유한체와 DLP

이 인 석
isll@snu.ac.kr

2010년 6월 16일

진짜 제목

“네가 유한체를 아느냐?”

- (1948) $q = 2$; Hamming Code
- $q = 3, 5, 4, 7, 9, 11, \ldots$
- $q = 8$ (수십 쪽); *“사람의 솜씨가 아니다!”*
- (1959) $q = p^n$ (2쪽); 소수 p, 자연수 n

“네가 유한체를 아느냐?”

= 네가 (학부)대수학을 배웠느냐?

- 수학과 전공 필수 교과목 한 학기 강의 내용
- 80분에……

- 최소의 사전 지식
  - 나눗셈 (정수, 다항식, 분할, quotient)
  - 벡터공간, basis (기저), dimension (차원)
  - 추상적인 생각보다는 typical example 이해하려는 자세
- 오늘의 주제는 나눗셈 !

차례

- 정수의 잉여류
- Group
- Ring, Field, Vector Space
- 다항식의 잉여류 (유한체)
- Discrete Logarithm Problem (DLP)
- Characteristic p의 별세계
- 유한체 vs. 무한체
- 유한체의 유일성

정수의 잉여류

- 정수의 잉여류와 잉여산
- Euclidean Algorithm
- $(\mathbb{Z}_n)^\times$와 Euler Phi Function

정수의 잉여류(Residue Class)

- 자연수 a 를 5 로 나눈 나머지가 3 일 때, (a^2+7a-8) 을 5 로 나눈 나머지는?
  - (훈련 받은 대로) $a = 5k+3$ 으로 놓고……
  - 누가 가르쳐주지 않아도
  - $3^2+7 \times 3-8 = 22$, 답; 2
  - $3^2+2 \times 3+2 = 17$, 답; 2

- 나머지들이 사는 세상이 있고
- 나머지들 간의 연산(잉여산)이 가능

정수의 잉여류들의 세계 $\mathbb{Z}_n$

- n 으로(n > 1) 나눈 '나머지들의 세계' = $\mathbb{Z}_n$
  - "Z sub n"
- $\mathbb{Z}_5$ 에 사는 것(원소)들
  - [나머지 3] = [나머지 8] = [나머지 −2] = …
  - 표기법; [나머지 3] = 3(mod 5)
  - 3(mod 5)의 이름은 잉여류(residue class)
  - 즉, 3(mod 5) = 8(mod 5) = −2(mod 5)
  - 간단히; $3 \equiv 8 \equiv -2 \pmod 5$
- $\mathbb{Z}_3 = \{0(\text{mod } 3), 1(\text{mod } 3), 2(\text{mod } 3)\}$

잉여류

- $a \equiv b \pmod{n}$, ("modulo n")
  $\Leftrightarrow$ a, b 를 n 으로 나눈 나머지가 같다
  $\Leftrightarrow$ (a-b) 는 n 의 배수

- 보기
  - $6 \equiv -1 \pmod{7}$, $7 \equiv 0 \pmod{7}$
  - $n-1 \equiv -1 \pmod{n}$, $2n \equiv n \pmod{n}$
  - $3^4 \equiv 1 \pmod{5}$, $4^{61} \equiv 4 \pmod{61}$, (Fermat)
  - $408! \equiv -1 \pmod{409}$, (Wilson)

Bar Notation

- Bar Notation (‘Magic Bar’)
- [(5 로 나눈) 나머지 3] = 3(mod 5) = $\underline{3}$
  - $\underline{3} = \underline{8} = \underline{-2}$, $\underline{0} = \underline{5} = \underline{10}$
- $\mathbb{Z}_n = \{\underline{0}, \underline{1}, \underline{2}, \ldots, \underline{n-1}\} = \{\underline{n}, \underline{n+1}, \underline{2}, \ldots, \underline{-1}\}$
  - $|\mathbb{Z}_n| = n$
- 원래는 overbar……

잉여류의 새로운 이해

- '잉여류(Residue Class)'의 '류'는 '집합'
  - $\underline{3} = 3 (\mathrm{mod}\ 5) = \{\ldots, -7, -2, 3, 8, \ldots\}$
  - $\underline{-2} = \underline{3} = \underline{8}$
  - (앞으로 슬슬) 3 와 3 을 혼동 !
- (초등학교 때) 비슷한 경험; 분수
  - $[1/2] = \{1/2, 2/4, 180/360, -3/-6, \ldots\}$
  - $[1/2] = [2/4] = [-3/-6]$
  - $[1/2]$ 과 $1/2$ 을 혼동 !

잉여산(Residue Calculus)

- 완전한 민주주의
  - 전체 $\mathbb{Z}$를 잉여류(지역구)들로 분할(partition)
  - 누구나 (지역구의) 대표가 될 수 있다
    - $\underline{3} = \underline{8}$, $\underline{-1} = \underline{9}$ (in $\mathbb{Z}_5$)
  - 누가 대표로 나가든 ($\mathbb{Z}_5$ 의 연산) 결과는 같다
    - 잉여류 $\underline{3}$ 의 대표가 3 이든 8 이든
    - 잉여류 $\underline{4}$ 의 대표가 (-1) 이든 9 이든
    - $\underline{3}+\underline{-1} = \underline{8}+\underline{9}$
    - $\underline{3} \times \underline{-1} = \underline{8} \times \underline{9}$

잉여산

- '나머지들 간의 연산이 가능하다'
  = '누가 (잉여류의)대표로 나가든 (연산)결과는 같다'

- a = a′, b = b′ 이면
  - 즉, (a−a′) 과 (b−b′) 이 n 의 배수이면
  - 덧셈; a+b = a′+b′
    - 증명; (a+b)−(a′+b′) = (a−a′)+(b−b′)
    - 필요한 성질; n 의 배수의 합은 n 의 배수
  - 곱셈; ab = a′b′
    - 증명; ab−a′b′ = (a−a′)b+a′(b−b′)
    - 필요한 성질; n 의 배수의 배수는 n 의 배수

분수의 연산

- (초등학교 때) 비슷한 경험; 분수
  - [a/b] = [a′/b′], [c/d] = [c′/d′] 이면
    - 즉, ab′ = a′b, cd′ = c′d 이면
  - [a/b]+[c/d] = [a′/b′]+[c′/d′]
  - [a/b] × [c/d] = [a′/b′] × [c′/d′]

잉여류들의 세계 $\mathbb{Z}_n$

- $\underline{a} = \underline{a'}$, $\underline{b} = \underline{b'}$ (in $\mathbb{Z}_n$) 이면
  - $\underline{a+b} = \underline{a'+b'}$, $\underline{ab} = \underline{a'b'}$
- 따라서, $a, b \in \mathbb{Z}$ (즉, $\underline{a}, \underline{b} \in \mathbb{Z}_n$) 일 때

  $$\underline{a}+\underline{b} = \underline{a+b}, \quad \underline{a} \cdot \underline{b} = \underline{ab}$$

  로 정의
- $\mathbb{Z}_n$ 의 덧셈과 곱셈이 '잘 정의되어 있다(well-defined)'

잉여류들의 세계 $\mathbb{Z}_n$

- 결합법칙, 분배법칙, 교환법칙 모두 성립
  - 증명은 'Magic Bar'; 이었다 끊었다 반복……
  - 보기; 분배법칙, 곱셈의 결합법칙

$$\underline{a}(\underline{b}+\underline{c}) = \underline{a}(\underline{b}+\underline{c}) = \underline{a(b+c)} = \underline{ab+ac} = \underline{ab}+\underline{ac} = \underline{a}\,\underline{b}+\underline{a}\,\underline{c}$$

$$\underline{a}\cdot(\underline{b}\cdot\underline{c}) = \underline{a}\cdot\underline{bc} = \underline{a(bc)} = (\underline{ab})\underline{c} = \underline{ab}\cdot\underline{c} = (\underline{a}\cdot\underline{b})\cdot\underline{c}$$

