_3, y_3)$ 이다. 여기서

$$k = \frac{y_2 - y_1}{x_2 - x_1}, \quad x_3 = k^2 - a - (x_1 + x_2), \quad y_3 = k(x_1 - x_3) - y_1$$

(4) $y_1 \neq 0$ 일 때, $P + P = (x_3, y_3)$ 이다. 여기서

$$k = \frac{3{x_1}^2 + 2ax_1 + b}{2y_1},$$

$$x_3 = k^2 - a - 2x_1, \quad y_3 = k(x_1 - x_3) - y_1$$

앞의 정리에서 $F = \mathbb{F}_q$ 인 경우에

$$D = -27c^2 - 4a^3c - 4b^3 + a^2b^2 + 18abc$$

는 q 에 따라 다음과 같음을 의미한다.

$q = 3^m$ 일 때, $D = 2a^3c + 2b^3 + a^2b^2$

$q = 5^m$ 일 때, $D = 3c^2 + a^3c + b^3 + a^2b^2 + 3abc$

$q = 7^m$ 일 때, $D = c^2 + 3a^3c + 3b^3 + a^2b^2 + 4abc$

보기 1 실수체 $\mathbb{R}$ 에서 다음과 같은 타원곡선을 생각해 보자.

$$E: \quad y^2 = x^3 + 1$$

먼저 $D = -27 \neq 0$ 이고 또 덧셈군 $G(E, \mathbb{R})$ 에서 다음이 성립한다.

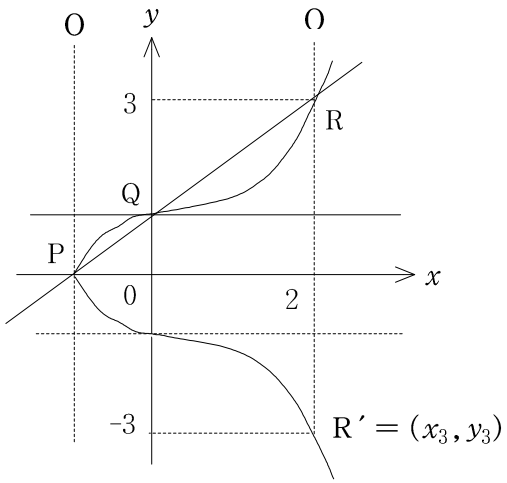
(1) $\mathrm{P} = (-1, 0)$ 일 때, 다음이 성립한다.

$$\mathrm{P} + \mathrm{P} = \mathrm{O} \quad \text{즉} \quad -\mathrm{P} = \mathrm{P} = (-1, 0)$$

(2) 타원곡선 E 위의 두 점

$$\mathrm{P} = (x_1, y_1) = (-1, 0), \qquad \mathrm{Q} = (x_2, y_2) = (0, 1)$$

에 대하여 직선 PQ 의 방정식은 $y = x + 1$ 이고, 또 이 직선이 E 와 새로 만나는 점은 $\mathrm{R} = (2, 3)$ 이므로 $\mathrm{P} + \mathrm{Q} = (2, -3)$ 이다.



실제로,

$$\mathrm{P} + \mathrm{Q} = (x_3, y_3)$$

이라고 할 때, 다음이 성립한다.

$$k = \frac{y_2 - y_1}{x_2 - x_1} = \frac{1-0}{0+1} = 1,$$

$$x_3 = k^2 - a - (x_1 + x_2)$$
$$= 1 - 0 - (-1 + 0) = 2,$$

$$y_3 = k(x_1 - x_3) - y_1$$
$$= (-1 - 2) - 0 = -3$$

(3) 타원곡선 위의 점 $\mathrm{Q} = (0, 1)$ 에서의 접선의 기울기는 $k = \dfrac{3{x_1}^2}{2y_1} = 0$ 이므로 접선의 방정식은 $y = 1$ 이다.

또, $y = 1$ 을 $y^2 = x^3 + 1$ 에 대입하여 얻은 방정식 $x^3 = 0$ 은 삼중근 $x = 0$ 을 가지므로 접선과 타원곡선과의 교점은 $\mathrm{Q} = (0, 1)$ 이고, 따라서 다음이 성립한다.

$$2\mathrm{Q} = \mathrm{Q} + \mathrm{Q} = (0, -1)$$

보기 2 체 $\mathbb{F}_5 = \{0,1,2,3,4\}$ 위에서의 타원곡선

$$E : \quad y^2 = x^3 + 1$$

에 대하여 $D = 3c^2 + a^3c + b^3 + a^2b^2 + 3abc = 3 \neq 0$ 이고, 체 $\mathbb{F}_5$ 에서

$$0^2 = 0, \quad (\pm 1)^2 = 1, \quad (\pm 2)^2 = 4$$

이므로 (x, y) 가 이 타원곡선 위의 점일 때 다음이 성립한다.

$x = 0$ 인 경우에 $y^2 = 0^3 + 1 = 1$ 이므로 $y = 1,\ y = -1 = 4$ 이다.

$x = 1$ 인 경우에 $y^2 = 1^3 + 1 = 2$ 이고 이러한 y는 존재하지 않는다.

$x = 2$ 인 경우에 $y^2 = 2^3 + 1 = 4$ 이므로 $y = 2,\ y = -2 = 3$ 이다.

$x = 3$ 인 경우에 $y^2 = 3^3 + 1 = 3$ 이고 이러한 y는 존재하지 않는다.

$x = 4 = -1$ 인 경우에 $y^2 = (-1)^3 + 1 = 0$ 이므로 $y = 0$ 이다.

따라서 $G(E, \mathbb{F}_5)$는 다음과 같은 위수 6 인 덧셈군이다.

$$G(E, \mathbb{F}_5) = \{(0,1), (0,4), (2,2), (2,3), (4,0), \mathrm{O}\}$$

그리고, 다음이 성립한다.

