Roots of unity

January 19, 2017

Contents

1 복소수란 무엇인가?

어쩌면 필자가 학생 여러분들을 과소평가하고 있는지도 모른다. 하지만 적어도 필자는 단순히 $i = \sqrt{-1}$이라는 사실을 안 이후에 복소수가 무엇인지 깨닫기까지 수년의 시간이 걸렸다. 실수 체계를 복소수로 확장함으로써 생기는 이점에는 여러가지가 있겠지만, 그 중 몇 가지만, 특히 필자에게 감동적으로 다가왔던 성질을 중심으로, 소개하고자 한다. 복소수를 잘 아는 학생들도 중요한 성질들을 되새길 겸 소설책 읽듯 읽어주기를 바란다.

1.1 방정식의 근으로서

옛날 사람들은 방정식을 푸는 일을 참 좋아했다. 차수가 1인 다항식 방정식은 아주 쉽게 풀 수 있었고, 차수가 2인 다항식 방정식도 푸는 방법을 개발했다. 하지만 항상 한 개의 해를 갖는 1차 방정식과 다르게 2차 방정식은 해를 (중근을 포함해서) 2개 가지는 경우가 있었고 없는 경우도 있었다. 대표적으로 $x^2 + 1 = 0$은 해를 갖지 않는다. 이렇게 2차 방정식이 해의 개수에 따라 두 부류로 나뉘는 것에 불만을 갖기 시작한 사람들이 늘었고, 어느 순간 사람들은 $x^2 + 1 = 0$가 사실 두 근을 갖는다고 가정해보기 시작했다. 만약 x가 해가 되면 $-x$도 해가 되어야 하므로 다음과 같이 정의해보았다.

정의 1.1.1. 방정식 $x^2 + 1 = 0$의 두 근을 $i, -i$로 정의하자.

그러면 당연히 $i^2 = (-i)^2 = -1$이 성립할 것이다. 여기서 의문을 제기하는 사람도 있을 것 같다: i와 $-i$를 어떻게 구분할 수 있을까? 만약 내 옆에 있는 친구도 $x^2+1 = 0$의 두 근을 i와 $-i$로 정의했을 경우, 내 i와 친구의 i가 같을지, 아니면 내 i와 친구의 $-i$가 같을 것인지 절대로 알 수 없는 것 아닌가? 실제로 i와 $-i$를 구별하는 방법은 전혀 없다. 이상하게 느껴질 수도 있겠지만 i와 $-i$는 다른 수지만 명확히 분리해내는 거은 불가능하다. 하지만 그렇게 때문에 내가 정의한 i가 다른 i와 같다고 가정해도 무방한 것이다. 이것이 갈루아 이론이라는 아주 멋진 이론의 밑그림이 되는 발상이다. 잠시 이야기가 옆길로 새었다. 한 줄로 정리하자면, 여러분들은 이런 걱정을 할 필요가 없고, 그냥 i는 i라고 편하게 생각하고 살아가면 된다.

이제 i가 있게 된 이상, 여기에 실수를 곱해볼 수도 있다. 예를 들어 $2 \times i = 2i$는 $x^2 + 4 = 0$의 근이 될 것이라고 생각할 수 있다. 여기에 실수를 더해보는 것도 가능할 것이다. 즉, $3 + 2i$와 같은 것도 i로부터 파생되는 '수'라고 생각해볼 수 있다. 두 '수'를 곱하면 어떤 일이 일어날까? 만약 $a + bi$와 $c + di$를 곱하면

$$(a + bi)(c + di) = ac + bci + adi + bdi^2 = (ac - bd) + (bc + ad)i$$

가 되어 또 다시 $x + yi$ 꼴의 수가 된다. 이것은 2차 항이 0차 항도 될 수 있기 때문에 나타나는 현상이다. 또한 한 수를 다른 수로 나누는 행위도 가능하다.

$$\frac{1}{a+bi} = \frac{a-bi}{(a+bi)(a-bi)} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$$

이므로 $a=b=0$만 아니라면 $a^2+b^2\neq 0$이 되어 나눗셈도 가능해진다. 그러므로 집합

$$\mathbb{C}=\{a+bi : a,b\in\mathbb{R}\}$$

을 정의하고 이 집합의 원소들을 **복소수(complex numbers)**라고 부른다면 다음이 성립할 것이다.

정리 1.1.2. *복소수들의 집합 $\mathbb{C}$는 덧셈, 뺄셈, 곱셈, 0이 아닌 수에 의한 나눗셈 모두에 대해 닫혀있다.*[1]

그럼 이제 웬만한 2차방정식은 풀 줄 알게 된다. 예를 들어 $x^2-2x+3=0$과 같은 방정식이 있다고 하면, 근의 공식에 의해

$$x=1\pm\sqrt{1^2-3}=1\pm\sqrt{-2}=1\pm\sqrt{2}\sqrt{-1}=1\pm\sqrt{2}i$$

이 된다. 판별식이 음수가 아니면 그냥 $\sqrt{\ }$를 사용하고, 음수면 -1을 뺀 후 $\sqrt{-1}$을 i로 처리하면 우리가 아는 2차방정식의 근의 공식을 항상 적용할 수 있을 것이다.

