

연 습 문 제 (4.1)

1. 체 $\mathbb{Z}_2 = \{0, 1\}$ 위에서 다음을 간단히 하여라.

$$(1) (x^2+x+1) + (x^2+1) \quad (2) (x^3+x+1) + (x^3+x^2+1)$$

$$(3) (x^2+x+1)(x^2+1) \quad (4) (x^3+x+1)(x^3+x^2+1)$$

$$[\text{풀이}] (1) (x^2+x+1) + (x^2+1) = x$$

$$(2) (x^3+x+1) + (x^3+x^2+1) = x^2+x$$

$$(3) (x^2+x+1)(x^2+1) = x^4+x^3+x+1$$

$$(4) (x^3+x+1)(x^3+x^2+1) = x^6+x^5+x^4+x^3+x^2+x+1$$

2. 체 $\mathbb{Z}_2 = \{0, 1\}$ 위에서 다음 두 다항식 $f(x)$, $g(x)$ 의 최대공약수 $d(x)$ 를 구하고, $d(x)$ 를 $d(x) = f(x)s(x) + g(x)t(x)$ 의 꼴로 나타내어라.

$$(1) f(x) = x^4+x^3+x^2+1, \quad g(x) = x^2+1$$

$$(2) f(x) = x^8+x^7+x^6+x^5+1, \quad g(x) = x^6+x^2+1$$

$$(3) f(x) = x^6+x^5+x^4+x^3+x^2+x+1, \quad g(x) = x^4+x^3+x^2+1$$

[풀이] (1) 아래 계산에 의하여

$$f(x) = g(x)(x^2+x) + (x+1),$$

$$g(x) = (x+1)(x+1)$$

이므로 $f(x)$, $g(x)$ 의 최대공약수는 $d(x) = x+1$ 이고 다음이 성립한다.

$$d(x) = x+1 = f(x) + g(x)(x^2+x)$$

$$\begin{array}{r|l}
 \begin{array}{r}
 x^2 \quad x^4+x^3+x^2+1 \\
 +x \quad x^4+x^2 \\
 \hline
 \quad x^3+1 \\
 \quad x^3+x \\
 \hline
 \quad \quad x+1
 \end{array}
 &
 \begin{array}{r}
 x^2+1 \\
 x^2+x \\
 \hline
 x+1 \\
 x+1 \\
 \hline
 0
 \end{array}
 &
 \begin{array}{l}
 x \\
 +1 \\
 \\
 \hline
 \end{array}
 \end{array}$$

(2) 아래 계산에 의하여

$$f(x) = g(x)(x^2+x+1) + x^5+x^4+x^3+x$$

$$g(x) = (x^5+x^4+x^3+x)(x+1) + x^3+x+1$$

$$x^5+x^4+x^3+3 = (x^3+x+1)(x^2+x)$$

이므로 $d(x) = x^3 + x + 1$ 이다.

1	1 1 1 1 0 0 0 0 1	1 0 0 0 1 0 1	1
	1 0 0 0 1 0 1 0 0	1 1 1 0 1 0 0	
1	1 1 1 1 0 1 0 1	1 1 0 0 0 1	1
	1 0 0 0 1 0 1 0	1 1 1 0 1 0	
1	1 1 1 1 1 1 1	1 0 1 1	
	1 0 0 0 1 0 1		
1	1 1 1 0 1 0		
	1 0 1 1 0 0		
1	1 0 1 1 0		
	1 0 1 1 0		
	0		

그리고,

$$d(x) = x^3+x+1 = (x^5+x^4+x^3+x)(x+1) + g(x)$$

$$x^5+x^4+x^3+x = f(x) + g(x)(x^2+x+1)$$

이므로 다음이 성립한다.

$$\begin{aligned}
 d(x) &= \{f(x) + g(x)(x^2+x+1)\}(x+1) + g(x) \\
 &= f(x)(x+1) + g(x)\{(x^2+x+1)(x+1) + 1\} \\
 &= f(x)(x+1) + g(x)x^3
 \end{aligned}$$

3. 체 $\mathbb{Z}_2 = \{0, 1\}$ 위에서 다음 다항식은 모두 기약이 아님을 확인하여라.

$$x^3, \quad x^3+x^2, \quad x^3+x, \quad x^3+1, \quad x^3+x^2+x, \quad x^3+x^2+x+1$$

[풀이] 정리 4.1.6을 이용하여 이들 다항식이 \mathbb{Z}_2 위에서 기약이 아님을 밝힌다.