(1) $\mathrm{P} = (4,0)$ 이면, $-\mathrm{P} = \mathrm{P}$ 이다.

(2) $\mathrm{P} = (2,3),\ \mathrm{Q} = (4,0)$ 일 때, $\mathrm{P} + \mathrm{Q} = (x_3, y_3)$ 이라고 하면,

$$k = \frac{y_2 - y_1}{x_2 - x_1} = \frac{-3}{2} = 2 \cdot 2^{-1} = 2 \cdot 3 = 1$$

$$x_3 = k^2 - (x_1 + x_2) = 1^2 - (2+4) = 1 - 1 = 0,$$

$$y_3 = k(x_1 - x_3) - y_1 = 2 - 3 = -1 = 4$$

이므로 $\mathrm{P} + \mathrm{Q} = (0,4)$ 이다.

(3) $\mathrm{P} = (2,3)$ 일 때, $2\mathrm{P} = \mathrm{P} + \mathrm{P} = (x_3, y_3)$ 이라고 하면

$$k = \frac{3{x_1}^2}{2y_1} = \frac{3 \cdot 2^2}{2 \cdot 3} = \frac{2}{1} = 2,$$

$$x_3 = k^2 - 2x_1 = 0, \quad y_3 = k(x_1 - x_3) - y_1 = 1$$

이므로 $2\mathrm{P} = (0,1)$ 이다. 마찬가지로, 다음이 성립한다.

$$3\mathrm{P} = 2\mathrm{P} + \mathrm{P} = (4, 0), \quad 4\mathrm{P} = 3\mathrm{P} + \mathrm{P} = (0, 4),$$
$$5\mathrm{P} = 4\mathrm{P} + \mathrm{P} = (2, 2), \quad 6\mathrm{P} = 5\mathrm{P} + \mathrm{P} = \mathrm{O}$$

따라서 덧셈군 $G(E, \mathbb{F}_5)$는 P 를 생성원으로 가지는 순환군이다. 즉,

$$G(E, \mathbb{F}_5) = \langle \mathrm{P} \rangle = \{\mathrm{O}, \mathrm{P}, 2\mathrm{P}, 3\mathrm{P}, 4\mathrm{P}, 5\mathrm{P}\}, \quad 6\mathrm{P} = \mathrm{O}$$

보기 3 체 $\mathbb{F}_7 = \{0,1,2,3,4,5,6\}$ 위에서의 타원곡선

$$E : \quad y^2 = x^3 + 3$$

에 대하여 $D = c^2 + 3a^3c + 3b^3 + a^2b^2 + 4abc = 3^2 = 2 \neq 0$ 이다.

한편, 체 $\mathbb{F}_7$ 에서 $0^2 = 0$, $(\pm 1)^2 = 1$, $(\pm 2)^2 = 4$, $(\pm 3)^2 = 2$ 이므로 $G(E, \mathbb{F}_7)$은 다음과 같은 13 개의 원소로 이루어진 덧셈군이다.

$$G(E, \mathbb{F}_7) = \{(1, 2), (1, 5), (2, 2), (2, 5), (3, 3), (3, 4),$$
$$(4, 2), (4, 5), (5, 3), (5, 4), (6, 3), (6, 4), \mathrm{O}\}$$

예를 들어, $\mathrm{P} = (1, 2)$ 일 때,

$$k = \frac{3{x_1}^2}{2y_1} = \frac{3}{2 \cdot 2} = 3 \cdot 4^{-1} = 3 \cdot 2 = 6 = -1,$$
$$x_3 = k^2 - 2x_1 = (-1)^2 - 2 \cdot 1 = 1 - 2 = -1 = 6,$$
$$y_3 = k(x_1 - x_3) - y_1 = (-1) \cdot 2 - 2 = -4 = 3$$

이므로 $2\mathrm{P} = \mathrm{P} + \mathrm{P} = (6, 3)$ 이고, 또 $3\mathrm{P} = (2, 2)$ 이다.

실제로, $G(E, \mathbb{F}_7)$는 위수 13 인 순환군이고 또 임의의 원소 $\mathrm{P} \neq \mathrm{O}$ 에 대하여 다음이 성립한다.

$$G(E, \mathbb{F}_7) = \langle \mathrm{P} \rangle = \{\mathrm{O}, \mathrm{P}, 2\mathrm{P}, 3\mathrm{P}, \cdots, 12\mathrm{P}\}, \quad 13\mathrm{P} = \mathrm{O}$$

정리 1 에서 $F = \mathbb{F}_q$, $q = 3^m$ 인 경우에

$$D = 2a^3c + 2b^3 + a^2b^2$$

이므로 $b = 0$, $a^3c \neq 0$ 또는 $a = 0$, $b \neq 0$ 일 때 $D \neq 0$ 이다. 또, (4) 의 등식 에서 $3{x_1}^2$, $2ax_1$, $2y_1$, $-2x_1$ 은 각각 0, $-ax_1$, $-y_1$, x_1 과 같으므로 이들 세 등식은 각각 다음과 같이 고쳐 쓸 수 있다.

$$k=\frac{ax_1-b}{y_1},$$

$$x_3=k^2-a+x_1,\quad y_3=k(x_1-x_3)-y_1$$

따라서 다음 따름정리가 성립한다.