- 항등원(identity element)
  - 덧셈의 항등원; $\underline{0}$, $(\underline{a}+\underline{0} = \underline{a})$
  - 곱셈의 항등원; $\underline{1}$, $(\underline{a}\cdot\underline{1} = \underline{a})$

- (마치 정수들처럼) 잉여류들의 덧셈, 곱셈 자유자재로 가능

잉여류들의 세계 $\mathbb{Z}_n$

- 표기법; $3^2 = \underline{3} \cdot \underline{3} = \underline{3^2}$

- 보기; $3^5 \equiv 3 \pmod 5$, $\underline{3}^5 = \underline{3} \in \mathbb{Z}_5$
  - $\underline{3}^2 = \underline{3} \cdot \underline{3} = \underline{9} = \underline{4}$,
  - $\underline{3}^3 = \underline{3}^2 \cdot \underline{3} = \underline{4} \cdot \underline{3} = \underline{12} = \underline{2}$,
  - $\underline{3}^4 = \underline{3}^3 \cdot \underline{3} = \underline{2} \cdot \underline{3} = \underline{6} = \underline{1}$,
  - $\underline{3}^5 = \underline{3}^4 \cdot \underline{3} = \underline{1} \cdot \underline{3} = \underline{3}$
    - $\underline{3}^5 = \underline{3}^3 \cdot \underline{3}^2 = \underline{2} \cdot \underline{4} = \underline{8} = \underline{3}$
  - $\mathbb{Z}_5 = \{\underline{0}, \underline{1}, \underline{3}, \underline{3}^2, \underline{3}^3\}$

- *이 정도만 잘 이해하면……*

잉여류들의 세계 $\mathbb{Z}_n$

- 뺄셈 $(\underline{a}-\underline{b})$ 는 $(\underline{a}+-\underline{b})$ 로 이해
  - 이때 $-\underline{b}$ 는 덧셈에 관한 $\underline{b}$ 의 역원소, $(\underline{b}+-\underline{b}=\underline{0})$

- 나눗셈? 곱셈에 관한 inverse 존재?
  - $\underline{a} \neq \underline{0}$ 일 때,
  - $\underline{a}\cdot\underline{b}=\underline{1}$ 인 $\underline{b}=\underline{a}^{-1}$ 존재?

  - 보기; $\underline{3}\cdot\underline{2}=\underline{1}\in\mathbb{Z}_5$, 즉 $\underline{3}^{-1}=\underline{2}$

    $[\underline{4}$ 나누기 $\underline{3}]=\underline{4}\cdot\underline{2}=\underline{3}$

잉여류들의 세계 $\mathbb{Z}_n$

- 그러나, $\underline{2} \in \mathbb{Z}_4$ 의 inverse $\underline{2}^{-1}$ 없음 !
  - $\underline{3} \in \mathbb{Z}_4$ 의 inverse 는 $\underline{3}$
- 게다가, $\underline{2} \cdot \underline{2} = \underline{0} \in \mathbb{Z}_4$
  - [non-zero] x [non-zero] = [zero] !
  - zero-divisor
- $\mathbb{Z}_n$ 의 어떤 원소가 inverse 를 갖는가 ?
  - 열쇠; Euclidean Algorithm(유클리드의 호제법)

Euclidean Algorithm

- *(학부)대수학의 모든 것은 division algorithm의 결과*
  - $a, b \in \mathbb{Z}$, $b \neq 0$
  - $a = bq + r$, $0 \leq r < b$ 인 q, r 존재(유일)

- Euclidean Algorithm
  - a, b; 정수이면, $ax+by = (a,b)$ 인 정수 x, y 존재
  - 단, (a,b) = [a 와 b 의 최대공약수]

    - Division Algorithm 몇 번 계속
    - 원래는 최대공약수 구하는 알고리즘

Euclidean Algorithm

- $a, b \neq 0$; 자연수

$$a = r_{-1} = bq_1 + r_1 \quad (0 < r_1 < r_0 = b)$$
$$b = r_0 = r_1 q_2 + r_2 \quad (0 < r_2 < r_1)$$
$$r_1 = r_2 q_3 + r_3 \quad (0 < r_3 < r_2)$$
$$\vdots$$
$$r_{i-1} = r_i q_{i+1} + r_{i+1} \quad (0 < r_{i+1} < r_i)$$
$$r_i = r_{i+1} q_{i+2} \quad (0 = r_{i+2})$$

  - $r_{i+1} = (a,b) = \gcd(a,b)$
  - r_k 모두 $ax_k + by_k$ 꼴
  - 따라서 $ax+by = (a,b)$ 인 x, y 존재

Euclidean Algorithm

- [정리] $\underline{a} \in \mathbb{Z}_n$ has an inverse $\Leftrightarrow$ $(a,n) = 1$
  - 증명; $(a,n) = 1$
    $\Leftrightarrow$ $ax+ny = 1$ 인 x, y 존재
    $\Leftrightarrow$ $\underline{a}\,\underline{x}+\underline{n}\,\underline{y} = \underline{a}\,\underline{x}+\underline{0}\,\underline{y} = \underline{a}\,\underline{x} = \underline{1}$ 인 $\underline{x} \in \mathbb{Z}_n$ 존재
- 그런데, $\underline{a} = \underline{b} \in \mathbb{Z}_n$ 이면, $(a,n) = (b,n)$?
  - 물론 ! (민주주의)

Euler Phi Function

- $(\mathbb{Z}_n)^\times = \{\underline{a} \in \mathbb{Z}_n \mid (a,n) = 1\}$
  $= $ inverse 갖는 잉여류들의 집합

- $|(\mathbb{Z}_n)^\times| = |\{a \in \mathbb{Z} \mid 1 \leqq a < n,\ (a,n) = 1\}|$
  $= \varphi(n)$, (Euler phi function)

  - $\varphi(2) = 1,\ \varphi(3) = 2,\ \varphi(4) = 2,\ \varphi(5) = 4,\ \varphi(6) = 2$
  - p; 소수 $\Rightarrow \varphi(p) = p-1,\ \ \varphi(p^n) = p^n - p^{n-1}$
  - $(a,b)=1 \ \Rightarrow \varphi(ab) = \varphi(a)\cdot\varphi(b)$

Group

- Group
- Abelian Group
- Cyclic Group

Group

- 집합 G 에 (2항)연산 * 가 정의되어 있고
  - 결합법칙; $(g*h)*k = g*(h*k)$ for all $g,h,k \in G$
  - $\exists\ e \in G$ such that $g*e = e*g = g$ for all $g \in G$
  - For $g \in G$, $\exists\ g' \in G$ such that $g*g' = g'*g = e$

  만족하면, $G = (G,*)$ 를 group 이라고 부른다

- e = [G 의 항등원]
  - e 는 g 의 선택과 무관
- (셋째 조건의) g′ = [g 의 역원]
  - [g 의 역원] 은 g 에 따라 결정됨

Abelian Group

- G; abelian (commutative) group

  $\Leftrightarrow$ $g*h = h*g$ for all $g, h \in G$

  - Only abelian groups today

- 보기;
  - $(\mathbb{Z},+)$, $(\mathbb{Z}_n,+)$, $(\mathbb{C},+)$, ...
  - $((\mathbb{Z}_n)^\times, 곱)$; $\underline{1} \in (\mathbb{Z}_n)^\times$, $\underline{ab}^{-1} = \underline{a}^{-1}\underline{b}^{-1}$, $(\underline{a}^{-1})^{-1} = \underline{a}$
  - $(U_n, 곱) = \{w \in \mathbb{C} \mid w^n = 1\}$, $|U_n| = n$
  - Elliptic curve