실제로, 이들 다항식은 체 \mathbb{Z}_2 위에서 다음과 같이 인수분해된다.

$$\begin{aligned} x^3 &= xxx = x^2x, & x^3+x^2 &= x^2(x+1), \\ x^3+x &= x(x^2+1), & x^3+1 &= (x+1)(x^2+x+1), \\ x^3+x^2+x &= x(x^2+x+1), & x^3+x^2+x+1 &= (x+1)^3 \end{aligned}$$

4. 체 $\mathbb{Z}_3 = \{0, 1, 2\}$ 위에서 다음 세 다항식이 기약다항식임을 밝혀라.

$$f(x) = x^2 + 1, \quad p(x) = x^2 + x + 2, \quad q(x) = x^2 + 2x + 2$$

[풀이] 정리 4.1.6을 이용하여 증명한다.

$$\begin{aligned} (1) \quad f(0) &= 0^2 + 1 = 1 \neq 0, \\ f(1) &= 1^2 + 1 = 2 \neq 0, \\ f(2) &= 2^2 + 1 = 1 + 1 \neq 0 \end{aligned}$$

이므로 $f(x)$ 는 체 \mathbb{Z}_3 위에서 기약이다.

$$\begin{aligned} (2) \quad p(0) &= 0^2 + 0 + 2 = 2 \neq 0, \\ p(1) &= 1^2 + 1 + 2 = 1 \neq 0, \\ p(2) &= 2^2 + 2 + 2 = 1 + 2 + 2 = 2 \neq 0 \end{aligned}$$

이므로 $p(x)$ 는 체 \mathbb{Z}_3 위에서 기약이다.

$$\begin{aligned} (3) \quad q(0) &= 0^2 + 2 \cdot 0 + 2 = 2 \neq 0, \\ q(1) &= 1^2 + 2 \cdot 1 + 2 = 1 + 2 + 2 = 2 \neq 0, \\ q(2) &= 2^2 + 2 \cdot 2 + 2 = 1 + 2 + 2 = 2 \neq 0 \end{aligned}$$

이므로 $q(x)$ 는 체 \mathbb{Z}_3 위에서 기약이다.

연 습 문 제 (4.2)

2. 체 $\mathbb{F}_2 = \{0, 1\}$ 위에서 $q(x) = x^3 + x^2 + 1$ 는 기약다항식이다.

이제 $q(\beta) = 0$ 인 원소 β 를 도입하여 Galois 체 \mathbb{F}_8 을 만들고, 또 β 는 체 \mathbb{F}_8 의 원시원소이고 $q(x)$ 는 체 \mathbb{F}_2 위의 3 차의 원시다항식임을 밝혀라.

$$\begin{aligned} [\text{풀이}] \quad \mathbb{F}_{2^3} &= \{a_0 + a_1\beta + a_2\beta^2 \mid a_0, a_1, a_2 \in \mathbb{F}_2\} \\ &= \{0, 1, \beta, 1 + \beta, \beta^2, 1 + \beta^2, \beta + \beta^2, 1 + \beta + \beta^2\} \end{aligned}$$

$$q(\beta) = \beta^3 + \beta^2 + 1 = 0 \quad \text{즉} \quad \beta^3 = 1 + \beta^2$$

$$\beta^4 = \beta(1 + \beta^2) = \beta + \beta^3 = \beta + 1 + \beta^2 = 1 + \beta + \beta^2$$

$$\beta^5 = \beta(1 + \beta + \beta^2) = \beta + \beta^2 + \beta^3 = \beta + \beta^2 + 1 + \beta^2 = 1 + \beta$$

$$\beta^6 = \beta\beta^5 = \beta(1 + \beta) = \beta + \beta^2$$

$$\beta^7 = \beta^2 + \beta^3 = -1 = 1$$

따라서

$$\mathbb{F}_{2^3}^* = \langle \beta \rangle = \{1, \beta, \beta^2, \dots, \beta^6\}, \quad \beta^7 = 1$$

이므로 β 는 체 \mathbb{F}_8 의 원시원소이고 $q(x)$ 는 체 \mathbb{F}_2 위의 3 차의 원시다항식이다.

3. 체 \mathbb{F}_2 위의 다항식 $p(x) = x^5 + x^2 + 1$ 는 5 차의 원시다항식이다.

이제 $p(a) = 0$ 인 원소 a 를 도입하여 Galois 체 \mathbb{F}_{2^5} 를 만들고

$$\mathbb{F}_{2^5}^* = \langle a \rangle = \{1, a, a^2, \dots, a^{30}\}, \quad a^{31} = 1$$

임을 밝혀라. 또, 다음을 $a_0 + a_1a + a_2a^2 + a_3a^3 + a_4a^4$ 의 꼴로 나타내어라.

$$(1) (1 + a + a^4)(1 + a^2 + a^3) \quad (2) (1 + a + a^4)^{-1}$$

[풀이] $\mathbb{F}_{2^5} = \{a_0 + a_1a + a_2a^2 + a_3a^3 + a_4a^4 \mid a_0, a_1, a_2, a_3, a_4 \in \mathbb{F}_2\}$