따름정리 2 Galois 체 $\mathbb{F}_{3^m}$ 위에서의 타원곡선

$$E:\quad y^2=x^3+ax^2+bx+c$$

에 대하여 $b=0,\ a^3c\neq 0$ 또는 $a=0,\ b\neq 0$ 이라고 하자. 이 때, 집합

$$G(E,\mathbb{F}_{3^m})=\{(x,y)\in \mathbb{F}_{3^m}{}^2 \mid y^2=x^3+ax^2+bx+c\}\cup\{\mathrm{O}\}$$

의 원소 O 와 $\mathrm{P}=(x_1,y_1),\ \mathrm{Q}=(x_2,y_2)$ 에 대하여 다음과 같이 정의하면 이와 같이 정의한 덧셈에 관하여 $G(E,\mathbb{F}_{3^m})$ 은 유한 덧셈군을 이룬다.

(1) $\mathrm{O}+\mathrm{O}=\mathrm{O},\quad \mathrm{O}+\mathrm{P}=\mathrm{P}+\mathrm{O}=\mathrm{P}$

(2) $x_2=x_1,\ y_2=-y_1$ 이면, $\mathrm{P}+\mathrm{Q}=\mathrm{Q}+\mathrm{P}=\mathrm{O}$ 이다.

즉, $\mathrm{P}=(x_1,y_1)$ 에 대하여 $-\mathrm{P}=(x_1,-y_1)$ 이다.

(3) $x_2\neq x_1$ 일 때, $\mathrm{P}+\mathrm{Q}=\mathrm{Q}+\mathrm{P}=(x_3,y_3)$ 이다. 여기서

$$k=\frac{y_2-y_1}{x_2-x_1},\quad x_3=k^2-a-(x_1+x_2),\quad y_3=k(x_1-x_3)-y_1$$

(4) $y_1\neq 0$ 일 때, $\mathrm{P}+\mathrm{P}=(x_3,y_3)$ 이다. 여기서

$$k=\frac{ax_1-b}{y_1},\quad x_3=k^2-a+x_1,\quad y_3=k(x_1-x_3)-y_1$$

Galois 체 $\mathbb{F}_{2^m}$ 은 표수가 2 인 유한체이므로, Galois 체 $\mathbb{F}_{2^m}$ 에서 다음이 성립한다.

$$x_1+x_1=0,\quad -x_1=x_1,\quad (x_1+x_2)^2=x_1+x_2$$

이제 Galois 체 $\mathbb{F}_{2^m}$ 위에서 다음과 같은 타원곡선을 생각해 보자.

$$E_1:\quad y^2+xy=x^3+ax^2+c\qquad (c\neq 0)$$

점 $P=(x_1, y_1)$ 가 이 타원곡선 위의 점이라고 할 때, $x=x_1$ 을 E_1 에 에 대입하여 정리하면 다음 결과를 얻는다.

$$y^2+x_1y=x_1{}^3+ax_1{}^2+c=y_1{}^2+x_1y_1,$$
$$y^2+y_1{}^2=x_1y+x_1y_1 \text{ 즉 } (y+y_1)^2+x_1(y+y_1)=0,$$
$$(y+y_1)(y+y_1+x_1)=0,$$
$$y+y_1=0 \quad \text{또는} \quad y+y_1+x_1=0$$

따라서 $y=y_1$ 또는 $y=y_1+x_1$ 이므로 직선 $x=x_1$ 과 타원곡선 E_1 의 교점은 $P=(x_1, y_1)$, $P'=(x_1, y_1+x_1)$ 뿐이다. 이 사실을 이용하면, 정리 .1 의 증명과 마찬가지 방법으로 다음이 성립함을 증명할 수 있다.

정리 3 Galois 체 $\mathbb{F}_{2^m}$ 위에서의 타원곡선

$$E_1 : \quad y^2+xy=x^3+ax^2+c \qquad (c\neq 0)$$

에 대하여

$$G(E_1, \mathbb{F}_{2^m})=\{(x, y)\in \mathbb{F}_{2^m}{}^2 \mid y^2+xy=x^3+ax^2+c\}\cup\{O\}$$

이라고 할 때, $G(E_1, \mathbb{F}_{2^m})$ 의 원소 O, $P=(x_1, y_1)$, $Q=(x_2, y_2)$ 에 대하여 다음과 같이 정의하면 이와 같이 정의된 덧셈에 관하여 $G(E_1, \mathbb{F}_{2^m})$ 은 유한 덧셈군을 이룬다.

(1) $O+O=O, \quad O+P=P+O=P$

(2) $x_2=x_1$, $y_2=x_1+y_1$ 이면, $P+Q=Q+P=O$ 이다.
즉, $P=(x_1, y_1)$ 에 대하여 $-P=(x_1, y_1+x_1)$ 이다.

(3) $x_1\neq x_2$ 이면, $P+Q=Q+P=(x_3, y_3)$ 이다. 여기서

$$k=\frac{y_1+y_2}{x_1+x_2},$$
$$x_3=k^2+k+a+(x_1+x_2), \quad y_3=k(x_1+x_3)+y_1+x_3$$

(4) $x_1\neq 0$ 이면, $P+P=(x_3, y_3)$ 이다. 여기서

$$x_3=x_1{}^2+\frac{c}{x_1{}^2}, \quad y_3=x_1{}^2+\left(x_1+\frac{y_1}{x_1}\right)x_3+x_3$$

보기 4 체 $\mathbb{F}_2 = \{0, 1\}$ 위의 다항식 $p(x) = x^4 + x + 1$ 는 4차의 원시다항식이다(보기 4.2.5). 이제 $p(\alpha) = 0$ 인 원소 α 를 도입하면, 다음과 같이 2^4 개의 원소로 이루어진 Galois 체 $\mathbb{F}_{2^4}$ 를 얻는다.