하지만 여기서 문제가 있다. 우리가 '수'로 생각하는 것들이 늘어남에 따라 2차 다항식으로 간주하는 것들도 따라서 생기기 때문이다. 예를 들어 $x^2-i=0$와 같은 방정식도 이제는 2차방정식의 범주 안에 속한다고 봐야 한다. 하지만 이 방정식을 푸는 방법은 배운 적이 없는 것 같다. 그러면 다음과 같이 다시 또 정의를 할까?

"방정식 $x^2-i=0$의 두 근을 $j,-j$로 정의하자."

사실 그럴 필요가 전혀 없다. 이 방정식은 $\mathbb{C}$ 안에서 이미 두 개의 근을 갖기 때문이다. $(a+bi)^2=i$라 한 후 전개하면 $a^2-b^2=0$과 $2ab=1$을 얻는데, 이 연립방정식을 풀면 $(a,b)=(\sqrt{2}/2,\sqrt{2}/2),(-\sqrt{2}/2,-\sqrt{2}/2)$로 정확히 두 개의 근을 가짐을 확인할 수 있다! 놀라움은 여기서 멈추지 않는다.

연습문제 1.1.A. 방정식 $x^3=i$의 근을 모두 구하여라.

풀어보면 알겠지만, 위의 방정식은 3개의 근을 갖는다. 더 신기한 사실은, 이것이 모든 다항식에 대해 성립한다는 것이다. 임의로 다항식 하나를 적어보자.

$$x^5+43x^4+3x^3+2016x^2+8x+30=0$$

이 다항식은 다음과 같이 인수분해하여 적을 수 있다.

$$(x+43.974)(x+0.002+0.122i)(x+0.002-0.122i)(x-0.489+6.752i)(x-0.489-6.752i)=0$$

복소수들은 $ab=0$이면 $a=0$ 또는 $b=0$인 성질을 가지고 있으므로[2] 위 방정식의 근은 $x=-43.974$, $-0.002\pm 0.122i$, $0.489\pm 6.752i$로 정확히 다섯 개임을 알 수 있다. 실제로 다음이 성립한다.

[1] 이러한 성질을 가진 집합을 체(field)라고 부른다.

[2] 만약 $a\neq 0$이면 양 변을 a로 나누어 $b=0$을 얻을 수 있다.

정리 1.1.3 (대수학의 기본 정리)**.** *차수가 d인 방정식은 $\mathbb{C}$ 안에서 (중근을 포함하여) 정확히 d개의 근을 갖는다. 바꿔 말하자면, 계수가 복소수인 d차 다항식은 항상 d개의 일차식의 곱으로 인수분해 가능하다.*

이 정리는 증명이 매우 까다로운 관계로 그냥 사실로 받아들이는 편이 나을 것이다. (시험에서도 증명 없이 사용해도 될 것이라 믿는다.) 그렇지만 증명을 모르는 학생에게도 이 정리의 신비함에 대한 공감은 필요하다. 복소수를 정의할 때, 우리는 단순히 $x^2 + 1 = 0$이라는 아주 임의적으로 보이는 방정식의 근을 추가하기만 했다. 그런데 그 결과물은 모든 실계수 다항식이 근을 갖게되는 집합이며, 심지어 모든 복소수계수 다항식도 정확히 차수개의 근을 갖는다! 이것이 왜 그리 신기한 현상인지 모르겠다면 지금까지 한 이야기에서 실수들의 집합 $\mathbb{R}$을 유리수들의 집합 $\mathbb{Q}$로 바꿔보아라. 수 i 하나만 추가해서 모든 유리계수 다항식이 근을 가지도록 하는 것은 택도 없는 일이다.

여담으로, 차수가 d인 다항식이 근을 d개보다 많이 가질 수는 없을까? 복소수 x_1가 다항식 $p(x)$의 근이 된다면, 흔히 조립제법이라고 불리는 성질 덕분에 $p(x) = (x-x_1)p_1(x)$와 같이 인수분해된다. 그 다음 x_2가 다항식 $p(x)$의 다른 근이라면, $p_1(x)$의 근도 될 것이므로 $p(x) = (x-x_1)p_1(x) = (x-x_1)(x-x_2)p_2(x)$로 인수분해된다. 이런식으로 다항식 $p(x)$의 근이 $x_1, \ldots, x_r$이라면

$$p(x) = (x - x_1) \cdots (x - x_r)p_r(x)$$

인 다항식 $p_r(x)$이 될 것이고, 이 식에서 양 변의 차수를 비교해보면 $\deg p = r + \deg p_r \geq r$을 얻는다. 그렇기 때문에 차수가 d인 다항식은 (중근을 포함해서) 최대 d개의 해밖에 갖지 못한다.