$$a^5 + a^2 + 1 = 0 \quad \Leftrightarrow \quad a^5 = 1 + a^2$$

$a^1 = a,$	$a^{17} = 1 + a + a^4,$
$a^2 = a^2,$	$a^{18} = 1 + a,$
$a^3 = a^3,$	$a^{19} = a + a^2,$
$a^4 = a^4,$	$a^{20} = a^2 + a^3,$
$a^5 = 1 + a^2,$	$a^{21} = a^3 + a^4,$
$a^6 = a + a^3,$	$a^{22} = 1 + a^2 + a^4,$
$a^7 = a^2 + a^4,$	$a^{23} = 1 + a + a^2 + a^3,$
$a^8 = 1 + a^2 + a^3,$	$a^{24} = a + a^2 + a^3 + a^4,$
$a^9 = a + a^3 + a^4,$	$a^{25} = 1 + a^3 + a^4,$
$a^{10} = 1 + a^4,$	$a^{26} = 1 + a + a^2 + a^4,$
$a^{11} = 1 + a + a^2,$	$a^{27} = 1 + a + a^3,$
$a^{12} = a + a^2 + a^3,$	$a^{28} = a + a^2 + a^4,$
$a^{13} = a^2 + a^3 + a^4,$	$a^{29} = 1 + a^3,$
$a^{14} = 1 + a^2 + a^3 + a^4,$	$a^{30} = a + a^4,$
$a^{15} = 1 + a + a^2 + a^3 + a^4,$	$a^{31} = 1$
$a^{16} = 1 + a + a^3 + a^4,$	

따라서 다음이 성립한다.

$$\mathbb{F}_{2^5}^* = \langle a \rangle = \{1, a, a^2, \dots, a^{30}\}, \quad a^{31} = 1$$

(1) 위의 표를 이용하여 다음 결과를 얻는다.

$$(1 + \alpha + \alpha^4)(1 + \alpha^2 + \alpha^3) = \alpha^{17} \alpha^8 = \alpha^{25} = 1 + \alpha^3 + \alpha^4$$

또한, $\alpha^5 = 1 + \alpha^2$, $\alpha^6 = \alpha + \alpha^3$, $\alpha^7 = \alpha^2 + \alpha^4$ 임을 이용하여 다음 결과를 얻을 수도 있다.

$$\begin{aligned} & (1 + \alpha + \alpha^4)(1 + \alpha^2 + \alpha^3) \\ &= 1 + \alpha^2 + \alpha^3 + \alpha + \alpha^3 + \alpha^4 + \alpha^4 + \alpha^6 + \alpha^7 \\ &= 1 + \alpha + \alpha^2 + \alpha^6 + \alpha^7 \\ &= 1 + \alpha + \alpha^2 + \alpha + \alpha^3 + \alpha^2 + \alpha^4 \\ &= 1 + \alpha^3 + \alpha^4 \end{aligned}$$

(2) $\xi = 1 + \alpha + \alpha^4$ 이라고 할 때, 앞의 표에 의하여 $\xi = \alpha^{17}$ 이므로 ξ^{-1} 는 다음과 같다.

$$\xi^{-1} = \alpha^{-17} = \alpha^{14} = 1 + \alpha^2 + \alpha^3 + \alpha^4$$

또한, ξ^{-1} 는 표를 이용하지 않고 다음과 같이 구할 수 있다.

먼저 $g(x) = x^4 + x + 1$ 이라고 하면, $g(\alpha) = \alpha^4 + \alpha + 1 = \xi$ 이고, 또 $g(x)$ 와 $p(x) = x^5 + x^2 + 1$ 는 서로 소이고 다음이 성립한다.

$$\begin{aligned} p(x) &= g(x)x + (x+1), \\ g(x) &= (x+1)(x^3 + x^2 + x) + 1 \\ x+1 &= 1(x+1) \end{aligned}$$

x	$x^5 + x^2 + 1$	$x^4 + x + 1$	x^3
	$x^5 + x^2 + x$	$x^4 + x^3$	
$x+1$	$x+1$	$x^3 + x + 1$	$+x^2$
	$x+1$	$x^3 + x^2$	
	0	$x^2 + x + 1$	$+x$
		$x^2 + x$	
		1	

따라서

$$\begin{aligned} 1 &= (x+1)(x^3+x^2+x) + g(x) \\ x+1 &= p(x) + g(x)x \end{aligned}$$

이므로 다음이 성립한다.

$$\begin{aligned} 1 &= \{p(x) + g(x)x\}(x^3+x^2+x) + g(x) \\ &= p(x)(x^3+x^2+x) + g(x)(x^4+x^3+x^2+1) \end{aligned}$$

따라서

$$\begin{aligned} 1 &= p(a)(a^3+a^2+a) + g(a)(a^4+a^3+a^2+1) \\ &= g(a)(a^4+a^3+a^2+1) \end{aligned}$$

이므로 $\xi^{-1} = 1+a^2+a^3+a^4$ 이다.