표기법

	multiplicative notation	additive notation
group	$g, h \in (G, 곱)$	$a, b \in (A, +)$
항등원	$1 = 1_G$	$0 = 0_A$
역원	g^{-1}	$-a$
지수	$g^1 = g,\ g^0 = 1,\ g^{-1} = g^{-1}$	$1a = a,\ 0a = 0_A,\ (-1)a = -a$
	$g^2 = gg,\ g^3 = ggg$	$2a = a+a,\ 3a = a+a+a$
	$g^{-2} = g^{-1}g^{-1} = (g^{-1})^2$	$(-2)a = (-a)+(-a) = 2(-a)$
	$g^{-3} = g^{-1}g^{-1}g^{-1} = (g^{-1})^3$	$(-3)a = 3(-a)$

Exponential Law (지수법칙)

	multiplicative notation	additive notation
m,n; 정수	$g^m g^n = g^{m+n}$	ma+na = (m+n)a
	$(g^m)^n = g^{mn}$	n(ma) = (nm)a
	$g^n h^n = (gh)^n$	n(a+b) = na+nb
		(분배법칙?)

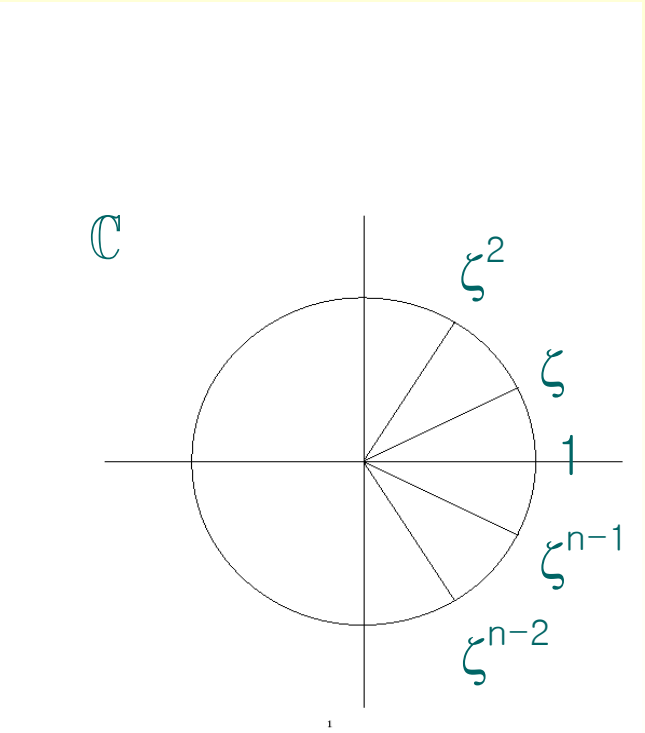
Cyclic Group

- For $g \in G$, denote (multiplicative notation)
  $\langle g \rangle = \{\ldots, g^{-2}, g^{-1}, 1, g, g^2, g^3, \ldots\} \leq G$
  - 주의; $i \neq j$ 라고 해서 꼭 $g^i \neq g^j$ 일 필요 없음
  - 즉, $\langle g \rangle$ 는 g 를 포함하는 G 의 가장 작은 subgroup

- G is cyclic $\Leftrightarrow$ $G = \langle g \rangle$ for some $g \in G$
  - g = [generator of G]
  - $|G|=n$ 이면 $g^n=1$ (따라서 모든 $a \in G$에 대해 $a^n=1$)

  - $\mathbb{Z} = \langle 1 \rangle = \{\ldots, (-2)\cdot 1, (-1)\cdot 1, 0, 1, 2\cdot 1, 3\cdot 1, \ldots\}$
  - $\mathbb{Z}_n = \langle \underline{1} \rangle = \{\underline{0}, 2\cdot\underline{1}, 3\cdot\underline{1}, \ldots, (n-1)\cdot\underline{1}\}$
  - $U_n = \langle \zeta_n \rangle$, 단 $\zeta_n = \sin(2\pi/n) + i\cos(2\pi/n)$

$$U_n = \{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\} = \langle\zeta\rangle$$



$$\zeta = \sin(2\pi/n) + i \cdot \cos(2\pi/n)$$

Cyclic Group

- Cyclic group의 구조는 (정말) 완전히 이해
  - Cyclic group의 분류
    - 본질적으로 $\mathbb{Z}$ 와 $\mathbb{Z}_n$ 뿐('본질적으로'는 무슨 뜻?)
  - Cyclic group 의 subgroup 도 cyclic
  - $G = \langle g \rangle$, $|G| = n$
    - d divides n ⇒ 원소수 d 인 subgroup 존재(유일)
    - $|g^m| = n/(m,n)$
      - [number of generators of G]= $\varphi(n)$
    - $|\{h \in G \mid h^m = 1\}| = (m,n)$
  - 증명; easy……

- 그러나, 'computational problem' DLP……

Ring, Field, Vector Space

- Ring 과 Unit Group
- Field
- Extension Field 와 Vector Space
- Polynomial Ring R[t]
- Division Algorithm in R[t]

Ring

- 덧셈과 곱셈이 정의되어 있는 집합 R 이 조건
  - (R,+); abelian group
  - 곱셈의 결합법칙; (xy)z = x(yz)
  - 분배법칙; x(y+z) = xy+xz

  만족하면, R = (R,+,곱) 을 ring 이라고 부른다

- 보기; $\mathbb{Z}$, $\mathbb{Z}_n$, $\mathbb{R}$, $\mathbb{C}$, ...
  - $\mathbb{Z}[\sqrt{-1}] = \{m+n\sqrt{-1} \in \mathbb{C} \mid m,n \in \mathbb{Z}\}$, (Gaussian integers)
  - Only commutative rings(xy = yx) today

Ring 에서의 표기법

- 물론 덧셈은 'additive notation' 사용
  곱셈은 'multiplicative notation' 사용
- [덧셈의 항등원] = $0 = 0_R$
- [곱셈의 항등원] = $1 = 1_R$
- 약속; $0 \neq 1$

- Denote; $2 \cdot 1_R = 1_R + 1_R = 2_R$, $(3_R, 4_R, \ldots)$
- 주의; $\mathbb{Z}_5$ 에서는 $1_R = 6_R$, $5_R = 0_R$, ...
  - 슬슬 2 와 2_R 혼동!

Unit Group

- $u \in R$ is a unit (invertible)
  $\Leftrightarrow \exists\ v \in R$ such that $uv = 1$ (denote $v = u^{-1}$)
- $R^\times = \{u \in R \mid u \text{ is a unit}\} = [\text{unit group of } R]$
  - Recall; $(\mathbb{Z}_n)^\times$, $\mathbb{C}^\times = \mathbb{C} - \{0\}$
- $(R^\times, \text{곱})$ 은 실제로 (multiplicative) group
  - $1 \in R^\times$
  - $u \in R^\times \Rightarrow u^{-1} \in R^\times$, $((u^{-1})^{-1} = u)$
  - $u, v \in R^\times \Rightarrow uv \in R^\times$, $((uv)^{-1} = v^{-1}u^{-1})$

Field(體, Corps(불) , Körper(독))

- Ring (F,+,곱) is a field ⇔ $F^{\times} = F - \{0\}$
  - F 의 모든 non-zero element 는 unit, $(1 \in F)$
  - 사칙연산(가감승제) 가능
  - $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$
  - $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$, ('분모의 유리화')
- Field 에는 zero-divisor 없음
  - $xy = 0 \Rightarrow [x = 0 \text{ or } y = 0]$
    - $x \neq 0 \Rightarrow y = 1y = x^{-1}xy = x^{-1}0 = 0$