$$\mathbb{F}_{2^4} = \{a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 \mid a_0, a_1, a_2, a_3 \in \mathbb{F}_2\}$$

$$p(\alpha) = \alpha^4 + \alpha + 1 = 0 \quad \text{즉} \quad \alpha^4 = 1 + \alpha$$

$$\begin{array}{lll} \alpha^1 = \alpha, & \alpha^2 = \alpha^2, & \alpha^3 = \alpha^3 \\ \alpha^4 = 1 + \alpha, & \alpha^5 = \alpha + \alpha^2, & \alpha^6 = \alpha^2 + \alpha^3 \\ \alpha^7 = 1 + \alpha + \alpha^3, & \alpha^8 = 1 + \alpha^2, & \alpha^9 = \alpha + \alpha^3 \\ \alpha^{10} = 1 + \alpha + \alpha^2, & \alpha^{11} = \alpha + \alpha^2 + \alpha^3, & \alpha^{12} = 1 + \alpha + \alpha^2 + \alpha^3 \\ \alpha^{13} = 1 + \alpha^2 + \alpha^3, & \alpha^{14} = 1 + \alpha^3, & \alpha^{15} = 1 \end{array}$$

이제 Galois $\mathbb{F}_{2^4}$ 위에서 다음과 같은 타원곡선을 생각해 보자.

$$E_1 : \quad y^2 + xy = x^3 + \alpha^4 x^2 + 1$$

점 (x_1, y_1) 가 이 타원곡선 위의 점일 때, $(x_1, y_1 + x_1)$ 도 이 타원곡선 위의 점이다. 따라서 (x, y) 가 이 타원곡선 위의 점일 때 다음이 성립한다.

$x = 0$ 인 경우에 $y^2 = 1$ 이므로 $y = 1$ 이다.

$x = 1$ 인 경우에 $y^2 + y = 1 + \alpha^4 + 1$ 즉 $y(y + 1) = \alpha^4$ 이고 또

$$\alpha^6(\alpha^6 + 1) + \alpha^4 = \alpha^6\alpha^{13} = \alpha^{19} = \alpha^4$$

이므로 $y = \alpha^6$, $y = \alpha^6 + 1 = \alpha^{13}$ 이다.

$x = \alpha$ 인 경우에 $y^2 + \alpha y = \alpha^3 + \alpha^6 + 1$ 즉 $y^2 + \alpha y = \alpha^8$ 이고

이러한 y 는 존재하지 않는다.

$x = \alpha^2$ 인 경우에 $y^2 + \alpha^2 y = \alpha^6 + \alpha^8 + 1$ 즉 $y^2 + \alpha^2 y = \alpha^3$ 이고

이러한 y 는 존재하지 않는다.

$x = \alpha^3$ 인 경우에 $y^2 + \alpha^3 y = \alpha^9 + \alpha^{10} + 1 = \alpha^2 + \alpha^3 = \alpha^6$ 이므로

$y(y + \alpha^3) = \alpha^6$ 이고 또

$$\alpha^8(\alpha^8 + \alpha^3) = \alpha^8\alpha^{13} = \alpha^{21} = \alpha^6$$

이므로 $y = \alpha^8$, $y = \alpha^8 + \alpha^3 = \alpha^{13}$ 이다.

이와 같은 방법으로 $G(E_1, \mathbb{F}_{2^4})$ 가 다음과 같은 위수 16 인 덧셈군임을 알 수 있다(문제 5 참조).

$$\begin{aligned} G(E_1, \mathbb{F}_{2^4}) = \{&(0,1), (1,\alpha^6), (1,\alpha^{13}), (\alpha^3,\alpha^8),\\ &(\alpha^3,\alpha^{13}), (\alpha^5,\alpha^3), (\alpha^5,\alpha^{11}), (\alpha^6,\alpha^8),\\ &(\alpha^6,\alpha^{14}), (\alpha^9,\alpha^{10}), (\alpha^9,\alpha^{13}), (\alpha^{10},\alpha),\\ &(\alpha^{10},\alpha^8), (\alpha^{12},0), (\alpha^{12},\alpha^{12}), O\} \end{aligned}$$

그리고, $P = (x_1, y_1) = (1, \alpha^6)$ 일 때, $2P = P + P = (x_3, y_3)$ 이라고 하면, 정리 4.4.3 에 의하여

$$x_3 = {x_1}^2 + \frac{c}{{x_1}^2} = 1^2 + \frac{1}{1^2} = 1 + 1 = 0,$$

$$y_3 = {x_1}^2 + (x_1 + \frac{y_1}{x_1})\, x_3 + x_3 = 1^2 + 0 + 0 = 1$$

이므로 $2P = (0, 1)$ 이다.

또, 정리 4.4.3 에 의하여 $4P = 2P + 2P = O$ 이다.

Galois 체 $\mathbb{F}_{2^m}$ 위에서 다음과 같은 타원곡선을 생각해 보자.

$$E_2 : \quad y^2 + ey = x^3 + bx + c \qquad (c \neq 0,\ e \neq 0)$$

점 $P = (x_1, y_1)$ 가 이 타원곡선 위의 점이라고 할 때, $x = x_1$ 을 방정식 $y^2 + ey = x^3 + bx + c$ 에 대입하여 정리하면 다음 결과를 얻는다.

$$\begin{aligned} &y^2 + ey = {x_1}^3 + bx_1 + c = {y_1}^2 + ey_1,\\ &y^2 + {y_1}^2 = e(y + y_1) \quad \text{즉} \quad (y + y_1)^2 = e(y + y_1),\\ &(y + y_1)(y + y_1 + e) = 0,\\ &y + y_1 = 0 \quad \text{또는} \quad y + y_1 + e = 0 \end{aligned}$$

따라서 $y = y_1$ 또는 $y = y_1 + e$ 이므로 직선 $x = x_1$ 과 타원곡선 E_2 와의 교점은 $P = (x_1, y_1)$, $P' = (x_1, y_1 + e)$ 뿐이다. 이 사실을 이용하면, 정리 1 의 증명과 마찬가지 방법으로 다음 정리가 성립함을 밝힐 수 있다.