4. 체 \mathbb{F}_2 위의 다항식 $r(x) = x^4 + x^3 + x^2 + x + 1$ 는 4 차의 기약다항식이지만 원시다항식은 아니다(보기 4.2.6). 이제 $r(\beta) = 0$ 인 원소 β 를 도입하여 Galois 체 \mathbb{F}_{2^4} 를 만들고 또 다음이 성립함을 확인하여라.

$$\langle \beta \rangle = \{1, \beta, \beta^2, \beta^3, \beta^4\}, \quad \mathbb{F}_{2^3}^* \neq \langle \beta \rangle$$

$$[\text{풀이}] \quad \mathbb{F}_{2^3} = \{a_0 + a_1\beta + a_2\beta^2 + a_3\beta^3 \mid a_0, a_1, a_2, a_3 \in \mathbb{F}_2\}$$

$$r(\beta) = \beta^4 + \beta^3 + \beta^2 + 1 = 0 \quad \text{즉} \quad \beta^4 = 1 + \beta + \beta^2 + \beta^3$$

$$\beta^4 = 1 + \beta + \beta^2 + \beta^3$$

$$\begin{aligned} \beta^5 &= \beta(1 + \beta + \beta^2 + \beta^3) \\ &= \beta + \beta^2 + \beta^3 + \beta^4 = -1 = 1 \end{aligned}$$

따라서

$$\langle \beta \rangle = \{1, \beta, \beta^2, \beta^3, \beta^4\}, \quad \beta^5 = 1$$

이고 $\mathbb{F}_{2^3}^* \neq \langle \beta \rangle$ 이다.

5. 보기 4.2.4 에서 논한 Galois 체 \mathbb{F}_{2^3} 에 대하여, 원시원소 α 를 밑으로 가지는 이산로그표를 만들어라.

[풀이]

$$\begin{aligned}\alpha^1 &= \alpha, \\ \alpha^2 &= \alpha^2, \\ \alpha^3 &= 1 + \alpha \\ \alpha^4 &= \alpha + \alpha^2, \\ \alpha^5 &= 1 + \alpha + \alpha^2, \\ \alpha^6 &= 1 + \alpha^2 \\ \alpha^7 &= 1 = \alpha^0\end{aligned}$$

따라서 \mathbb{F}_{2^3} 의 α 를 밑으로 가지는 이산로그표는 다음과 같다.

ξ	1	α	$1+\alpha$	α^2	$1+\alpha^2$	$\alpha+\alpha^2$	$1+\alpha+\alpha^2$
$\text{ind}_\alpha \xi$	0	1	3	2	6	4	5

6. 체 $\mathbb{F}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ 에서 $g = 2$ 가 \mathbb{F}_{11} 의 원시원소임을 밝히고 또 g 를 밑으로 가지는 이산로그표를 만들어라.

[풀이] 체 \mathbb{F}_{11} 에서 $g = 2$ 일 때 다음이 성립한다.

$$\begin{aligned}g &= 2, & g^2 &= 4, & g^3 &= 8, & g^4 &= 5, & g^5 &= 10, \\ g^6 &= 9, & g^7 &= 7, & g^8 &= 3, & g^9 &= 6, & g^{10} &= 1 = g^0\end{aligned}$$

따라서 $g = 2$ 는 체 \mathbb{F}_{11} 의 원시원소이다.

그리고 g 를 밑으로 가지는 이산로그표는 다음과 같다.

a	1	2	3	4	5	6	7	8	9	10
$\text{ind}_g a$	0	1	8	2	4	9	7	3	6	5

7. 체 $\mathbb{F}_3 = \{0, 1, 2\}$ 위에서 $p(x) = x^2 + x + 2$ 는 기약다항식임을 밝혀라.

그리고, $p(\alpha) = 0$ 인 원소 α 를 도입하여 얻은 Galois 체 \mathbb{F}_{3^2} 에서 α 는 원시원소이고 $p(x)$ 는 체 \mathbb{F}_3 위의 2 차의 원시다항식임을 밝혀라.

[풀이] 체 \mathbb{F}_3 위에서

$$p(0) = 0^2 + 0 + 2 = 2 \neq 0,$$

$$p(1) = 1^2 + 1 + 2 = 1 \neq 0,$$

$$p(2) = 2^2 + 2 + 2 = 2 \neq 0$$

이므로 $p(x)$ 는 기약다항식이다(정리 4.1.16). 그리고,

Galois 체 \mathbb{F}_{3^2} 에서 다음이 성립한다.

$$\mathbb{F}_{3^2} = \{a_0 + a_1\alpha \mid a_0, a_1 \in \mathbb{F}_3\}$$

$$p(\alpha) = \alpha^2 + \alpha + 2 = 0 \quad \text{즉} \quad \alpha^2 = -2 - \alpha = 1 + 2\alpha$$

$$\alpha^3 = \alpha + 2\alpha^2 = \alpha + 2(1 + 2\alpha) = \alpha + 2 + \alpha = 2 + 2\alpha$$

$$\alpha^4 = 2\alpha + 2\alpha^2 = 2\alpha + 2(1 + 2\alpha) = 2\alpha + 2 + \alpha = 2$$

$$\alpha^5 = 2\alpha,$$

$$\alpha^6 = 2\alpha^2 = 2(1 + 2\alpha) = 2 + \alpha,$$

$$\alpha^7 = 2\alpha + \alpha^2 = 2\alpha + 1 + 2\alpha = 1 + \alpha$$

$$\alpha^8 = \alpha + \alpha^2 = -2 = 1$$

그러므로

$$\mathbb{F}_{3^2}^* = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7\} = \langle \alpha \rangle, \quad \alpha^8 = 1$$

이고, α 는 Galois 체 $\mathbb{F}_{3^2}^*$ 의 원시원소이고 따라서 $p(x)$ 는 체 \mathbb{F}_3 위의 2 차의 원시다항식이다.