Field

- [정리] $\mathbb{Z}_n$ is a field $\Leftrightarrow$ n; prime
  - 다시 증명 (아까 언제 증명?)
  - ($\Rightarrow$) $n = 6 \Rightarrow \underline{0} = \underline{6} = \underline{2} \cdot \underline{3} \Rightarrow$ zero-divisor
  - ($\Leftarrow$) $\underline{a} \neq \underline{0} \Rightarrow (a,n) = 1 \Rightarrow$ a 는 unit
    - n 의 약수는 1 과 n 뿐, Euclidean Algorithm
- $\mathbb{Z}_p$ = [finite field with p elements] = $\mathbb{F}_p$
  - p; prime
  - Finite field with $q = p^n$ elements? 잠시 후……

Extension Field

- E is an extension field of F (write E/F) iff

  F is a subfield of E (write F≤E) iff
  - E, F; field, $F \subseteq E$
  - F 의 연산은 E 의 연산을 제한한 것
  - E, F 의 0, 1 공통

- 보기; $\mathbb{C}/\mathbb{R}$, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$
  - $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$

    $= \mathbb{Q}$와 $\sqrt{2}$ 포함하는 가장 작은 field

Vector Space

- E, F; field, E/F ⇒ E; vector space over F
  - E-위의 F-상수곱을 E의 곱셈으로 정의
    - a∈F, b∈E일 때, [a상b = a곱b] 로 정의
    - F의 원소는 scalar이면서 동시에 vector
  - $\mathbb{C}/\mathbb{R}$; $\dim_{\mathbb{R}}(\mathbb{C}) = 2$, $\mathbb{R}$-basis; {1, $\sqrt{-1}$}
  - $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$; $\dim_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2})) = 2$, $\mathbb{Q}$-basis; {1, $\sqrt{2}$}

복습; Algebraic Structures

	group	ring	vector space
연산	(G,*)	(R,+,곱)	(V,+,상)
항등원	e	덧셈; 0 곱셈; 1	덧셈; 0
결합법칙	*	덧셈, 곱셈	덧셈
분배법칙	없음	하나	둘
추가 조건	역원	(R,+); abel group	(V,+); abel group (ab)v=a(bv), 1v=v
field; 특수한 ring			

다항식의 잉여류

- Polynomial Ring R[t]
- 다항식의 잉여류
- Finite Field
- Computation in Finite Field
- AES (Rijndael)

Polynomial Ring R[t]

- Polynomial(다항식, 정식) over R; (단 R; ring)

$$f(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0, \quad (a_i \in R)$$

  - $[a_n t^n + \cdots + a_1 t + a_0]$ 전체를 formal symbol 로 이해!
  - $a_n \neq 0$ 이면, $\deg(f) = n$, (최고차항)

- R[t] = [the set of all polynomials over R]
  - R[t] 는 ring
    - 덧셈, 곱셈
  - 잘 아는 것 같지만……

Division Algorithm in R[t]

- $a(t), b(t) \in R[t]$, $[b(t)$의 최고차항 계수$] \in R^{\times}$
  - $a(t) = b(t) \cdot q(t) + r(t)$, $\deg(r) < \deg(b)$
  - $\deg(0) = -\infty$, $\deg(1) = 0$
- 인수 정리('인수'는 '약수'의 고어)
  - $c \in R$, $f(t) \in R[t]$, $f(c) = 0 \Rightarrow (t-a)$ divides $f(t)$ in $R[t]$
    - $f(t) = (t-c) \cdot q(t) + r(t)$, $\deg(r) < 1$, $r(t) = r \in R$
    - $t = c$ '대입', $0 = f(c) = r$

새로운 세계; 다항식의 잉여류

- 지금까지 $\mathbb{Z}_n$ (정수의 잉여류) 공부
- 이제 다항식(정식)의 잉여류 공부
- 첫째 시간 잉여류와 잉여산 (전부) 다시 반복
  - F; field, $f(t) \in F[t]$, $n = \deg(f) \geq 1$
  - [f(t) 로 나눈 나머지들의 세계] = $F[t]_{f(t)}$
  - (다항식의) 잉여류들 간 덧셈, 곱셈; well-defined
  - $F[t]_{f(t)}$; ring 이면서 F-vector space

  - $F[t]_{f(t)}$ 는 아주 나쁜 '임시표기법'…… 사실은 $\mathbb{Z}_n$ 도

다항식의 잉여류와 잉여산

- $a(t) \equiv b(t) \pmod{f(t)}$
  $\Leftrightarrow \underline{a(t)} = \underline{b(t)} \in F[t]_{f(t)}$
  $\Leftrightarrow f(t)$ divides $a(t)-b(t)$ in $F[t]$
  - 슬슬 $\underline{a(t)}$ 와 $a(t)$ 혼동

- $\deg(f) = n \geq 1 \Rightarrow F[t]_{f(t)} = \{\underline{h(t)} \mid h(t) \in F[t], \deg(h) < n\}$

- $F[t]_{f(t)}$-위에 F-상수곱을 $a \cdot \underline{h(t)} = \underline{a \cdot h(t)}$ 로 정의, $(a \in F)$
  - $F[t]_{f(t)}$; n-dimensional F-vector space
  - F-basis; $\{\underline{1}, \underline{t}, \underline{t^2}, \ldots, \underline{t^{n-1}}\} = \{\underline{1}, \underline{t}, \underline{t^2}, \ldots, \underline{t^{n-1}}\}$

다항식의 잉여류들의 세계

- 보기; $f(t)=t^2+1\in\mathbb{R}[t]$
  - $\mathbb{R}[t]_{f(t)}=\{\underline{at+b}\mid a,b\in\mathbb{R}\}$
  - $t^2+1\equiv 0 \pmod{f(t)}$, $t\equiv t^2+t+1 \pmod{f(t)}$, ...
  - $\underline{t^2+1}=\underline{0}$, $\underline{t}=\underline{t^2+t+1}$, $\underline{3t+2}=\underline{(t^2+1)\cdot h(t)+(3t+2)}$, ...
  - $\underline{t^2}=\underline{-1}$, (제곱해서 (-1) 되는 것 존재)
    - $\mathbb{R}[t]_{f(t)}\approx\mathbb{C}$? '≈'의 의미는 ?
- 마찬가지로, $f(t)=t^2-2\in\mathbb{Q}[t]$
  - $\mathbb{Q}[t]_{f(t)}=\{\underline{at+b}\mid a,b\in\mathbb{Q}\}$
  - $\underline{t^2}=\underline{2}$, (제곱해서 2 되는 것 존재)
    - $\mathbb{Q}[t]_{f(t)}\approx\mathbb{Q}(\sqrt{2})$? '≈'의 의미는 ?

다항식의 잉여류들의 세계

- Ring $F[t]_{f(t)}$ 는 언제 field 가 되는가?
  - Euclidean Algorithm in F[t]
  - F[t] 의 최대공약수 ('최대'; degree 최대)

번역기	정수	다항식
나눗셈의 나머지 조건	$0 \leq r < b$	$\deg(r) < \deg(b)$ $\deg(0) = -\infty$
크기	절대값	degree
소수	prime	irreducible

Irreducible Polynomial

- n; prime number ⇔ n 의 약수는 1, n 뿐
- $f(t) \in F[t]$; irreducible polynomial
  ⇔ f(t) 의 약수는 1, f(t) 뿐

- [정리] $F[t]_{f(t)}$; field ⇔ f(t); irreducible
  - 증명? 아까 이미 증명!