연습문제 1.1.B. 임의의 실계수 다항식 $f(x)$는 차수가 2 이하인 실계수 다항식의 곱으로 나타낼 수 있음을 보여라.[3]

마지막으로 두 수 i와 $-i$를 구별하지 못한다는 성질에 대한 부연설명을 하고자 한다. 만약 위의 연습문제를 풀지 못했다면 이 부분을 읽고 다시 풀어보길 바란다. $f(x+yi) = x - yi$인 전단사함수 $f : \mathbb{C} \to \mathbb{C}$를 생각해볼 수 있다. 쉽게 말하자면, 이 함수는 i를 모두 $-i$로 바꿔버리는 함수이다. 이 함수는 흔히 **복소켤레**(**complex conjugate**)라고 부르고, f라는 표기 대신 $\overline{x + yi} = x - yi$와 같이 위에 선분을 그리는 방법이 주로 사용된다.

연습문제 1.1.C. 함수 $\overline{\bullet} : \mathbb{C} \to \mathbb{C}$이 임의의 $a, b \in \mathbb{C}$에 대해 다음을 만족함을 보여라.

- $\overline{a+b} = \overline{a} + \overline{b}$, $\overline{ab} = \overline{a}\overline{b}$.
- $\overline{\overline{a}} = a$.
- $\overline{a} = a$일 필요충분조건은 $a \in \mathbb{R}$.

[3]힌트 : 우선 f를 차수가 1인 복소계수 다항식으로 인수분해해라. 그 다음 i와 $-i$를 구별할 수 없다는 성질을 이용하여라.

위의 세 성질에 의해 발생하는 재미난 현상들이 있다. 예를 들어 $a+\overline{a}$의 켤레는 $\overline{a}+\overline{\overline{a}} = a+\overline{a}$가 되어 $a+\overline{a}$는 항상 실수이다. 마찬가지로 $a\overline{a}$도 항상 실수이다. (갈루아 이론을 아는 학생들은 필자가 왜 이런 이야기를 하는지 눈치챌 수 있을 것이다.) 또한 $z \in \mathbb{C}$가 어떤 실계수 다항식 $p(x)$의 근이 된다면, $\overline{z}$도 근이 된다. 이것은 $p(x) = a_d x^d + \cdots + a_1 x + a_0$라면

$$p(\overline{z}) = a_d \overline{z}^d + \cdots + a_1 \overline{z} + a_0 = \overline{a_d z^d + \cdots + a_1 z + a_0} = \overline{p(z)} = 0$$

가 되기 때문이다.

연습문제 1.1.D. 임의의 실수 x에 대해 $f(x) \geq 0$이 성립하는 실계수 다항식 $f(x)$가 있다. 이때 두 실계수 다항식 $g(x)$와 $h(x)$가 존재하여 $f(x) = g(x)^2 + h(x)^2$이 됨을 보여라.

1.2 평면 위의 점으로서

복소수 하나는 $x+yi$와 같은 꼴을 가지므로 두 개의 실수에 대한 정보를 담고 있다. 따라서 복소수 하나에 대해, 평면 위의 점을 하나 대응시켜줄 수 있을 것이다. 정확하게는 아래와 같이 복소수와 평면 위의 점을 대응시키자.

$$x+yi \in \mathbb{C} \quad \Longleftrightarrow \quad (x,y) \in \mathbb{R}^2$$

편의상 함수 $\Re, \Im : \mathbb{C} \to \mathbb{R}$을 다음과 같이 정의하자.

$$\Re(x+yi) = x \qquad \Im(x+yi) = y$$

그러면 복소수와 점 사이의 대응을 $z \in \mathbb{C} \Longleftrightarrow (\Re(z), \Im(z)) \in \mathbb{R}^2$으로 표현할 수도 있다.[4] 여기서 $\Re(z)$와 $\Im(z)$를 각각 z의 **실수부**(**real part**)와 **허수부**(**imaginary part**)라 부른다.

복소수를 평면 위의 점으로 생각했을 때 어떠한 장점이 있을까? 우선 복소수의 합부터 살펴보자. 복소수 $0, a, b$에 해당하는 점을 O, A, B라 하자. 이때 $a+b$에 해당하는 점 X는 $OAXB$가 평행사변형이 되도록 하는 점이다. 즉, 복소수를 더하는 연산은 벡터를 더하는 연산과 동일하다.

연습문제 1.2.A. 복소수 a, b, c에 대응되는 점을 A, B, C라 하자. 이때 사각형 $CAXB$가 평행사각형이 되도록 하는 점 X에 해당하는 복소수를 a, b, c로 표현하여라.

그렇다면 복소수의 곱은 어떻게 표현될까? 복소수 $0, 1, a, b$에 해당하는 점을 O, I, A, B라 하고, ab에 해당하는 점을 X라 하자. 이때 신기하게도 닮음관계

$$\triangle OIA \sim \triangle OBX, \qquad \triangle OIB \sim \triangle OAX$$

[4] $\mathbb{C}$와 $\mathbb{R}^2$ 사이에 일대일 대응이 있다고 해서 $\mathbb{C}$ 위의 기하학과 $\mathbb{R}^2$ 위의 기하학이 같게 행동하는 것은 아니다. 우선 $\mathbb{C}$는 1차원 공간이고 $\mathbb{R}^2$은 2차원 공간이기 때문에 근본적인 차이가 존재한다. 예를 들어 $\mathbb{CP}^1$은 구와 같이 생겼지만 $\mathbb{RP}^2$는 괴상하게 생겼다.