8. 체 $\mathbb{F}_3 = \{0, 1, 2\}$ 위에서 $p(x) = x^3 + 2x^2 + x + 1$ 는 기약다항식임을 밝혀라. 그리고, $p(\alpha) = 0$ 인 원소 α 를 도입하여 얻은 Galois 체 \mathbb{F}_{3^3} 에서 $(\alpha^2 + 1)(\alpha^2 + 2\alpha + 1)$ 를 구하여라.

[풀이] 체 \mathbb{F}_3 위에서

$$\begin{aligned} p(0) &= 0^3 + 2 \cdot 0^2 + 1 \cdot 0 + 1 = 1 \neq 0 \\ p(1) &= 1^3 + 2 \cdot 1^2 + 1 \cdot 1 + 1 = 2 \neq 0 \\ p(2) &= 2^3 + 2 \cdot 2^2 + 1 \cdot 2 + 1 \\ &= 2 + 2 + 2 + 1 = 1 \neq 0 \end{aligned}$$

이므로 $p(x)$ 는 기약다항식이다.

그리고,

$$\alpha^3 + 2\alpha^2 + \alpha + 1 = 0 \quad \text{즉} \quad \alpha^3 = -1 - \alpha - 2\alpha^2$$

이므로

$$\alpha^3 = 2 + 2\alpha + \alpha^2, \quad \alpha^4 = 2\alpha + 2\alpha^2 + \alpha^3 = 2 + \alpha$$

이고 따라서 다음 결과를 얻는다.

$$\begin{aligned} (\alpha^2 + 1)(\alpha^2 + 2\alpha + 1) &= \alpha^4 + 2\alpha^3 + \alpha^2 + \alpha^2 + 2\alpha + 1 \\ &= \alpha^4 + 2\alpha^3 + 2\alpha^2 + 2\alpha + 1 \\ &= 2 + \alpha + 1 + \alpha + 2\alpha^2 + 2\alpha^2 + 2\alpha + 1 \\ &= 2 + 1 + 1 + \alpha + \alpha + 2\alpha + 2\alpha^2 + 2\alpha^2 \\ &= 1 + \alpha + \alpha^2 \end{aligned}$$

연 습 문 제 (4.3)

1. 체 $\mathbb{F}_{37} = \{0, 1, 2, \dots, 36\}$ 에서 $g = 2$ 는 원시원소이고 다음 표는 g 를 밑으로 가지는 이산로그표이다.

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$\text{ind}_2 a$	0	1	26	2	23	27	32	3	16	24	30	28	11	33	13	4	7

a	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
$\text{ind}_2 a$	17	35	25	22	31	15	29	10	12	6	34	21	14	9	5	20	8	19	18

위의 표를 이용하여 체 \mathbb{F}_{37} 의 원소 $\xi = 29$ 와 정수 $e_A = 5$, $e_U = 7$ 에 대하여 다음 물음에 답하여라(정리 3.1.5 참조).

- (1) $e_A d_A \equiv 1 \pmod{36}$, $1 \leq d_A < 36$ 인 d_A 를 구하여라.
- (2) $e_U d_U \equiv 1 \pmod{36}$, $1 \leq d_U < 36$ 인 d_U 를 구하여라.
- (3) 체 \mathbb{F}_{37} 의 원소 ξ^{e_U} , $(\xi^{e_U})^{e_A}$, $(\xi^{e_U e_A})^{d_U}$ 를 구하여라.
- (4) 체 \mathbb{F}_{37} 의 원소 $((\xi^{e_U e_A})^{d_U})^{d_A}$ 와 ξ 를 비교하여라.

[풀이] (1) 오른쪽 표에 의하여

$$(36, 5) = 1,$$

$$36 \cdot 1 + 5 \cdot (-7) = 1$$

이므로 다음이 성립한다.

$$5 \cdot (-7) \equiv 1 \pmod{36}$$

$$5 \cdot 29 \equiv 1 \pmod{36}$$

따라서 $d_A = 29$ 이다.

$$\begin{array}{c|cc|c} 7 & 36 & 5 & 5 \\ & 35 & 5 & \\ \hline & 1 & 0 & \end{array}$$

7
1 0 1
0 1 -7

(2) 오른쪽 표에 의하여

$$(36, 7) = 1,$$

$$36 \cdot 1 + 7 \cdot (-5) = 1$$

이므로 다음이 성립한다.

$$7 \cdot (-5) \equiv 1 \pmod{36}$$

$$5 \cdot 31 \equiv 1 \pmod{36}$$

따라서 $d_U = 31$ 이다.

