Number Theoretic Algorithms

More about Fields

March 27, 2019

와, 저는 여러분들이 대수적 구조에 이렇게 관심이 있을 줄 몰랐어요. 그래서 사실 되게 대강 준비해 갔는데, 잘 참여해 주시고 질문도 많이 해 주셔서 감사합니다. 이 자료는 제가 1주차 스터디를 진행하면서 체에 대해서 답변을 **잘못했거나** 완전히 설명하지 못한 부분들에 대해서 정확하게 설명드리고자 작성된 자료입니다.

설명을 위해서는 대수학적 지식이 많이 필요하기에, 관련 사실을 언급하고 대강 넘어갈 것이니, 미심쩍거나 이해가 되지 않는 부분이 있으시면 적극적으로 질문해 주셔도 됩니다!

1 원소의 개수

유한 체의 원소의 개수는 **order**라고 부릅니다.[1] 또 유한 체의 원소의 개수와 밀접한 관련이 있는 **characteristic**이라는 단어가 있는데, field F의 characteristic은

$$\exists n \in \mathbb{N}^+, \quad n := n \cdot 1 = \underbrace{1+1+\cdots+1}_{n \text{ times}} = 0$$

이라면 그런 n 중 최솟값이고, 아니면 0입니다.[2]

관습적으로, 자연수 n에 대해,

$$\underbrace{1+1+\cdots+1}_{n \text{ times}} = n \cdot 1 = n \in F$$

로 씁니다. 혼동의 여지가 있으면 $n \cdot 1 \in F$, $n \in \mathbb{N}$으로 쓰고, 없으면 막 섞어서 씁니다.

characteristic이 0이면 "체가 무한하다" 이외에 얘기해 주는 것이 딱히 없지만, characteristic이 0이 아니면 재밌는 얘기를 할 수 있습니다. 우리의 첫 번째 시작점은 유한 체의 characteristic이 소수라는 것입니다.

Claim 1. *유한 체의 characteristic은 소수이다.*

Proof. characteristic을 n이라 하면, 유한 체이므로 $n \neq 0$입니다. 또 $n \neq 1$이므로,[3] n은 소수이거나 합성수입니다. n을 합성수라 가정하면, $n = pm$이고 p는 소수, m은 2 이상의 자연수로

[1] 다른 대수적 구조에서도 계속 쓰이는 용어이기 때문에, 언급하고 넘어갑니다.
[2] 최솟값이 존재하느냐 같은 복잡한 얘기는 하지 맙시다.
[3] $1 \neq 0$은 체의 **공리**입니다.

쓸 수 있습니다. 이때,

$$\begin{aligned} p \cdot m &= (\underbrace{1+1+\cdots+1}_{p \text{ times}}) \cdot (\underbrace{1+1+\cdots+1}_{m \text{ times}}) \\ &= \underbrace{1 \cdot 1 + 1 \cdot 1 + \cdots + 1 \cdot 1}_{pm \text{ times}} \\ &= \underbrace{1+1+\cdots+1}_{n \text{ times}} = 0 \end{aligned}$$

이고, $p \neq 0$이라면 양변에 p^{-1}를 곱해 $m = 0$을 얻을 수 있으므로 $p = 0$이거나 $m = 0$인데, $p < n$이고 $m < n$이므로 어느 쪽이나 n의 최소성에 모순입니다. □

따라서, characteristic은 p로 쓰겠습니다.

characteristic이 소수 p로 존재하면 체 F로부터 **물려받은** 연산에 대해 $\mathbb{Z}_p = \langle 1 \rangle$ 체를 구성할 수 있습니다. 이 체 위에서 곱셈을 $\mathbb{Z}_p$에서만 생각해서 상수곱으로 삼으면, F over $\mathbb{Z}_p$를 vector space로 인식할 수 있고 $\dim F =: n$을 얘기할 수 있습니다. 따라서...

Claim 2. *임의의 유한 체 F와 F의 characteristic p에 대해 $|F| = p^n$을 만족하는 양의 자연수 n이 존재한다.*

증명은 $\dim F = n$으로 두고, 개수가 p^n 이상임을 vector space의 coordinate를 이용해서 증명하고, p^n 이하임을 basis의 개수가 n임을 이용해서 증명하면 됩니다.