Finite Field

- p; 소수, $F = \mathbb{Z}_p = \mathbb{F}_p$,
  $f(t) \in \mathbb{F}_p[t]$; irreducible, $\deg(f) = n > 0$
- $\mathbb{F}_p[t]_{f(t)}$; finite field with $q = p^n$ elements
  - $\mathbb{F}_p[t]_{f(t)}$; n-dimensional $\mathbb{F}_p$-vector space
  - $a_{n-1}t^{n-1} + \cdots + a_1 t + a_0$, $(a_i \in \mathbb{F}_p)$
  - Scalar a_i 후보 각 p-개뿐
- Denote $\mathbb{F}_p[t]_{f(t)} = \mathbb{F}_q$
  - $\mathbb{F}_q$ 는 f(t) 의 선택과 무관함을 암시……

주의; $\mathbb{F}_q \neq \mathbb{Z}_q$

- 물론 $\mathbb{F}_p = \mathbb{Z}_p$
- $n > 1$, $q = p^n$ 이면, $\mathbb{F}_q$ 와 $\mathbb{Z}_q$ 는 전혀 다름
  - $\mathbb{Z}_q$; field 아님
  - $(\mathbb{Z}_q, +) = \langle \underline{1} \rangle$; cyclic, $(\mathbb{F}_q, +)$; not cyclic
  - $((\mathbb{F}_q)^\times, \text{곱})$; cyclic, (잠시 후)
  - [참고] $(\mathbb{Z}_n)^\times$; cyclic $\Leftrightarrow$ $n = 2, 4, p^k, 2p^k$
    - 단, p; odd prime, k; 자연수)

Computation in Finite Field

- $(\mathbb{Z}_5)^\times = \langle \underline{3} \rangle = \{\underline{1}, \underline{3}, \underline{3}^2, \underline{3}^3\} = \langle \underline{2} \rangle$
- $(\mathbb{Z}_7)^\times = \langle \underline{3} \rangle = \{\underline{1}, \underline{3}, \underline{3}^2, \ldots, \underline{3}^5\} \neq \langle \underline{2} \rangle$

- $p = 2, \quad f(t) = t^2+t+1, \quad q = 2^2 = 4$
  - $(\mathbb{F}_4)^\times = \{\underline{1}, \underline{t}, \underline{t+1}\}$
  - $\underline{t}^2 = \underline{t+1}, \quad (\underline{-1} = \underline{1})$
  - $(\mathbb{F}_4)^\times = \{\underline{1}, \underline{t}, \underline{t}^2\} = \langle \underline{t} \rangle$; cyclic group

Computation in Finite Field

- $p = 2,\ \ f(t) = t^3+t+1,\ \ q = 2^3 = 8$
  - $(\mathbb{F}_8)^\times = \{1,\ t,\ t+1,\ t^2,\ t^2+1,\ t^2+t,\ t^2+t+1\}$
  - $t^3 = t+1,\ \ (-1 = 1)$
  - $t^4 = (t+1)t = t^2+t$
  - $t^5 = (t^2+t)t = t^3+t^2 = (t+1)+t^2 = t^2+t+1$
  - $t^6 = (t^2+t+1)t = t^3+t^2+t = (t+1)+t^2+t = t^2+1,\ (t+t = 0)$
    - $t^6 = (t^3)^2 = (t+1)^2 = t^2+2t+1 = t^2+1,\ \ (2t = 0)$
  - $t^7 = (t^2+1)t = t^3+t = 1$
  - $(\mathbb{F}_8)^\times = \{1,\ t,\ t^2,\ \ldots,\ t^6\} = \langle t \rangle$; cyclic group

Computation in Finite Field

- $p = 2,\ f(t) = t^3+t+1,\ q = 2^3 = 8$
  - $(\mathbb{F}_8)^\times = \langle t \rangle,\ t^3 = t+1$
- $p = 2,\ g(s) = s^3+s^2+1,\ q = 2^3 = 8$
  - $(\mathbb{F}_8)^\times = \langle s \rangle,\ s^3 = s^2+1$
- 둘 다 $\mathbb{F}_8$ 이라니?

- $p = 2,\ f(t) = t^4+t^3+t^2+t+1,\ q = 2^4 = 16$
  - $(\mathbb{F}_{16})^\times = \langle t+1 \rangle \neq \langle t \rangle$

Computation in Finite Field

- $p = 3,\ \ n = 3\ ,\ \ f(t) = t^3+2t+1,\ \ \mathbb{F}_{27}$
  - $-1 = 2,\ \ -2 = 4 = 1,\ \ 3 = 0$
  - $t^3 = -2t-1 = t+2$
  - $t^6 = (t^3)^2 = (t+2)^2 = t^2+4t+1 = t^2+t+1$
  - $(t^6+1)(t+2) = (t^2+t+2)(t+2) = t^3+t^2+2t+2t^2+2t+4$
    $= t^3+3t^2+4t+4 = t^3+t+1 = (t+2)+t+1$
    $= 2t+3 = 2t$

AES (Rijndael)

- AES (Advanced Encryption Standard)
  - DES (Data Encryption Standard) 의 '후속 모델'
  - 1 byte (8 bit) 단위 계산
  - 8 bit string 을 7-차 다항식으로 이해
    - $(1,1,0,0,1,0,1,0) = t^7+t^6+t^3+t$
  - $\mathbb{F}_2[t]_{f(t)} = \mathbb{F}_{256}$ 의 연산 사용
    - $p = 2$, $f(t) = t^8+t^4+t^3+t+1$, $q = 2^8 = 256$
    - 덧셈; bitwise XOR, 즉 $\mathbb{F}_2$-벡터공간 $(\mathbb{F}_2)^8$ 의 덧셈
    - 곱셈; $\mathbb{F}_{256}$ 의 곱셈

DLP

- Cyclic Group Again
- Primitive Root
- Discrete Logarithm Problem (DLP)
- Diffie-Hellman Key Exchange
- ElGamal Public-Key Cryptosystem

Cyclic Group Again

- [Theorem A]

  F; field, $H \leq (F^{\times}, \text{곱})$, $|H| < \infty \Rightarrow$ H; cyclic

  - 'Finite multiplicative subgroup of a field is cyclic'
    - Proof without motivation; 30 분
    - Proof with motivation; 1 개월
      - Finite abelian group 의 분류, Jordan decomposition, ……

- 따라서 (p; 소수, $q = p^n$)
  - $(\mathbb{F}_p)^{\times} = (\mathbb{Z}_p)^{\times} = \langle \underline{a} \rangle$ for some $\underline{a}$
  - $(\mathbb{F}_q)^{\times} = \langle \gamma \rangle$ for some γ

Cyclic Group Again

- $(\mathbb{F}_q)^\times = \langle\gamma\rangle$, ($\gamma$; primitive root in $(\mathbb{F}_q)^\times$)
  - $\alpha^{q-1} = 1$ for all $\alpha \in \mathbb{F}_q$
    - $\alpha^q = \alpha$ for all $\alpha \in \mathbb{F}_q$
  - $a, b \in \mathbb{Z} \Rightarrow [\gamma^a = \gamma^b \Leftrightarrow a \equiv b \pmod{(q-1)}]$

- *문제의 본질 (?);*
  - Existence proof of γ is NOT constructive
    - [# of generators of $(\mathbb{F}_q)^\times$] = $\varphi(q-1)$
  - *$\mathbb{F}_q$의 곱셈 구조는 q에 묘하게 depend ……*

Primitive Root Modulo p

- a; primitive root mod p (p; 소수)
  $\Leftrightarrow (\mathbb{F}_p)^{\times} = (\mathbb{Z}_p)^{\times} = \langle \underline{a} \rangle$, a; '최소'
  - 모든 기초정수론 책 부록;
    primitive root mod p 의 list (p <1000)
  - Primitive root 구하는 뾰족한 방법 없다는 뜻
    - a = 2, 3 많이 보이고
    - p = 409 ⇒ a = 21
      - $(\mathbb{F}_{409})^{\times}$의 generator 개수 $\varphi(409-1) = 128$
      - $(\mathbb{F}_{419})^{\times}$의 generator 개수 $\varphi(419-1) = 180$
      - $(\mathbb{F}_{421})^{\times}$의 generator 개수 $\varphi(421-1) = 96$

p	a
401	3
409	21
419	2
421	2
431	7
433	5
439	15
443	2
妙 !	