(3) 이산로그표에 의하여 $\text{ind}_2 \xi = \text{ind}_2 29 = 21$ 이므로

$$\text{ind}_2 \xi^{e_U} \equiv e_U \text{ind}_2 \xi \equiv 7 \cdot 21 \equiv 3 \pmod{36},$$

$$\text{ind}_2 (\xi^{e_U})^{e_A} \equiv e_A \text{ind}_2 \xi^{e_U} \equiv 5 \cdot 3 \equiv 15 \pmod{36},$$

$$\text{ind}_2 (\xi^{e_U e_A})^{d_U} \equiv d_U \text{ind}_2 \xi^{e_U e_A} \equiv 31 \cdot 15 \equiv 33 \pmod{36}$$

이고 따라서 이산로그표에 의하여 다음 결과를 얻는다.

$$\xi^{e_U} = 8 \quad (\xi^{e_U})^{e_A} = 23, \quad (\xi^{e_U e_A})^{d_U} = 14$$

(4) $(\xi^{e_U e_A})^{d_U} = 14$, $d_A = 29$ 이므로 위의 (3) 과 (1) 에 의하여

$$\begin{aligned} \text{ind}_2 ((\xi^{e_U e_A})^{d_U})^{d_A} &\equiv d_A \text{ind}_2 ((\xi^{e_U e_A})^{d_U}) \\ &\equiv 29 \cdot 33 \equiv 21 \pmod{36} \end{aligned}$$

이고 따라서 $((\xi^{e_U e_A})^{d_U})^{d_A} = \xi$ 이다.

2. 체 $\mathbb{F}_2 = \{0, 1\}$ 위의 6 차의 원시다항식 $p(x) = x^6 + x + 1$ 에 대하여

Galois 체 \mathbb{F}_{2^6} 의 원소 α 가 $p(\alpha) = 0$ 인 원시원소일 때 다음이 성립한다.

$$\alpha^6 + \alpha + 1 = 0 \quad \text{즉} \quad \alpha^6 = 1 + \alpha$$

이 결과를 이용하여 다음 원소를

$$a_0 + a_1 \alpha + a_2 \alpha^2 + a_3 \alpha^3 + a_4 \alpha^4 + a_5 \alpha^5 \quad (a_0, \dots, a_5 \in \mathbb{F}_2)$$

의 꼴로 나타내어라.

$$(1) \alpha^6, \alpha^7, \alpha^8, \dots, \alpha^{12}$$

$$(2) \alpha^{-1}, \alpha^{-2}$$

$$5 \left| \begin{array}{cc|c} 36 & 7 & 7 \\ 35 & 7 & \\ \hline 1 & 0 & \end{array} \right|$$

5
1 0 1
0 1 -5

[풀이] (1) $\alpha^6 = 1 + \alpha$,

$$\alpha^7 = \alpha + \alpha^2,$$

$$\alpha^8 = \alpha^2 + \alpha^3,$$

$$\alpha^9 = \alpha^3 + \alpha^4,$$

$$\alpha^{10} = \alpha^4 + \alpha^5,$$

$$\alpha^{11} = \alpha^5 + \alpha^6 = 1 + \alpha + \alpha^5,$$

$$\alpha^{12} = \alpha + \alpha^2 + \alpha^6 = 1 + \alpha^2$$

(2) $\alpha^6 = 1 + \alpha$ 이므로

$$\alpha + \alpha^6 = 1 \quad \text{즉} \quad \alpha(1 + \alpha^5) = 1$$

이므로 $\alpha^{-1} = 1 + \alpha^5$ 이다.

그리고, 이 결과와 (1) 에 의하여 다음 결과를 얻는다.

$$\begin{aligned} \alpha^{-2} &= (\alpha^{-1})^2 = (1 + \alpha^5)^2 \\ &= 1 + \alpha^{10} = 1 + \alpha^4 + \alpha^5 \end{aligned}$$

연 습 문 제 (4.4)

1. 실수체 \mathbb{R} 위에서 타원곡선 $y^2 = x^3 - x^2 - 4x + 8$ 위의 세 점

$$P = (1, 2), \quad Q = (-2, 2), \quad R = (2, 2)$$

에 대하여 $P + Q = (2, -2)$, $2R = (-2, 2) = Q$ 임을 밝혀라.

[풀이] 정리 4.4.1 을 이용하여 구한다.

(1) $P = (1, 2)$, $Q = (-2, 2)$ 에 대하여

$$k = \frac{y_2 - y_1}{x_2 - x_1} = \frac{2 - 2}{-2 - 1} = 0,$$

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

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

이므로 $P + Q = (2, -2)$ 이다.

(2) $R = (2, 2)$ 에 대하여

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

$$x_3 = k^2 - a - 2x_1 = 1^2 + 1 - 2 \cdot 2 = -2,$$

$$y_3 = k(x_1 - x_3) - y_1 = (2 + 2) - 2 = 2$$

이므로 $2R = (-2, 2) = Q$ 이다.

4. Galois 체 $\mathbb{F}_{11} = \{0, 1, \dots, 9, 10\}$ 위에서의 타원곡선

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

에 대하여 다음이 성립함을 확인하여라.

$$(1) \quad G(E, \mathbb{F}_{11}) = \{(2, 4), (2, 7), (3, 5), (3, 6), (5, 2), (5, 9), \\ (7, 2), (7, 9), (8, 3), (8, 8), (10, 2), (10, 9), O\}$$

$$(2) \quad P = (2, 4) \text{ 일 때, } 2P = (5, 9), 3P = (8, 8), 6P = (7, 2) \text{ 이다.}$$

[풀이] (2) 정리 4.4.1 을 이용하여 증명한다.