따라서, 원소의 개수가 6개인 체는 존재하지 않습니다.

2 Classification of Finite Fields

우리는 모든 대수적 구조의 실체를 절대 공부할 수 없습니다. 실례를 **배우기** 시작하면 당장 집합만 해도 사과들의 집합, 오렌지들의 집합을 모두 다 공부해야 하므로, 시간 낭비입니다.[4] 그래서 대수학의 시작인 선형대수학에서는 "사실상 같다"를 수학적으로 엄밀하게 정의하는 데 많은 시간을 들입니다.

그리고 "사실상 같은" 대수적 구조들을 하나로 인식합니다. 이 말은 유식하게는 up to isomorphism 어쩌구 하는 말들인데, 아무튼 분류해 놓고 이 분류를 열심히 공부합니다. 예를 (많이) 들면:

- 집합의 경우 up to isomorphism 같은 것은 **cardinality**에 의한 분류입니다. 집합에는 특수한 대수적 구조가 없으므로, 크기가 같으면 같은 집합이 되겠죠.
    - 따라서, cardinality가 1인 집합은 모두 같은 것으로 봅니다. 이 덕에 우리는 사과의 집합, 오렌지의 집합, 여러분 한 명의 집합을 일일이 공부하지 않고, cardinality가 1인 집합을 배우고 다른 집합에 대해서 더 공부해 볼 수 있습니다.[5]

[4] 실례를 드는 것이 나쁘다는 것은 아닙니다. 다만 이것은 어디까지나 추상적 구조를 이해하기 위한 수단이 되어야지, 그 자체가 목적이 되어서는 안 된다는 말입니다.

[5] 우리는 심지어 cardinality가 1인 집합, 2인 집합을 일일이 배우지도 않습니다.

  - 여러분은 모두 $\mathbb{N}$과 $\mathbb{Q}$가 cardinality가 같고, $\mathbb{N}$과 $\mathbb{R}$은 cardinality가 다르다는 얘기를 들어보셨을 겁니다. 이 말은 $\mathbb{N}$과 $\mathbb{Q}$를 집합으로서 구분할 수 있는 방법은 **없다**는 의미이고, $\mathbb{N}$과 $\mathbb{R}$는 다른 구조를 모두 생각하지 않고 집합으로서만 생각해도 다른 점이 보인다는 의미입니다.

- 체 F를 고정했을 때, vector space over F의 경우 up to isomorphism 같은 것은 **dimension**에 의한 분류입니다.[6]

- 1983년까지 finite simple group을 분류하기 위한 수많은 수학자들의 노력이 있었습니다. 결론적으로 simple groups of prime order, alternating groups, the Lie groups, sporadic groups와 Tits group으로 분류되었습니다.

  - simple group은 연산을 물려받은 subgroup 중 **아름다운** 녀석들이 자기 자신과 제일 작은 녀석밖에 없는, 가장 단순한 group입니다.[7]

그리고, 우리는 유한 체를 분류하려고 합니다. 먼저, Fermat의 소정리를 확장합니다.

Claim 3 (Fermat)**.** *임의의 원소 $a \in F$에 대해, $|F| = p^n$으로 두고 p는 소수라 하면, $a^{p^n} - a = 0$이다.*

Proof. 1주차 자료 6번의 증명 과정은, 사실 $\mathbb{Z}_p$가 체라는 것 이외에 어떠한 다른 특성도 사용하지 않습니다. 따라서 이 증명의 $\mathbb{Z}_p$를 임의의 체 F로 바꾸어 읽으면 그대로 $a \neq 0$이면 $a^{p^n-1} = 1$이라는 사실의 증명이 됩니다. 이제 다항식 조작을 통해 남은 부분은 쉽게 증명할 수 있습니다. □

그런데 왜 굳이 $|F| = p^n$을 고집하는 걸까요? 이 특수한 형태가 바로 up to isomorphism 분류하는 데 큰 도움을 주기 때문입니다.[8] 이제 곱셈에 대한 생성원을 찾기 위해 다음을 받아들입니다:

> 다항식 $x^{p^d} - x$는 $\mathbb{Z}_p$에서 차수가 d 이하인 모든 기약다항식들의 곱이다.