Discrete Logarithm Problem

- Cyclic group 에 대해서는 완전히 이해하지만
  - $(\mathbb{Z}_5)^x = \langle 3 \rangle$, $3^c = 2$ 일 때, $c = ?$ ㅎㅎ
  - $(\mathbb{Z}_{409})^x = \langle 21 \rangle$, $21^c = 99$ 일 때, $c = ?$ ㅠㅠ
- DLP; $G = \langle g \rangle$, given $h = g^c \in G$, find $c \in \mathbb{N}$
  - $c = \log_g h$
    - Baby-step giant-step, index calculus, Pohlig-Hellman Pollard rho, Pollard lambda 등 공격법
    - $|G|$; 750-1000 bit 사용

Diffie-Hellman Key Exchange

- Setup
  - G = <g> 와 |G| (중앙 관리기관이) 공개
  - 사용자 A 의 비밀키 a, B 의 비밀키 b, ... (0 < a, b < |G|)
  - A 는 g^a 계산해 공개, B 는 g^b 계산해 공개, ...
    - 원래 k 명 대칭키 단순 교환; k(k+1)/2 개의 비밀키 필요
    - 지금은 공개키 k 개면 충분
- A(Alice) 와 B(Bob) 둘만의 비밀키 공유
  - A computes $(g^b)^a$, B computes $(g^a)^b$
  - A 와 B 는 비밀키 $(g^b)^a = (g^a)^b$ 공유
- Diffie-Hellman Problem
  - Given g^a, g^b and g^{ab}, find a

ElGamal Public-Key Cryptosystem

- Setup
  - $G = \langle g \rangle$ 와 $|G|$ 를 (중안관리기관이) 공개
  - 사용자 A 의 비밀키 a, B 의 비밀키 b, ... , $(0 < a, b < |G|)$
  - A 는 g^a 계산해 공개, B 는 g^b 계산해 공개, ...
- ElGamal Encryption/Decryption
  - A 가 B 에게 message $m \in G$ 를 보낼 때
    - Choose a random number r, $(0 < r < |G|)$
    - Compute $x = m \cdot (g^b)^r$ and $y = g^r$, send the pair (x,y) to B
  - B 의 decryption
    - Compute $x \cdot y^{-b} = m \cdot (g^b)^r \cdot (g^r)^{-b} = m \cdot g^{br} \cdot g^{-br} = m$
- G; $(\mathbb{F}_q)^x$, elliptic curve, ...

Char p 의 별세계

- Characteristic
- 왜 원소 6 개인 유한체는 없는가?
- Characteristic p 의 별세계
- Freshman's Dream
- 유한체 위의 선형대수

Characteristic

- [characteristic of a ring R] = char(R)
  - $|1_R|$ = [order of 1_R in the additive group (R,+)]
  - 정의: $\mathrm{char}(R) = 0 \Leftrightarrow n \cdot 1_R \neq 0_R$ if $0 \neq n \in \mathbb{Z}$
  - 정의: $m > 0$ 일 때,

    $\mathrm{char}(R) = m \Leftrightarrow$ m 은 $m \cdot 1_R = 0_R$ 인 최소의 자연수

  - $\mathrm{char}(\mathbb{Z}) = \mathrm{char}(\mathbb{Q}) = \mathrm{char}(\mathbb{R}) = \mathrm{char}(\mathbb{C}) = 0$
  - $\mathrm{char}(\mathbb{Z}_n) = n$, $\mathrm{char}(\mathbb{F}_p) = \mathrm{char}(\mathbb{F}_q) = p$

Characteristic of a Field

- F; field ⇒ char(F) = 0 or p, (p; prime)
  - char(F) = 6 ⇒ $0_F = 6 \cdot 1_F = (2 \cdot 1_F) \cdot (3 \cdot 1_F)$
    ⇒ zero-divisor in F

- 환영; 'world of positive characteristic'
  - 만약 char(F) = 0 이면,
    - 무한집합 $\mathbb{N} = \{1_F, 2 \cdot 1_F, 3 \cdot 1_F, \ldots\} \subset F$

왜 원소 6 개인 유한체 없는가?

- F; finite field $\Rightarrow |F| = p^n$, (p; prime)
  - Let $\mathrm{char}(F) = p > 0$
  - $\mathbb{F}_p \leq F$
    - $\mathbb{F}_p = \{0_F, 1_F, 2\cdot 1_F, 3\cdot 1_F, \ldots, (p-1)\cdot 1_F\} \leq F$
      - $\mathbb{F}_p$ 는 characteristic p 인 최소의 field
  - 즉, $F/\mathbb{F}_p$, (extension field)
  - F; finite dimensional $\mathbb{F}_p$-vector space
  - Let $\dim_{\mathbb{F}_p}(F) = n$
  - 이제 $|F| = p^n$

Characteristic p 의 별세계

- [$\mathbb{F}_q$ 의 덧셈] = [$\mathbb{F}_p$-벡터공간 $(\mathbb{F}_p)^n$ 의 덧셈]
  - $\{\alpha_1, \dots, \alpha_n\}$; $\mathbb{F}_p$-벡터공간 $\mathbb{F}_q$ 의 basis
  - $\mathbb{F}_q = \{c_1\alpha_1 + \cdots + c_n\alpha_n \mid c_1,\dots,c_n \in \mathbb{F}_p\}$
  - Identify $c_1\alpha_1 + \cdots + c_n\alpha_n$ with $(c_1,\dots,c_n) \in (\mathbb{F}_p)^n$
- $\mathbb{F}_q$ 의 곱셈; $(\mathbb{F}_q)^\times$ 는 cyclic group

- 덧셈; 우리가 제일 잘 아는 벡터공간의 덧셈
- 곱셈; cyclic group은 (정말) 완전히 이해
- 이 둘이 묘하게 얽혀……

Characteristic p 의 별세계

- char(F) = p > 0
  - $\Leftrightarrow p \cdot 1_F = 1_F + \cdots + 1_F = 0_F$
  - $\Leftrightarrow p \cdot \alpha = 0_F$ for all $\alpha \in F$
    - $p \cdot \alpha = \alpha + \cdots + \alpha = (1_F + \cdots + 1_F)\alpha = 0_F\,\alpha = 0_F$
- char(F) = 2
  - $\Leftrightarrow 2 = 1+1 = 0 \Leftrightarrow \alpha + \alpha = 0$ for all $\alpha \in F$
  - $\Leftrightarrow 1 = -1 \Leftrightarrow \alpha = -\alpha$ for all $\alpha \in F$
    - char(F) = 2 이면 2-차방정식의 근의 공식 없음 !