먼저 $P = (2, 4) = (x_1, y_1)$ 일 때 $2P = (x_3, y_3)$ 이라고 하면

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

이고, 또 체 \mathbb{F}_{11} 에서 $8 \cdot 7 = 1$ 즉 $8^{-1} = 7$ 이므로 다음이 성립한다.

$$k = 2 \cdot 8^{-1} = 2 \cdot 7 = 3,$$

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

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

따라서 $2P = (5, 9)$ 이다.

다음에 $P = (2, 4) = (x_1, y_1)$, $2P = (5, 9) = (x_2, y_2)$ 이라 하고

$3P = P + 2P = (x_3, y_3)$ 이라고 하면,

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

이고 또 체 \mathbb{F}_{11} 에서 $3 \cdot 4 = 1$ 즉 $3^{-1} = 4$ 이므로 다음이 성립한다.

$$k = \frac{5}{3} = 5 \cdot 4 = 9,$$

$$x_3 = k^2 - a - (x_1 + x_2) = 9^2 - 7 = 4 - 7 = -3 = 8,$$

$$y_3 = k(x_1 - x_3) - y_1 = 9(2 - 8) - 4 = 1 - 4 = -3 = 8$$

따라서 $3P = (8, 8)$ 이다.

끝으로,

$$3P = (8, 8) = (x_1, y_1), \quad 6P = 3P + 3P = (x_3, y_3)$$

이라고 하면 다음이 성립한다.

$$k = \frac{3x + b}{2y_1} = \frac{3 \cdot 8^2 + 1}{2 \cdot 8} = \frac{-5}{5} = -5 \cdot 5^{-1} = -1,$$

$$x_3 = k^2 - a - 2x_1 = 1 - 2 \cdot 8 = 1 + 6 = 7,$$

$$\begin{aligned} y_3 &= k(x_1 - x_3) - y_1 = (-1) \cdot (8 - 7) - 8 \\ &= -1 - 8 = -9 = 2 \end{aligned}$$

따라서 $6P = (7, 2)$ 이다.

5. 보기 4.4.4 에 대하여 다음 물음에 답하여라.

- (1) $(\alpha^5, \alpha^3), (\alpha^5, \alpha^{11}), (\alpha^6, \alpha^8), (\alpha^6, \alpha^{14})$ 은 모두 $G(E_1, \mathbb{F}_{2^4})$ 에 속함을 확인하여라.
- (2) $P = (\alpha^5, \alpha^{11})$ 일 때, $2P, 3P, 4P$ 를 구하여라.

[풀이] 보기 4.4.4 에 의하여 다음이 성립한다.

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

- (1) Galois \mathbb{F}_{2^4} 위에서 다음과 같은 타원곡선을 생각해 보자.

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

점 $P = (x_1, y_1)$ 가 이 타원곡선 위의 점일 때, 점 $(x_1, y_1 + x_1)$ 도 이 타원곡선 위의 점이므로 다음이 성립한다.

$x = \alpha^5$ 인 경우에

$$y^2 + \alpha^5 y = \alpha^{15} + \alpha^{14} + 1 = 1 + \alpha^{14} + 1 = \alpha^{14}$$

이므로 $y(y + \alpha^5) = \alpha^{14}$ 이고 또

$$\alpha^3(\alpha^3 + \alpha^5) = \alpha^3 \alpha^{11} = \alpha^{14}$$

이고, 따라서 $y = \alpha^3, y = \alpha^3 + \alpha^5 = \alpha^{11}$ 이다.

그러므로 $(\alpha^5, \alpha^3), (\alpha^5, \alpha^{11})$ 는 $G(E_1, \mathbb{F}_{2^4})$ 에 속한다.

마찬가지 방법으로 $(\alpha^6, \alpha^8), (\alpha^6, \alpha^{14})$ 가 모두 $G(E_1, \mathbb{F}_{2^4})$ 에 속한다는 것을 밝힐 수 있다.

(2) 먼저 $P = (a^5, a^{11}) = (x_1, y_1)$, $2P = (x_3, y_3)$ 이라고 하면,

$$\begin{aligned} x_3 &= x_1^2 + \frac{c}{x_1^2} = a^{10} + \frac{1}{a^{10}} \\ &= a^{10} + a^{-10} = a^{10} + a^5 = 1, \end{aligned}$$

$$\begin{aligned} y_3 &= x_1^2 + \left(x_1 + \frac{y_1}{x_1}\right)x_3 + x_3 \\ &= a^{10} + \left(a^5 + \frac{a^{11}}{a^5}\right) \cdot 1 + 1 \\ &= a^{10} + a^5 + a^6 + 1 = 1 + a^2 + a^3 = a^{13} \end{aligned}$$

이므로 $2P = (1, a^{13})$ 이다.