정리 4 Galois 체 $\mathbb{F}_{2^m}$ 위에서의 타원곡선

$$E_2 : \quad y^2 + ey = x^3 + bx + c \qquad (c \neq 0,\ e \neq 0)$$

에 대하여

$$G(E_2, \mathbb{F}_{2^m}) = \{(x, y) \in \mathbb{F}_{2^m}{}^2 \mid y^2 + ey = x^3 + bx + c\} \cup \{O\}$$

이라고 할 때, $G(E_2, \mathbb{F}_{2^m})$의 원소 O, $P = (x_1, y_1)$, $Q = (x_2, y_2)$에 대하여 다음과 같이 정의하면, 이와 같이 정의된 덧셈에 관하여 $G(E_2, \mathbb{F}_{2^m})$은 유한 덧셈군을 이룬다.

(1) $O + O = O, \quad O + P = P + O = P$

(2) $x_2 = x_1$, $y_2 = e + y_1$ 일 때, $P + Q = Q + P = O$ 이다.

즉 $P = (x_1, y_1)$에 대하여 $-P = (x_1, e + y_1)$ 이다.

(3) $x_2 \neq x_1$ 일 때, $P + Q = (x_3, y_3 + e)$ 이다. 여기서

$$k = \frac{y_1 + y_2}{x_1 + x_2},$$

$$x_3 = k^2 + (x_1 + x_2), \quad y_3 = k(x_1 + x_3) + y_1 + e$$

(4) $P + P = (x_3, y_3)$ 여기서

$$k = \frac{x_1{}^2 + b}{e},$$

$$x_3 = k^2, \quad y_3 = k(x_1 + x_3) + y_1 + e$$

앞에서 논한 덧셈군 $G(E, \mathbb{F}_q)$, $G(E_1, \mathbb{F}_{2^m})$, $G(E_2, \mathbb{F}_{2^m})$에서의 덧셈 $P + Q$를 보다 빠르게 계산해내는 고속화 알고리즘이 개발되어 있다.

§ 5.9.2 타원곡선을 이용한 암호체계

여기서는, [4] 의 §4.5 의 내용을 소개하기로 한다.

타원곡선에 대한 이론은 오래 전부터 광범위하게 연구되어 왔으나, 최근에 이르러 타원곡선을 이용한 정수의 인수분해 알고리즘과 타원곡선을 이용한 암호체계에 대한 연구가 활발히 진행되고 있다.

이 절에서는, 타원곡선을 이용한 여러 가지 공개 열쇠 암호체계에 대하여 논하기로 한다. 그리고, 타원곡선을 이용한 정수의 인수분해 알고리즘에 대해서는 '해설 인수분해'를 참조하기 바란다.

임의의 素數 p 와 양의 정수 m 에 대하여 $q = p^m$ 이라고 할 때, Galois 체 $\mathbb{F}_q$ 가 정의되고 체 $\mathbb{F}_q$ 에서의 타원곡선 E 에 대하여 덧셈군 $G(E, \mathbb{F}_q)$ 는 유한군이다. 덧셈군 $G(E, \mathbb{F}_q)$ 의 위수가 N 일 때, 이 유한군의 각 원소 P 에 대하여

$$NP = P + \cdots + P = O \qquad (P \text{는 } N \text{개})$$

이며, P 의 위수를 n_P 라고 하면

$$\langle P \rangle = \{O, P, 2P, \cdots, (n_P - 1)P\},$$

$$n_P P = P + \cdots + P = O \qquad (P \text{는 } n_P \text{개})$$

이고 Lagrange 의 정리에 의하여 n_P 는 N 의 약수이다.

한편, n_P 가 상당히 큰 경우에 각 양의 정수 k 에 대하여 $Q = kP$ 인 Q 를 구하는 일은 쉬우나, 임의의 $Q \in \langle P \rangle$, $Q \neq O$ 에 대하여

$$Q = kP, \qquad 1 \leq k < n_P$$

인 정수 k 를 구하는 일은 그리 쉽지 않다.

이산로그를 구하는 문제를 **이산로그 문제**라고 한다.

타원곡선에 관한 이산로그 문제를 이용한 공개 열쇠 암호체계에서는 먼저 적당한 Galois 체 $\mathbb{F}_q$ 를 정한다. 여기서 $q = p^m$ 가 홀수인 경우에는,

$$E : \quad y^2 = x^3 + ax^2 + bx + c$$

와 같은 꼴의 타원곡선을 택하여 앞의 정리 1 또는 따름정리 2 를 이용한다.

한편, $q = 2^m$ 인 경우에는

$$E_1 : \quad y^2 + xy = x^3 + ax^2 + c \qquad (c \neq 0)$$

$$E_2 : \quad y^2 + ey = x^3 + bx + c \qquad (c \neq 0,\ e \neq 0)$$

와 같은 꼴의 타원곡선을 택하여 정리 4.4.3 또는 정리 4.4.4 를 이용한다.

실제로는 주로 Galois 체 $\mathbb{F}_{2^m}$ 위에서의 타원곡선을 이용하며, 이 경우에 공격자의 공격을 피하려면 덧셈군 $G(E_1, \mathbb{F}_{2^m})$ 또는 $G(E_2, \mathbb{F}_{2^m})$ 의 위수가 2^{120} 보다 크거나 상당히 큰 소인수를 가져야 한다는 사실이 알려져 있다.