Freshman's Dream

- $\alpha, \beta \in F$, $\mathrm{char}(F) = p$ 이면, $(\alpha+\beta)^p = \alpha^p + \beta^p$
  - 이항정리: $(\alpha+\beta)^p = \alpha^p + {}_pC_1\,\alpha^{p-1}\beta + {}_pC_2\,\alpha^{p-2}\beta^2 + \cdots + \beta^p$
  - $0 < k < p$ 이면, ${}_pC_k$ 는 p 의 배수, F 에서 p 의 배수는 0
- $(\alpha+\beta)^{p^m} = \alpha^{p^m} + \beta^{p^m}$, $(\alpha-\beta)^{p^m} = \alpha^{p^m} - \beta^{p^m}$
  - $\alpha^{p^m} = 1 \Rightarrow \alpha = 1$, $\alpha^{p^m} = \beta^{p^m} \Rightarrow \alpha = \beta$
    - $0 = \alpha^{p^m} - \beta^{p^m} = (\alpha-\beta)^{p^m} \Rightarrow \alpha-\beta = 0$, $\alpha = \beta$
  - $(p = 2)$ $\alpha^2 = 1 \Rightarrow \alpha = 1$, $\alpha^2 = \beta^2 \Rightarrow \alpha = \beta$

유한체 vs. 무한체

- 유한체 위의 선형대수
- 다항식 vs. 다항함수
- 다항함수 vs. 함수
- Boolean Function

유한체 위의 선형대수

- 앞으로 '선대' 책 다시 볼 때; char p case 확인!
  - Bilinear form, quadratic form 나오면, char(F) ≠ 2
  - 그 외에는 char 0 case 와 큰 차이 없음
- Counting Problems
  - $|GL_d(q)| = |\{A \in M_d(\mathbb{F}_q) \mid \det(A) \neq 0\}|$
    $= (q^d-1)(q^d-q)(q^d-q^2)\cdots(q^d-q^{d-1})$
  - $|SL_d(q)| = |\{A \in M_d(\mathbb{F}_q) \mid \det(A) = 1\}| = ?$
  - dim(V) = d, [# of 1-dim'l subspaces] = $(q^d-1)/(q-1)$
  - dim(V) = d, [# of r-dim'l subspaces] = ??
  - $|\{A \in M_d(\mathbb{F}_q) \mid \text{rank}(A) = r\}| = ??$

유한체 위의 선형대수

- Coding Theory; [linear code] = $C \leq (\mathbb{F}_q)^m$
  - $C^{\perp} = \{x \in (\mathbb{F}_q)^m \mid \langle x,y \rangle = 0 \text{ for all } y \in C\}$; dual code
  - $\dim(C)+\dim(C^{\perp}) = m$, (why??)
    - 길이 0인 벡터($\neq 0$) 존재, no Gram-Schmidt orthogonalization

- $\exists\ A,B \in M_d(F)$ such that $AB-BA = dI$?
  - No, if char(F) = 0
    - $\text{Trace}(AB-BA) = 0 \neq d = \text{Trace}(dI)$
  - Yes, for example, if char(F) = 2 = d
    - $\text{Trace}(2I) = 0$
    - 보기; $E_{1,2}E_{2,1} - E_{2,1}E_{1,2} = E_{1,1} - E_{2,2} = I$ in $M_2(\mathbb{F}_2)$
      - 단, $E_{i,j}$ = [(i,j)-좌표만 1, 나머지 모두 0]

복소수체와 유한체 비교

- $E = \mathbb{Q}[t]_{t^2-2}$, $F = \mathbb{Q}[t]_{t^2-3}$,
  - E는 $\mathbb{Q}$와 [제곱해서 2인 것] = $\underline{t}$ 포함하는 가장 작은 field
  - $\mathbb{Q}(\sqrt{2})$도 $\mathbb{Q}$와 $\sqrt{2}$를 포함하는 가장 작은 field
  - 즉, $E \approx \mathbb{Q}(\sqrt{2})$, $F \approx \mathbb{Q}(\sqrt{3})$
  - 그러나, $E \approx \mathbb{Q}(\sqrt{2}) \not\approx \mathbb{Q}(\sqrt{3}) \approx F$
    - 왜냐하면, F에는 제곱해서 2인 것 없음

- $K = \mathbb{F}_5[t]_{t^2-2}$, $L = \mathbb{F}_5[t]_{t^2-2}$,
  - $K \approx \mathbb{F}_{25} \approx L$
    - 본질적인 차이; $K \approx$ [splitting field of $(t^{25}-t)$ over $\mathbb{F}_5$] $\approx L$

다항식 vs. 다항함수

- Polynomial f(t); formal symbol 로 이해

- $\varepsilon : F \to F$ is a polynomial function(다항함수)

  $\Leftrightarrow \exists\ f(t) \in F[t]$ such that $\varepsilon(\alpha) = f(\alpha)$ for all $\alpha \in F$

  - 이때 $\varepsilon = \varepsilon^f$ 로 표기
  - ε; 다항함수 $\Leftrightarrow \varepsilon = \varepsilon^f$ for some $f(t) \in F[t]$

다항식 vs. 다항함수

- 유한체 위에서는 [다항식] ≠ [다항함수]
  - $f(t), g(t) \in \mathbb{F}_q[t]$, $f(t) = t^q$, $g(t) = t$
    - $f(t) \neq g(t)$, (다른 degree, 다른 다항식)
    - But, $f(\alpha) = \alpha^q = \alpha = g(\alpha)$ for all $\alpha \in \mathbb{F}_q$
    - 즉, $\varepsilon^f = \varepsilon^g$, (같은 함수)
- 왜 지금까지.....?
  - F; infinite field ⇒ [다항식] = [다항함수]
    - $f(t) \neq g(t) \in F[t]$ ⇒ $f(\alpha) - g(\alpha) = 0$ 인 α 유한개뿐

다항함수 vs. 함수

- [정리] $\varepsilon : \mathbb{F}_q \to \mathbb{F}_q$; 함수 $\Leftrightarrow$ ε; 다항함수
  - $|\{\varepsilon : \mathbb{F}_q \to \mathbb{F}_q \mid \varepsilon$은 함수 $\}| = q^q$
  - $|\{f[t] \in \mathbb{F}_q[t] \mid \deg(f) < q\}| = q^q$
  - $f[t], g(t) \in \mathbb{F}_q[t]$, $\deg(f), \deg(g) < q \Rightarrow \varepsilon^f \neq \varepsilon^g$
    - $\varepsilon^f(\alpha) = \varepsilon^g(\alpha)$ for all $\alpha \in \mathbb{F}_q \Rightarrow f(t)-g(t)$ has q roots
    - But $\deg(f-g) < q$, 모순

다항함수 vs. 함수

- [정리]

  $f[t] \in \mathbb{F}_q[t]$, $\varepsilon^f = \varepsilon^0 \Leftrightarrow f[t]$; $(t^q - t)$의 배수
  - $[f[t] \in (t^q - t) \Rightarrow \varepsilon^f = \varepsilon^0]$; 자명
  - $\varepsilon^f = \varepsilon^0$ 이면, $f(t) = (t^q - t)q(t) + r(t)$
    - $0 = f(\alpha) = (\alpha^q - \alpha)q(\alpha) + r(\alpha) = r(\alpha)$ for all $\alpha \in \mathbb{F}_q$
    - But, $\deg(r) < q \Rightarrow r(t) = 0$, $t^q - t$ divides $r(t)$

- 사실 $\mathbb{F}_q[t]_{t^q - t} \approx \{\varepsilon : \mathbb{F}_q \to \mathbb{F}_q \mid \varepsilon$; 다항함수$\}$
  - First Isomorphism Theorem

다항함수 vs. 함수

- 즉, 유한체 위에서는
  - [함수] = [다항함수]
  - 또, [다변수 함수] = [다변수 다항함수]
    - 증명; 비슷.....
    - 약간 미묘....., No Division Algorithm !
- No exp, log, sin, cos, Γ, ...