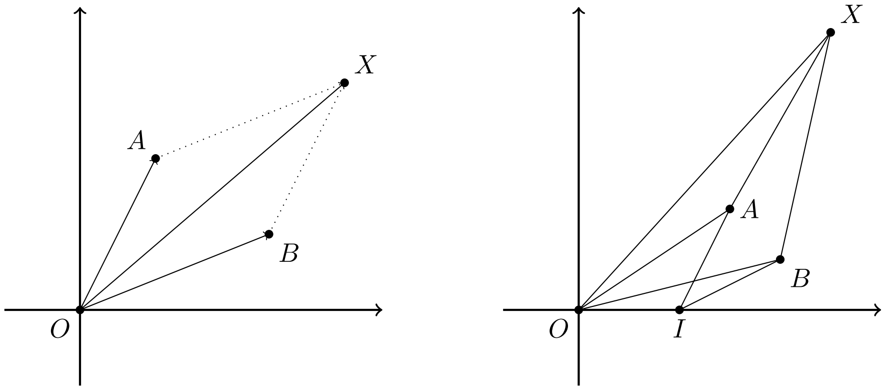

Figure 1: 두 복소수 a와 b를 합할 때와 곱할 때

가 성립한다. 이것은 a와 b의 좌표를 설정하고 길이를 가지고 열심히 계산해보면 증명할 수 있다.

연습문제 1.2.B. 위의 닮음이 성립함을 증명하여라.

연습문제 1.2.C. 복소수 $0, a, b, c$에 해당하는 점을 O, A, B, C라 하자. 이때 $\triangle OCA \sim \triangle OBX$가 되는 점 X에 대응되는 복소수를 a, b, c로 표현하여라.

이렇듯 복소수의 곱은 결국 회전닮음변환과 같다. 그러므로 복소수의 기하학에서 '각'의 보존이 아주 중요한 역할을 한다. 복소수의 기하학을 이 통신강좌에서 다룰 생각은 눈꼽만큼도 없지만, 연습삼아 다음 문제들을 풀어보자.

연습문제 1.2.D. 서로 다른 세 점 A, B, C에 대응되는 복소수를 a, b, c라 하자. 이때 A, B, C가 한 직선 위에 존재할 필요충분조건은

$$\frac{a-b}{b-c}$$

가 실수인 것임을 보여라.

연습문제 1.2.E. 서로 다른 네 점 A, B, C, D에 대응되는 복소수를 a, b, c, d라 하자. 이때 A, B, C, D가 한 원 위에 또는 한 직선 위에 존재할 필요충분조건은

$$\frac{(a-b)(c-d)}{(a-d)(b-c)}$$

가 실수인 것임을 증명하여라. (이 명제에서 $d = \infty$를 대입하면 이전 문제가 되는 것을 눈치챘는가?)

연습문제 1.2.F. 복소수 a, b, c, d가 $ad - bc \neq 0$을 만족한다고 하자. 변수 $z \in \mathbb{R}$가 실수축 위에서 움직일때,

$$\frac{az+b}{cz+d}$$

의 자취는 직선 또는 원에서 1개 또는 0개의 점을 뺀 집합이 됨을 보여라. (자취가 깔끔하지 않아 찜찜한 사람들을 위해: 만약 z에 ∞을 대입할 수 있다면, 자취가 항상 원이거나 직선에 ∞을 추가한 집합이 됨을 보여라.)

연습문제 1.2.G. 복소수 $0, z = x + yi$에 대응되는 점을 O, Z라 하자. 이때 $z\bar{z} = x^2 + y^2$임을 보여라. 따라서 $OZ = \sqrt{x^2 + y^2} = \sqrt{z\bar{z}}$가 된다. 복소수 z의 **절댓값(absolute value)**를 $|z| = OZ = \sqrt{z\bar{z}}$로 정의하자. 이때 임의의 복소수 a, b에 대해 $|ab| = |a||b|$임을 보여라.

1.3 길이와 방향으로서

복소수 a가 주어져있을 때, 이것을 거듭제곱해야하는 상황이 생기기 마련이다. 하지만 i라는 수가 행동하는 방식이 마냥 탐탁한 것은 아닌지라 $x + yi$의 거듭제곱을 깔끔하게 표현하기는 힘들다. 그러나 우리에겐 $\mathbb{C}$와 $\mathbb{R}^2$ 사이의 대응이라는 강력한 도구가 있고, 그 위에서의 복소수의 곱셈에 대한 나름의 직관적인 해석을 가지고 있다. 이 곱셈은 사실상 직교좌표보다는 극좌표계에 더 어울린다. a의 절댓값과 b의 절댓값을 곱하면 ab의 절댓값이 되고, a와 x축이 이루는 각과 b와 x축이 이루는 각을 *합하면* ab와 x축이 이루는 각이 된다. 따라서 복소수의 극좌표적 해석이 절실하게 필요함을 느낀다.