이미 §3.2 에서 논한 Diffie-Hellman 의 열쇠 교환 프로토콜은 p 가 素數일 때의 곱셈군 $\mathbb{Z}_p^* = \{0, 1, \cdots, p-1\}$ 을 이용한 것이고, 다음에 소개할 프로토콜은 이 프로토콜을 적당한 Galois 체 $\mathbb{F}_q$ 에서의 타원곡선 E 에 대한 유한 덧셈군 $G(E, \mathbb{F}_q)$ 를 이용한 프로토콜로 바꾸어 놓은 것이다

[1] 타원곡선을 이용한 열쇠 교환

두 사용자 A, B 가 동일한 비밀 열쇠를 서로 교환하기 위하여, 먼저 적당한 Galois 체 $\mathbb{F}_q$ 와 적당한 타원곡선 E 를 정하고 유한 덧셈군 $G(E, \mathbb{F}_q)$ 의 원소 중에서 그 위수가 상당히 큰 원소 P 를 정하여 $\mathbb{F}_q, E,$ P 를 공개한다.

(1) 사용자 A 는 양의 정수 r 를 임의로 택하여

$$\mathrm{Q}_1 = r\mathrm{P}$$

인 Q_1 을 구하고 이것을 B 에게 보낸다.

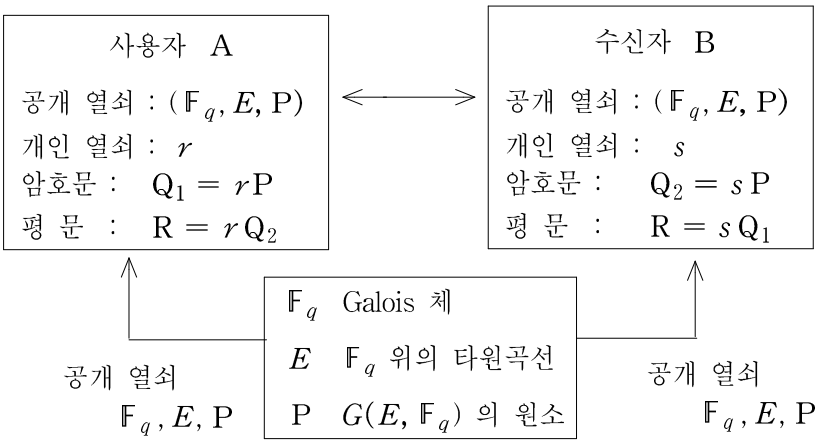
(2) 사용자 B 는 양의 정수 s 를 임의로 택하여

$$\mathrm{Q}_2 = s\mathrm{P}$$

인 Q_2 를 구하고 이것을 A 에게 보낸다.

(3) 사용자 A 는 $\mathrm{R} = r\mathrm{Q}_2$ 인 R 를 구하여 R 를 열쇠로 사용한다.

(4) 사용자 B 는 $\mathrm{R} = s\mathrm{Q}_1$ 인 R 를 구하여 R 를 열쇠로 사용한다.



앞의 단계 (3)과 단계 (4)에서

$$rQ_2 = r(sP) = rsP = s(rP) = sQ_1$$

이므로, 이 두 단계에서 구한 R는 일치한다.

그리고 $\mathbb{F}_q$, E와 P를 적절히 택하면, 공격자는 Q_1, Q_2를 알더라도 열쇠 R를 알아낼 수 없다. 실제로, R를 구하려면 r 또는 s의 값을 알아야 하는데, 이는 타원곡선에 대한 이산로그 문제로서 Q_1, Q_2를 이용하여 합당한 시간 안에 r 또는 s의 값을 구하기는 대단히 어렵다.

보기 1 체 $\mathbb{F}_{11} = \{0, 1, 2, \cdots, 9, 10\}$ 위에서의 타원곡선

$$E : \quad y^2 = x^3 + x + 6$$

에 대하여 $G(E, \mathbb{F}_{11})$은 다음과 같은 위수 13인 덧셈군이다(문제 4.4.4).

$$G(E, \mathbb{F}_{11}) = \{(2,4), (2,7), (3,5), (3,6), (5,2), (5,9),$$
$$(7,2), (7,9), (8,3), (8,8), (10,2), (10,9)\} \cup \{O\}$$

실제로, 점 $P = (2, 4)$에 대하여 다음이 성립한다.

$$G(E, \mathbb{F}_{11}) = \langle P \rangle = \{P, 2P, \cdots, 12P, O\}, \ 13P = O$$

이제 두 사용자 A, B가 같은 비밀 열쇠를 서로 교환하기 위하여 덧셈군 $G(E, \mathbb{F}_{11})$의 원소 중에서 $P = (2, 4)$를 택하고 $\mathbb{F}_{11}$, E, P를 공개한다.

(1) 사용자 A는 $r=2$를 택하여

$$Q_1 = rP = 2(2,4)$$

를 구하면 $Q_1=(5,9)$이고, 이것을 B에게 보낸다.

(2) 사용자 B는 $s=3$를 택하여

$$Q_2 = sP = 3(2,4)$$

를 구하면 $Q_2=(8,8)$이고, 이것을 A에게 보낸다.

(3) 사용자 A는 $R = rQ_2 = 2(8,8) = (7,2)$를 구하여 R를 열쇠로 사용한다.

(4) 사용자 B는 $R = sQ_1 = 3(5,9) = 7,2)$를 구하여 R를 열쇠로 사용한다.

위의 (1)과 (2)에서 Q_1, Q_2는 정리 4.4.1을 이용하여 다음과 같이 구한다.