Boolean Function

- $p = q = 2$ 일 때,
  - $[\eta : (\mathbb{F}_2)^m \to \mathbb{F}_2]$ = [Boolean function]
  - η; m-변수 (다항)함수
    - m-변수 (다항)함수 전부 2^{2^m}-개
- 보기($m = 2$); $\eta(x,y) = xy+x+y+1$, $(x, y \in \mathbb{F}_2)$
  - x^2, x^3, ... , y^2, y^3, ... 등은 나타나지 않음
    - $x^2 = x$
- $m = 3$ 이면, 부울 함수의 최대 항 개수는 $2^m = 8$
  - {x,y,z}의 부분집합 개수

Boolean Function

- $\varepsilon : \mathbb{F}_5 \to \mathbb{F}_5$
  - $\varepsilon(0) = 4,\ \varepsilon(1) = 3,\ \varepsilon(2) = 0,\ \varepsilon(3) = 3,\ \varepsilon(4) = 4$ 일 때
  - $\varepsilon(x) = ?x^4+?x^3+?x^2+?x^2+?,\ \ (? = 0, 1)$
    - Remember 'Lagrange Polarization'
- $\eta : (\mathbb{F}_2)^3 \to \mathbb{F}_2$
  - $\eta(x,y,z) = ?xyz+?xy+?yz+?zx+?x+?y+?z+?,\ (? = 0, 1)$
- $\eta : (\mathbb{F}_2)^8 \to \mathbb{F}_2$ 의 함수값 2^8-개가 주어졌을 때, η 를 8-변수 다항함수로 나타내라……
  - 미지수 256-개인 일차 연립방정식, (함수 후보 2^{256}-개)
  - 더 좋은 방법은 ??

유한체의 유일성

- 연산표
- Isomorphism
- 유한체의 유일성

연산표

- Groups; $(\mathbb{Z}_2,+)$, $(\clubsuit=\{짝,홀\},\heartsuit)$, $(U=\{1,-1\},곱)$
  - $U = U_2 < \mathbb{C}^\times$
  - 연산표

+	0	1
0	0	1
1	1	0

≈

♡	짝	홀
짝	짝	홀
홀	홀	짝

≈

곱	1	−1
1	1	−1
−1	−1	1

  - 셋 모두 '사실상 같다', 이름만 다를 뿐!

‘본질적으로 같다’

- (G,*), (G′,*′); group, $\psi : G \to G'$; ‘이름 바꾸기’
- G 와 G′ 이 이름만 다르고 ‘본질적으로 같다’
  - G 의 연산표와 G′ 의 연산표 완전히 겹친다
  - $\psi(x) = x'$ 으로 표기하면, $\psi(g*h)=g'*'h'=\psi(g)*'\psi(h)$
  - ‘연산해서 이름 바꾼 것’ = ‘이름 바꿔 연산한 것’

G	g	h	⋯
g	g*g	g*h	⋯
h	h*g	h*h	⋯
⋮	⋮	⋮	⋱

ψ → ≈

G′	g′	h′	⋯
g′	g′*′g′	g′*′h′	⋯
h′	h′*′g′	h′*′h′	⋯
⋮	⋮	⋮	⋱

Isomorphism

- $\psi : X \to Y$ is an isomorphism iff
  - ψ; bijection(일대일 대응관계)
  - '연산해서 이름 바꾼 것' = '이름 바꿔 연산한 것'
    - X,Y; group $\Rightarrow \psi(g*h) = \psi(g)*\psi(h)$
    - X,Y; ring $\Rightarrow \psi(x+y) = \psi(x)+\psi(y)$, $\psi(xy) = \psi(x)\psi(y)$
    - X,Y; 벡터공간 $\Rightarrow \psi(v+w) = \psi(v)+\psi(w)$, $\psi(av) = a\psi(v)$
- $X \approx Y$, if $\exists$ an isomorphism $\psi : X \to Y$
  - Say "X is isomorphic to Y"

유한체의 유일성

- [Theorem B]

  F, F'; finite field, $|F| = |F'| \Rightarrow F \approx F'$

  - '원소수가 같은 유한체는 본질적으로 같다'
  - 물론, [field isomorphism]=[ring isomorphism]
    - Field 는 특수한 ring
  - 증명; 1개월……, splitting field……

유한체의 유일성

- $F = \mathbb{F}_2[t]_{t^3+t+1}$, $K = \mathbb{F}_2[t]_{t^3+t^2+1}$; $|F| = 8 = |K|$
  - Recall; $F^\times = \langle t \rangle$, $K^\times = \langle s \rangle$
- Find an isomorphism $\psi : F \to K$?
  - If we put $\psi(t) = \beta$, must have $\psi(t^a) = \psi(t)^a = \beta^a$, $(a \in N)$
    - 물론 $\psi(0) = 0$, $\psi(1) = 1$
  - Must have $K^\times = \langle \beta \rangle$
    - $\psi : F^\times \to K^\times$ is a (multiplicative) group isomorphism
    - $K^\times$의 generator $s, s^2, \ldots, s^6$, $(\varphi(7)$-개)
  - $\psi(t)$ 의 후보 $s, s^2, \ldots, s^6$

유한체의 유일성

- 시도; (가장 멋있게) $\psi(t) = s$ 로 정의하면
  - $\psi(t+1) = \psi(t^3) = s^3 = s^2+1 \neq s+1 = \psi(t)+\psi(1)$
  - 실패……
- Want $0 = \psi(0) = \psi(t^3+t+1) = \psi(t)^3+\psi(t)+\psi(1)$
  - $s, s^2, \ldots, s^6$ 중 $x^3+x+1=0$ 의 root 은 s^3, s^5, s^6
- 예를 들어, $\psi(t) = s^3$ 으로 정의하면
  - $\psi(t+1) = \psi(t^3) = (s^3)^3 = s^2 = s^3+1 = \psi(t)+\psi(1)$, $(s^7 = 1)$ OK
  - ψ 는 원하던 isomorphism
- 정말?? 하루 더 필요……
  - Isomorphism Extension Theorem

연습문제

(1) 분수(유리수)의 덧셈, 곱셈이 well-defined 되어 있음을 보여라. (초등학교 때 확인 안 한 사람만.)

(2) If d is a common divisor of a, $b \in \mathbb{Z}$, show that d divides (a,b).

(3) Show that $\underline{a} = \underline{b} \in \mathbb{Z}_n$ implies $(a,n) = (b,n)$.

(4) E/F; field extension이면, E는 F-vector space임을 확인하라.

(5) 인수 정리의 증명에서 '$t = c$ 를 대입한다'는 말은 무슨 뜻?

(6) 왜 $\deg(0) = -\infty$ 라고 정의할까?

(7) $F[t]_{f(t)}$-위에 F-상수곱이 well-defined 되어 있음을 보여라.

(8) $F[t]_{f(t)}$ 의 unit group 을 묘사하라.

연습문제

(9) [슬라이드 52] $(\mathbb{F}_{16})^{\times} = \langle t+1 \rangle \neq \langle t \rangle$ 를 확인하라.

(10) [슬라이드 53] $f(t) = t^3+2t+1 \in \mathbb{F}_3[t]$ 는 irreducible?

(11) $6 \cdot 1_F = (2 \cdot 1_F) \cdot (3 \cdot 1_F)$ 임을 보여라.

(12) $0 < k < p$ 이면, ${}_pC_k$ 는 p 의 배수임을 보여라.

(13) [슬라이드 86] s^3, s^5, s^6 은 $x^3+x+1=0$ 의 root 임을 보여라.

(14) [슬라이드 79] 주어진 $\varepsilon : \mathbb{F}_5 \to \mathbb{F}_5$ 를 다항함수로 나타내라.

(15) Show $\mathbb{F}_q[t]/(t^q-t) \approx \{\varepsilon : \mathbb{F}_q \to \mathbb{F}_q \mid \varepsilon;$ 다항함수$\}$ as rings. (First define a ring structure on the right-hand side set.)