복소수 $z \neq 0$이 있을 때, $z/|z|$는 절댓값이 1이므로 좌표평면 상에 원점을 중심으로 가지는 단위원 위에 놓인다. 그러므로

$$z = |z|(\cos\theta + i\sin\theta)$$

인 각 θ가 존재할 것이다. 이 각을 z의 **편각(argument)**라 부르고 $\arg z$로 표기한다. 기하학적으로는 양의 x축 반직선을 반시계방향으로 얼마나 회전해야 z를 지나게 될 것인가에 대한 정보이다. 물론 θ를 $\theta + 2\pi$로 대체해도 같은 식이 성립한다. 그러므로 복소수의 편각은 하나의 실수로 결정된다기보다는, 실수이되 2π의 정수배만큼 차이나는 것은 같다고 생각하는 편이 옳다.

어째든 $z = |z|(\cos\theta + i\sin\theta)$와 $w = |w|(\cos\phi + i\sin\phi)$가 있을 때, 이 둘의 곱은

$$zw = |z||w|(\cos(\theta + \phi) + i\sin(\theta + \phi))$$

로 표현될 것이다.

연습문제 1.3.A (드 무아브르의 법칙). 임의의 θ과 음 아닌 정수 n에 대해 다음 등식을 증명하여라.

$$(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta$$

이것으로도 충분하지만, 여러모로 더욱 편리한 표기법을 소개하겠다. 함수 exp는

$$\exp(x) = e^x = 1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \cdots + \frac{x^n}{n!} + \cdots$$

와 같은 급수로 정의된다. 이 식에서 x에 ix를 대입해보자. 그러면

$$e^{ix} = 1 + ix + \frac{i^2x^2}{2} + \cdots = \left(1 - \frac{x^2}{2} + \frac{x^4}{24} - \cdots\right) + i\left(x - \frac{x^3}{6} + \cdots\right) = \cos x + i \sin x$$

가 공교롭게도 성립한다. 이 식을 이용하여 생각하면 등식 $e^{i\theta}e^{i\phi} = e^{i(\theta+\phi)}$가 조금 더 가깝게 다가올지도 모른다. 거꾸로 cos과 sin을 exp를 이용하여 계산할 수도 있다. $e^{i\theta} = \cos\theta + i\sin\theta$이고 $e^{-i\theta} = \cos\theta - i\sin\theta$이므로

$$\cos\theta = \frac{e^{i\theta} + e^{-i\theta}}{2}, \qquad \sin\theta = \frac{e^{i\theta} - e^{-i\theta}}{2i}$$

이다. 이 통신강좌에서는 앞으로 cos과 sin을 일절 사용하지 않겠다. 한편으로는 여러분이 $e^{i\theta}$와 같은 기호에 익숙해지라는 의도가 있고, 다른 한편으로는 이 함수를 다루는 것이 삼각함수보다 훨씬 편하기 때문이다. 우선 덧셈/뺄셈 공식을 알 필요가 없고, 함수가 단 한 개이며 배각공식이 매우 간단하다. 단점이라면 함숫값이 실수가 아니라는 점을 꼽을 수 있겠지만, 복소수를 다루는 입장에서 실수가 튀어나오는 것은 거추장스럽기만 하다. 학생 여러분도 이제 푸리에 전개와 같은 수학을 할 때에도 지수함수를 사용하는 연습을 차차 하기를 바란다.

이론이 시나브로 쌓여가며 어느새 이전에 못 풀던 문제들을 풀 능력이 생겼다.

연습문제 1.3.B. 임의의 복소수 a와 양의 정수 n에 대해 $x^n - a = 0$은 n개의 해를 가짐을 증명하여라.

이 장은 정리 1.1.3의 필자가 가장 좋아하는 증명으로 마무리하고자 한다. 물론 엄밀한 증명은 하지 못하겠지만 개략적으로 어떠한 아이디어를 사용하는지 알아보는 것을 목적으로 하자. 최소한 여러분에게 이 정리가 참이라는 사실을 의심 없이 믿도록 만들어보겠다. 올림피아드를 공부하는 입장에서 알아야 하는 내용은 아니므로 이해가 되지 않는 학생들은 무시해도 좋으나, 알아두어서 나쁠 것은 없을 것이다.

Sketch of proof of Theorem 1.1.3. 정리 1.1.3의 내용은 d차 다항식이 정확히 d개의 근을 가진다는 것이다. 하지만 1차 이상의 임의의 다항식이 적어도 한 개의 근을 가짐을 증명해도 충분하다. 그 이유는 $p(x) = (x - x_1)\cdots(x - x_r)p_r(x)$로 인수분해했을 때 $p_r(x)$이 2차 이상이라면 근을 가지므로 조립제법에 의해 계속해서 인수분해 가능해지기 때문이다. 따라서 우리는 임의의 1차 이상의 다항식이 복소근을 가짐을 증명할 것이다.

일반성을 잃지 않고 $p(x)$가 d차이며 최고차항의 계수가 1이라고 가정할 수 있다. 편의상 $p(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0$라 하자. $a_0 = 0$이라면 0이 근이 되므로, $a_0 \neq 0$이라고 가정해도 무방하다. 이제 어떤 $r > 0$에 대해, θ가 0 부터 2π까지 움질일 때 $p(re^{i\theta})$가 그리는 자취에 대해 잠깐 생각해보자. 무슨 일이 일어날지는 모르겠지만, 시작점과 끝점이 같다는 것은 확신할 수 있다. 즉, 자취는 교차점이 생길 수 있는 어떤 방향이 주어진 폐곡선이 될 것이다.