(1) $Q_1 = rP = 2P = P + P = (5,9)$

$$k = \frac{3x_1^{\,2} + 2ax_1 + b}{2y_1} = \frac{3\cdot 2^2 + 1}{2\cdot 4} = 2\cdot 8^{-1} = 2\cdot 7 = 3,$$

$$x_3 = k^2 - a - 2x_1 = 3^2 - 2\cdot 2 = 9 - 4 = 5,$$

$$y_3 = k(x_1 - x_3) - y_1 = 3(2-5) - 4 = -9 - 4 = 9$$

(2) $Q_2 = sP = 3P = P + 2P$

$$k = \frac{y_2 - y_1}{x_2 - x_1} = \frac{9-4}{5-2} = 5\cdot 3^{-1} = 5\cdot 4 = 9,$$

$$x_3 = k^2 - a - (x_1 + x_2) = 9^2 - (2+5) = 4 - 7 = 8,$$

$$y_3 = k(x_1 - x_3) - y_1 = 9(2-8) - 4 = 9\cdot 5 - 4 = 1 - 4 = 8$$

$$Q_2 = 3(2,4) = P + 2P = (2,4) + (5,9) = (8,8)$$

ElGamal 암호체계는 홀수인 素數 p에 대한 곱셈군 $\mathbb{Z}_p^*$의 특성을 이용한 암호체계이다(§3.4 참조). 다음 프로토콜은 이것을 유한 덧셈군 $G(E, \mathbb{F}_q)$를 이용한 프로토콜로 바꾸어 놓은 것이다.

[2] 타원곡선을 이용한 ElGamal 암호체계

(1) 수신자 A는 적당한 Galois 체 $\mathbb{F}_q$와 이 체 위에서의 적당한 타원곡선 E를 정하고 덧셈군 $G(E, \mathbb{F}_q)$의 원소 중에서 그 위수가 상당히 큰 원소 P를 정한다. 또, 양의 정수 r를 임의로(randomly) 택하고

$$\mathrm{Q} = r\mathrm{P}$$

를 구하여 $\mathbb{F}_q, E, \mathrm{P}, \mathrm{Q}$는 공개하고 r는 공개하지 않는다.

즉, 사용자 A의 공개 열쇠는 $\mathbb{F}_q, E, \mathrm{P}, \mathrm{Q}$이고 비밀 열쇠는 r이다.

(2) 송신자 U는 사용자 A에게 전송할 평문을 덧셈군 $G(E, \mathbb{F}_q)$의 원소 R로 나타낸다.

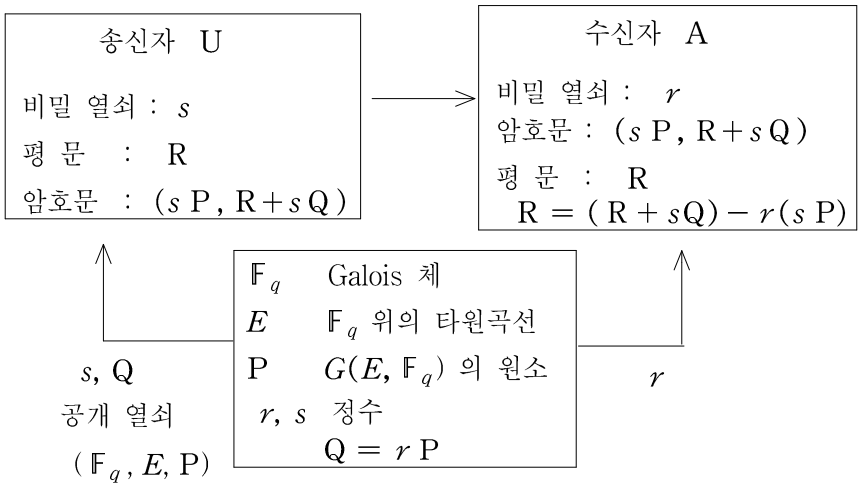
(3) 송신자 U는 양의 정수 s를 임의로 택하고, 평문 R에 대한 암호문 $(s\mathrm{P}, \mathrm{R}+s\mathrm{Q})$를 구하고 이것을 A에게 전송한다.

(4) 수신자 A는 자신의 비밀 열쇠 r를 이용하여

$$(\mathrm{R}+s\mathrm{Q}) - r(s\mathrm{P}) = \mathrm{R} + sr\mathrm{P} - rs\mathrm{P} = \mathrm{R}$$

를 구하고 이로부터 평문 R를 얻는다.

여기서 $\mathbb{F}_q, E, \mathrm{P}, r, \mathrm{Q}$는 A에 따라 달라지고 s는 U에 따라 달라진다.



이 암호체계에서 공격자가 $s\mathrm{P}$, $rs\mathrm{P}$ 를 알고 있더라도 $rs\mathrm{P} = r(s\mathrm{P})$ 로부터 r 를 구하려면 타원곡선에 대한 이산로그의 문제를 해결해야 한다.

이 프로토콜에서 유한 덧셈군 $G(E, \mathbb{F}_q)$ 의 위수를 결정하지 않아도 좋으므로 이 암호체계는 실용적인 면에서 대단히 유용하다.

보기 2 체 $\mathbb{F}_{11} = \{0, 1, 2, \cdots, 9, 10\}$ 에서의 타원곡선

$$E : \ y^2 = x^3 + x + 6$$

에 대하여 덧셈군 $G(E, \mathbb{F}_{11})$ 은 다음과 같다(보기 4.5.1 참조).

$$G(E, \mathbb{F}_{11}) = \{(2,4), (2,7), (3,5), (3,6), (5,2), (5,9),$$
$$(7,2), (7,9), (8,3), (8,8), (10,2), (10,9)\} \cup \{\mathrm{O}\}$$

수신자 A 는 덧셈군 $G(E, \mathbb{F}_{11})$ 의 원소 중에서 $\mathrm{P} = (2, 4)$ 를 택하고 또 $\mathbb{F}_{11}$, E, P 를 공개한다. 그리고 $r = 5$ 를 택하고

$$\mathrm{Q} = r\mathrm{P} = 5(2, 4) = (3, 5)$$

를 구하여, Q 는 공개하고 r 는 공개하지 않는다.