증명은... 제가 초등적 증명을 찾고 있습니다. 아마 이 다항식이 왜 이런 특성을 가지는지가 절실하게 필요해질 때는 초등적 증명이 되어 있으리라 생각합니다. 일단 믿어 주세요.

이를 이용해서 생성원에 대한 얘기를 해 봅시다. 생성원은 order가 field의 order보다 1 작은 원소를 얘기합니다.

Claim 4. *유한 체 F에는 생성원 g가 존재한다.*

Proof. $|F| = p^n$이라 하고, $p^n - 1 =: q$의 소인수분해 $p_1^{e_1} \cdots p_k^{e_k}$가 주어져 있다고 합시다. order가 $p_i^{r_i}$인 원소들이 존재함을 보이면, 그 원소의 곱이 g가 됩니다. 이를 위해서 $x^{q/p_i} - 1$의 해가 $(p^n - 1)$개보다 작음을 이용합니다. 따라서 이 다항식의 해가 아닌 원소 a_i가 주어져 있다면, $b_i := a_i^{q/(p_i^{e_i})}$가 우리가 찾는 원소가 됩니다. □

[6] dimension을 얘기하려면 Axiom of Choice를 믿어야 하나, 우리는 필요한 모든 공리를 믿습니다.

[7] field의 경우 $\mathbb{Z}_p$와 비슷합니다. $\mathbb{Z}_p$는 subfield가 자기 자신밖에 없습니다.

[8] 심지어 쓸 수 있는 공리가 훨씬 적은 group에서도 이 특수한 형태만큼은 너무나도 잘 다룰 수 있는 아름다운 정리가 있습니다. (Sylow)

이제 모든 준비가 끝났고, 유한 체를 분류해 봅시다!

Claim 5. *두 유한 체 F_1과 F_2가 $|F_1| = |F_2|$이면, $F_1 \simeq F_2$이다.*[9]

Proof. $|F_1| = |F_2| = p^n$이라고 합시다.

F_1에서 아무 생성원 g를 찾습니다. g는 $x^{p^n} - x$ 다항식의 해가 됩니다. 이 다항식 중 F_1에서 $(x - g)$를 포함하는 $\mathbb{Z}_p$에서의 기약다항식 $m(x)$를 잡습니다. 그러면 $m(x)$는 F_1에서 생성원이므로 $\mathbb{Z}_p$ 위에서 x^k를 $m(x)$로 나눈 나머지는 $(p^n - 1)$개입니다.

따라서 F_2에서 $m(x)$의 아무 해 h를 잡으면, h는 F_2의 생성원이 됩니다. 이제 $\varphi : F_1 \to F_2$를 $\varphi(g^i) = h^i$로 두면 φ가 우리가 찾는 isomorphism입니다. □

결론만 다시 얘기하면, 유한 체들은 개수만 같으면 같은 체로 바꿀 수 있다는 의미입니다! 따라서, $\mathbb{F}_n$의 표기를 사용할 수 있고, 실제로도 이 표기법은 많이 쓰입니다.

그러나 우리가 $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$의 표기를 고집하는 이유는 이 구조는 덧셈에 대해서 cyclic group이 되기 때문입니다.[10] 또 다항식이나 생성원에 대해서도 더 많은 얘기를 해 볼 수 있습니다. 한마디로 얘기하면 "이쁘기" 때문에,[11] 우리는 일단 $\mathbb{Z}_p$만을 생각합니다.

3 문제

1. **Claim 2**의 증명은 Sketch of Proof 수준입니다. 엄밀하게 증명하세요.
2. **Claim 4**의 증명은 Gap이 많습니다. 모두 채우세요.
3. **Claim 5**의 증명은 Sketch of Proof 수준입니다. 엄밀하게 증명하세요.

[9] F_1 is isomorphic to F_2라고 읽으시면 됩니다.

[10] notation도 group을 쓸 때 얘기하는 notation입니다.

[11] 그리고 대수적 구조에 관한 지식이 전무하기 때문에. 우리가 대수학의 언어를 알고 있다면, 훨씬 넓은 공간에서 훨씬 강력한 얘기들을 해 볼 수 있습니다.