이번에는 r을 움직여가며 폐곡선이 어떻게 변하는지 살펴보자. r이 아주아주 작다면, $p(x) \approx a_0$가 되므로 a_0 주변에 조그맣게 놓인 폐곡선이 될 것이다. 반면 r이 아주아주

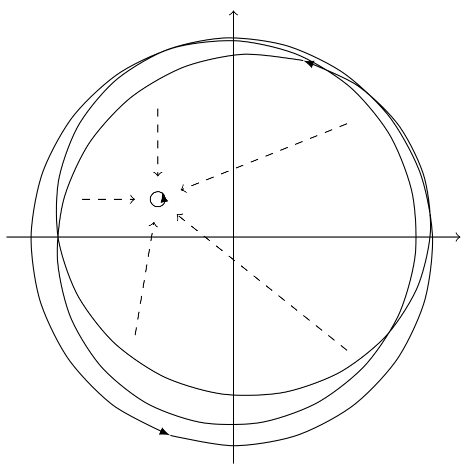

Figure 2: $p(re^{i\theta})$의 자취의 변화

크다면, x^d을 제외한 다른 항들은 x^d에 비해 무시할 수 있을만큼 작아질 것이다. 따라서 $p(re^{i\theta})$는 대강 $r^d e^{id\theta}$를 따라가며 반시계방향으로 d번 크게 원을 따라 돌 것이다.

이제 r을 아주아주 큰 값에서 아주아주 작은 값으로 천천히 옮기자. 이때 원점을 지나지 않는 각각의 폐곡선에 대해 다음과 같은 값을 생각해볼 수 있다. 원점에 서서 폐곡선 위의 점을 바라보는 사람을 생각하자. 점이 폐곡선을 따라 한 바퀴 돌 때 사람도 원점에서 회전을 할 것이다. 물론 반시계방향으로 회전하는 구간이 있을 수도 있고, 시계방향으로 회전하는 구간도 있을 수 있다. 하지만 어쨌든 처음과 마지막에 바라보는 점은 같으므로 회전한 바퀴의 수가 어떤 정수로 정해지게 된다. (반시계방향이면 양수, 시계방향이면 음수라 하자.) 예를 들어 그림 2에서 큰 r에 댛해 그 값은 3이고, 작은 r에 대해 0이다. 일반적인 경우에도 r이 아주아주 크다면 $p(re^{i\theta})$는 대강 $r^d e^{id\theta}$이므로 회전수는 d이고, 반면에 r이 아주아주 작다면 $p(re^{i\theta})$가 원점이 아닌 점 근처에서 운동하므로 회전수는 0이다.

즉 r이 처음에 아주 클 때에 회전수가 d이고 r을 줄여서 아주 작아지면 회전수가 0이 된다. 하지만 폐곡선이 원점을 지나는 일이 없다면 회전수는 변하지 않는다. 다시 말해서 회전수가 변화하려면 폐곡선이 원점을 지나쳐야만 한다. 초기 회전수는 $d > 0$이고 최종 회전수는 0이므로 곡선이 원점을 지나게 되는 r이 존재하고, 따라서 $p(x) = 0$은 근을 갖는다. $\square$

2 1의 제곱근들이 만들어내는 필터

서론이 불필요하게 길었다는 생각이 든다. 이제 복소수가 어떠한 것인지 알게 되었으니 본격적으로 이 통신강좌에서 다루고자 하는 이야기를 시작해보자.

2.1 1의 제곱근이란?

1의 제곱근(root of unity)란, 거듭제곱해서 1이 되는 수이다. 즉, 어떤 양의 정수 n에 대해 $x^n = 1$의 근이 되는 x를 1의 제곱근이라 부른다. 드 무아브르의 법칙에 의해 우리는 그 수들이 무엇인지 모두 알고 있다. 먼저 절댓값을 1이어야 하므로 그러한 x는 $e^{i\theta}$꼴일텐데, $e^{in\theta} = 1$이므로 $\theta = 0, 2\pi/n, 4\pi/n, \ldots, 2(n-1)\pi/n$이 된다. 따라서 **1의 n 제곱근(nth root or unity)**들은

$$1, e^{2\pi/n}, e^{4\pi/n}, \ldots, e^{2(n-1)\pi/n}$$

이 된다. 여기서 $\zeta_n = e^{2\pi/n}$이라는 표기법을 도입하자. 그러면 1의 n제곱근들을

$$1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}$$

과 같이 더 간단하게 쓸 수 있다. 물론 이 수들이 n개의 근이 되므로

$$x^n - 1 = (x-1)(x-\zeta_n)(x-\zeta_n^2)\cdots(x-\zeta_n^{n-1})$$

도 성립한다.

연습문제 2.1.A. 양의 정수 n, m에 대해 $\zeta_n^m = 1$일 필요충분조건은 $n \mid m$임을 보여라.

연습문제 2.1.B. 두 복소수 ζ와 ζ'가 1의 제곱근이라 할 때, 두 수의 곱 $\zeta\zeta'$도 1의 제곱근이 됨을 보여라.