송신자 U 가 수신자 A 에게 전송할 평문이 $\mathrm{R} = (8, 3)$ 일 때, 송신자 U 는 $s = 3$ 를 택하여

$$s\mathrm{P} = 3(2, 4) = (8, 8),$$
$$\mathrm{R} + s\mathrm{Q} = (8, 3) + 3(3, 5) = (8, 3) + (5, 9) = (2, 7)$$

를 계산하고 암호문 $(s\mathrm{P}, \mathrm{R} + s\mathrm{Q})$ 를 A 에게 전송한다.

수신자 A 는 자신의 비밀 열쇠 $r = 5$ 를 이용하여

$$(\mathrm{R} + s\mathrm{Q}) - r(s\mathrm{P}) = (2, 7) - 5(8, 8)$$

를 구하고 이로부터 평문 $\mathrm{R} = (8, 3)$ 를 얻는다.

Massey-Omura 암호체계는 Galois 체 $\mathbb{F}_q$ 의 곱셈군 $\mathbb{F}_q^*$ 가 위수 $q-1$ 인 순환군이라는 사실에 근거를 두고 있다(§4.3). 다음 프로토콜은 Galois 체 $\mathbb{F}_q$ 위에서의 타원곡선 E 에 대한 덧셈군 $G(E, \mathbb{F}_q)$ 를 이용한 것이다.

[3] 타원곡선을 이용한 Massey-Omura 암호체계

송신자 U가 수신자 A에게 비밀 전문을 보내려면, 먼저 적당한 Galois 체 $\mathbb{F}_q$를 택하여 $\mathbb{F}_q$를 공개하고 다음 여섯 단계의 절차를 밟는다.

(1) 수신자 A는 적당한 Galois체 $\mathbb{F}_q$와 체 $\mathbb{F}_q$ 위에서의 적당한 타원곡선 E를 정하여 $\mathbb{F}_q$, E와 덧셈군 $G(E, \mathbb{F}_q)$의 위수 N을 공개한다. 그리고,

$$(e_A, N) = 1, \qquad 1 \le e_A < N$$

인 정수 e_A를 택하고

$$e_A d_A \equiv 1 \pmod{N}, \qquad 1 \le d_A < N$$

인 정수 d_A를 구하여 e_A와 d_A는 공개하지 않는다.

(2) 송신자 U는

$$(e_U, N) = 1, \qquad 1 \le e_U < N$$

인 정수 e_U를 택하고

$$e_U d_U \equiv 1 \pmod{N}, \qquad 1 \le d_U < N$$

인 정수 d_U를 구하여 e_U와 d_U는 공개하지 않는다.

(3) 송신자 U는 A에게 보내려는 평문을 $G(E, \mathbb{F}_q)$의 원소 P로 나타내고, e_U를 이용하여 e_UP를 계산하고 이 결과를 A에게 보낸다.

(4) 수신자 A는 수신한 e_UP와 자신의 비밀 열쇠인 e_A를 이용하여

$$\mathrm{Q} = e_A(e_U \mathrm{P})$$

를 구하고 Q를 U에게 보낸다.

(5) 송신자 U는 수신한 Q와 자신의 비밀 열쇠인 d_U를 이용하여

$$\mathrm{R} = d_U \mathrm{Q}$$

를 계산하고 R를 A에게 보낸다.

(6) 수신자 A는 수신한 R와 비밀 열쇠인 d_A를 이용하여

$$d_A \mathrm{R} = d_A e_A \mathrm{P} = \mathrm{P}$$

를 구하고 이로부터 평문 P를 얻는다.

앞의 두 단계 (5), (6) 에서

$$d_U e_U \equiv 1 \pmod{N}, \quad d_A e_A \equiv 1 \pmod{N}$$

이고 또 Lagrange 의 정리에 의하여 $NP = O$ 이다. 따라서

$$(d_U e_U)P = P, \quad (d_A e_A)P = P$$

이고, 또

$$Q = e_A(e_U P)$$

이므로 다음이 성립한다.

$$\begin{aligned} R &= d_U Q = d_U e_A(e_U P) \\ &= e_A(d_U e_U)P = e_A P, \\ d_A R &= d_A e_A P = P \end{aligned}$$

이 프로토콜에서 공격자가 $e_U P$, $e_A P$, $e_A e_U P$ 를 알고 있을 때, 등식

$$\begin{aligned} (e_A e_U)P &= e_A(e_U P), \\ (e_A e_U)P &= e_U(e_A P) \end{aligned}$$

를 이용하여 비밀 열쇠 e_A, e_U 의 값을 얻으려면, 타원곡선에 대한 이산로그 문제를 풀어야 한다.

또, 이 암호체계를 이용하려면 먼저 유한 덧셈군 $G(E, \mathbb{F}_q)$ 의 위수 N 을 결정하여야 하는데, 이 문제는 일반적으로 어렵다.

유한 덧셈군 $G(E, \mathbb{F}_q)$, $G(E_1, \mathbb{F}_{2^m}), G(E_2, \mathbb{F}_{2^m})$ 의 위수를 구하는 일 구하는 일과 이들 덧셈군의 각 원소의 위수를 구하는 일은 대단히 중요하며 수학적으로도 여러 가지 문제와 연관되어 있다. 이러한 유한 덧셈군의 위수를 구하는 알고리즘으로는

Schoof 의 알고리즘,
SEA(Schoof-Elkies-Atkin) 알고리즘,
Satoh 의 알고리즘

등이 이용된다.