다음에 $P = (a^5, a^{11}) = (x_1, y_1)$, $2P = (1, a^{13}) = (x_2, y_2)$ 이라 하고

$3P = P + 2P = (x_3, y_3)$ 이라고 하면 다음이 성립한다.

$$k = \frac{y_1 + y_2}{x_1 + x_2} = \frac{a^{11} + a^{13}}{a^5 + 1} = \frac{1 + a}{1 + a + a^2} = \frac{a^4}{a^{10}} = a^{-6} = a^9,$$

$$\begin{aligned} x_3 &= k^2 + k + a^4 + (x_1 + x_2) = a^{18} + a^9 + a^4 + a^5 + 1 \\ &= a^3 + a^9 + a^4 + a^5 + 1 = a + a^2 = a^5 \end{aligned}$$

$$\begin{aligned} y_3 &= k(x_1 + x_3) + y_1 + x_3 = a^9(a^5 + a^5) + a^{11} + a^5 \\ &= a^{11} + a^5 = a^3 \end{aligned}$$

따라서 $3P = (a^5, a^3)$ 이다.

끝으로,

$$2P = (1, a^{13}) = (x_1, y_1), \quad 4P = 2P + 2P = (x_3, y_3)$$

이라고 하면 다음이 성립한다.

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

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

따라서 $4P = (0, 1)$ 이다,

6. 체 F 에 대하여 $G = \{(x, y) \in F^2 \mid x^2 + y^2 = 1\}$ 이라고 할 때, 다음 물음에 답하여라.

(1) $F = \mathbb{F}_5 = \{0, 1, 2, 3, 4\}$ 일 때, G 를 결정하여라.

(2) 체 F 의 표수가 2 일 때, $G = \{(x, x+1) \mid x \in F\}$ 임을 밝혀라.

[풀이] (1) 체 \mathbb{F}_5 에서

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

이므로 $x^2 + y^2 = 1$ 일 때 다음이 성립한다.

$x = 0$ 인 경우에 $y^2 = 1$ 이므로 $y = 1$ 또는 $y = 4$ 이다.

$x = \pm 1$ 인 경우에 $1 + y^2 = 1$ 즉 $y^2 = 0$ 이므로 $y = 0$ 이다.

$x = \pm 2$ 인 경우에 $y^2 = 2$ 이고 이러한 y 는 존재하지 않는다.

따라서 $G = \{(0, 1), (0, 4), (1, 0), (4, 0)\}$ 이다.

(2) 체 F 의 표수가 2 일 때, 다음이 성립한다.

$$x^2 + y^2 = 1 \Leftrightarrow (x + y)^2 = 1$$

$$\Leftrightarrow x + y = 1$$

$$\Leftrightarrow y = -x + 1$$

$$\Leftrightarrow y = x + 1$$

따라서 $G = \{(x, x+1) \mid x \in F\}$ 이다.

연 습 문 제 (4.5)

1. 사용자 A 가 체 $\mathbb{F}_{11} = \{0, 1, 2, \dots, 9, 10\}$ 에서의 타원곡선

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

에 대하여 덧셈군 $G(E, \mathbb{F}_{11})$ 의 위수 13 을 공개하고 또 사용자 A 와 U 가 각각

$$e_A = 3, \quad e_U = 5$$

를 택할 때 다음이 성립함을 확인하여라.

- (1) 두 정수 d_A, d_U 를 각각

$$\begin{aligned} e_A d_A &\equiv 1 \pmod{13}, & 1 \leq d_A \leq 12, \\ e_U d_U &\equiv 1 \pmod{13}, & 1 \leq d_U \leq 12 \end{aligned}$$

인 정수라고 할 때, $d_A = 9, d_U = 8$ 이다.

- (2) $P = (2, 4)$ 일 때, $e_U P = (3, 5)$ 이고 또 $Q = e_A(e_U P)$ 이라고 하면 $Q = (5, 9)$ 이다.

- (3) $Q = (5, 9)$ 일 때, $R = d_U Q$ 이라고 하면 $R = (8, 8)$ 이다.

- (4) $R = (8, 8)$ 일 때, $d_A R = (2, 4)$ 이다.

[풀이] (1) 먼저 $e_A = 3$ 일 때,

$$13 \cdot 1 + 3 \cdot (-4) = 1$$

이므로

$$3 \cdot (-4) \equiv 1 \pmod{13} \quad \text{즉} \quad 3 \cdot 9 \equiv 1 \pmod{13}$$

이므로 $d_A = 9$ 이다. 그리고 $e_U = 5$ 일 때

$$13 \cdot 2 + 5 \cdot (-5) = 1$$

이므로

$$5 \cdot (-5) \equiv 1 \pmod{13} \quad \text{즉} \quad 5 \cdot 8 \equiv 1 \pmod{13}$$

이므로 $d_U = 8$ 이다.

(2) $P = (2, 4)$ 일 때, 문제 4.4.4 에 의하여

$$2P = (5, 9), \quad 3P = (8, 8)$$

이고 이 사실과 정리 4.4.1 을 이용하여

$$e_U P = 5(2, 4) = 2P + 3P = (3, 5)$$

임을 밝힌다.

마찬가지로, $2(3, 5)$, $3(3, 5)$ 를 계산하여

$$Q = e_A(e_U P) = 3(3, 5) = (5, 9)$$

임을 밝힌다.