연습문제 2.1.C. 양의 정수 n, m, n', m'에 대해, $\zeta_n^m = \zeta_{n'}^{m'}$일 필요충분조건은 $m/n - m'/n'$이 정수인 것임을 보여라.

연습문제 2.1.C에 의해, 많은 1의 원시근들은 더 간단한 형태로 바꿀 수 있다. 한 번 $n = 6$일 때 1의 여섯제곱근들을 나열해보자.

$$\zeta_6^0 = 1, \quad \zeta_6 = \zeta_6, \quad \zeta_6^2 = \zeta_3, \quad \zeta_6^3 = \zeta_2 = -1 \quad \zeta_6^4 = \zeta_3^2, \quad \zeta_6^5 = \zeta_6^5$$

이들 중 더 간단한 형태로 바꿀 수 없는 것들은 ζ_n^k들 중 k와 n이 서로소인 것들이다. 이러한 수들을 **1의 원시n제곱근(primitive root of unity)**라 부른다. 예를 들어 1의 원시n제곱근의 개수는 $\phi(n)$이다.[5]

연습문제 2.1.D. 복소수 z에 대해, $\zeta^m = 1$인 최소의 양의 정수 m이 n인 것과 z가 1의 원시n제곱근인 것이 필요충분조건임을 보여라.

[5] 이 $\phi(n)$은 오일러 ϕ 함수라고 부르고, $0 < k \le n$이며 $\gcd(k, n) = 1$인 k의 개수를 나타낸다.

연습문제 2.1.E. 양의 정수 n과 k에 대해, $\gcd(n,k)=d$라 하고 ζ는 1의 원시n제곱근이라 하자. 이때 ζ^k는 1의 원시(n/d)제곱근임을 증명하여라.

눈치챘을지도 모르겠지만, 1의 원시제곱근들은 소수의 원시근과도 밀접한 연관이 있다. 소수 p의 **원시근(primitive root)**이란,

$$\{1, g, g^2, g^3, \dots, g^{p-2}\} \equiv \{1, 2, 3, \dots, p-1\} \pmod p \tag{1}$$

이 되도록 만드는 g이다. 원시근과 관련된, 증명하기는 매우 까다롭지만 유용한 정리가 있다.

정리 2.1.1. *임의의 소수는 원시근을 가진다.*

식 1에서 우변은 방정식 $x^{p-1} \equiv 1 \pmod p$의 $p-1$개의 근임을 확인할 수 있다.[6] 이것과 좌변과 비교해보면, g와 ζ_{p-1}이 엇비슷해 보인다. 이 비유는 이번 통강에서 종종 등장할 것이니 수상한 대목이 있다면 놓치지 않기를 바란다.

연습문제 2.1.F. 소수 p는 원시근을 $\phi(p-1)$개 가짐을 보여라.

연습문제 2.1.G. 소수 p와 $p-1$의 배수가 아닌 양의 정수 k에 대해 다음을 증명하여라.

$$p \mid 1^k + 2^k + \cdots + (p-1)^k$$

계산 연습을 할 겸 다음 문제도 풀어보자.

연습문제 2.1.H (Putnam 2015 A3)**.** 다음의 값을 계산하여라:

$$\prod_{a=1}^{2015} \prod_{b=1}^{2015} (1 + e^{2\pi i ab/2015})$$

2.2 개수를 셈하는 함수

조금 후에 알게 되겠지만, 1의 제곱근을 이용하여 문제를 풀 때 많은 경우에 수를 세는 함수를 만들 필요가 있다. 정확히 말하자면 수를 세는 함수가 아니라 우리가 원하는 답을 계수로 가지고 있는 무한급수이다. 수열 $\{a_n\}$에 대해, 그의 **생성함수(generating function)**을 다음과 같이 정의하자.

$$F(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots$$

예를 들어 $a_n = \binom{m}{n}$의 생성함수는

$$F(x) = \binom{m}{0} + \binom{m}{1}x + \binom{m}{2}x^2 + \cdots + \binom{m}{m}x^m = (1+x)^m$$

이다.

[6] 페르마의 소정리이다.

생성함수들 사이의 합은 당연하게도 수열의 합과 대응되도록 정의된다. 두 생성함수 $F(x) = \sum a_n x^n$과 $G(x) = \sum b_n x^n$의 합은

$$F(x) + G(x) = \sum_{n=0}^{\infty} (a_n + b_n) x^n$$

으로 정의된다. 하지만 곱은 다항식의 곱과 같이 정의된다.

$$F(x)G(x) = \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} a_n b_m x^{n+m} = \sum_{n=0}^{\infty} \left(\sum_{i=0}^{n} a_i b_{n-i} \right) x^n$$

말로 해석하자면, 첨자의 합이 n이 되는 항들을 곱해서 더한 값이 곱한 수열에서의 n번째 항이 되는 것이다. 조금 특이한 연산이지만, 이것이 생성함수를 강력한 도구로 만드는 특징이다.

한 가지 예를 들어보자. 수열 $a_n = 1$의 생성함수는 $1 + x + x^2 + \cdots$ 인데, 여기에 $1 - x$를 곱하면

$$(1 + x + x^2 + x^3 + \cdots)(1 - x) = 1$$

이 된다! 따라서

$$1 + x + x^2 + x^3 + \cdots = \frac{1}{1 - x}$$

이라 쓸 수 있다. (여기에서 "어 $x = 2$를 대입하면 성립하지 않는데..."하는 의문을 품는 학생들이 있을 수 있다. 하지만 저 둘이 같다는 것은 모든 x에 대해 등호가 성립한다는 뜻이 아니다. 단순히 생성함수적으로 같은 급수를 나타낸다는 표시일 뿐이다.)

연습문제 2.2.A. 수열 $a_n = n + 1$의 생성함수를 유리식으로 표현하여라.

선형 점화식이 있는 수열의 생성함수는 항상 유리식으로 표현할 수 있다. 예를 들어 $a_0 = 0$, $a_1 = 1$, $a_n = a_{n-1} + a_{n-2}$로 정의된 피보나치 수열을 생각해보자. $a_n - a_{n-1} - a_{n-2} = 0$이므로 생성함수에 $1 - x - x^2$을 곱하면

$$(1 - x - x^2)\left(\sum_{n=0}^{\infty} a_n \right) = a_0 + (a_1 - a_0)x + (a_2 - a_1 - a_0)x^2 + (a_3 - a_2 - a_1)x^3 + \cdots = x$$

임을 알 수 있다. 따라서 $\phi_1 = (1 + \sqrt{5})/2$, $\phi_2 = (1 - \sqrt{5})/2$라 하면

$$\sum_{n=0}^{\infty} a_n = \frac{x}{1 - x - x^2} = \frac{x}{(1 - \phi_1 x)(1 - \phi_2 x)} = \frac{1}{\sqrt{5}} \left(\frac{1}{1 - \phi_1 x} - \frac{1}{1 - \phi_2 x} \right)$$

이다. 여기서 $1/(1 - \phi x) = 1 + \phi x + \phi^2 x^2 + \cdots$이므로

$$a_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n \right)$$

이라는 사실까지 얻는다.

하지만 이렇게 점화식을 이용하여 생성함수를 구하는 것에는 한계가 있다. 가장 큰 문제는 수열의 점화식을 알아야만 생성함수를 구할 수 있다는 것이다. 피보나치 수열을

점화식 없이 조합적으로 정의하는 방법은, n을 1과 2의 합으로 (순서를 고려하여) 표현하는 방법을 a_{n+1}이라 하는 것이다. 이 정의로부터 피보나치 수열의 점화식을 곧바로 구해보자.

우선 $a_{m,n+1}$을 n을 1과 2를 총 m개 사용하여 표현하는 방법의 가짓수라 하자. 이 수열 $a_{m,n+1}$의 점화식은

$$\sum_{n=0}^{\infty} a_{m,n+1}x^n = (x+x^2)^m$$

이라 표현할 수 있을 것이다. 이것은 $(x+x^2)^m = (x+x^2)(x+x^2)\cdots(x+x^2)$를 전개했을 때 x^n이 만들어지려면 각 $x+x^2$에서 x 또는 x^2를 골라서 곱하되, 지수의 합이 정확히 n이 되어야 하므로 n을 m개의 1과 2의 합으로 표현하는 것과 대응되기 때문이다. 이제 $a_{n+1} = a_{0,n+1} + a_{1,n+1} + \cdots$이므로

$$\sum_{n=0}^{\infty} a_{n+1}x^n = \sum_{m=0}^{\infty}\sum_{n=0}^{\infty} a_{m,n+1}x^n = 1 + (x+x^2) + (x+x^2)^2 + \cdots = \frac{1}{1-x-x^2}$$

이다. 따라서

$$\sum_{n=0}^{\infty} a_n x^n = x\sum_{n=0}^{\infty} a_{n+1}x^n = \frac{x}{1-x-x^2}$$

이다. 이렇게 생성함수들의 곱을 전개했을 때의 계수들이 차수를 합해서 원하는 차수를 만드는 방법과 같아진다는 사실은 여기저기에서 많이 응용된다.

연습문제 2.2.B. 집합 $\{1, 2, \ldots, 2000\}$의 부분집합들 중 원소의 합이 n인 집합의 개수를 a_n이라 하자. 이때 a_n의 생성함수를 구하여라.

연습문제 2.2.C. 음 아닌 정수 n에 대해, n을 (순서를 고려하지 않고) 몇 개의 양의 정수의 합으로 표현하는 방법의 수를 p_n이라 하자. 예를 들어 $4 = 4 = 3+1 = 2+2 = 2+1+1 = 1+1+1+1$이므로 $p_4 = 5$이다. (편의상 $p_0 = 1$이라 하자.) 이때

$$\sum_{n=0}^{\infty} p_n x^n = \frac{1}{(1-x)(1-x^2)(1-x^3)\cdots}$$

임을 보여라.

이쯤에서 생성함수를 이용하여 풀 수 있는 유명한 문제를 하나 소개하겠다.

예제 2.2.1. 음 아닌 정수들의 집합이 유한개의 무한등차수열들로 분할되었다. 등차수열의 개수가 두 개 이상이라면, 공차가 같은 두 등차수열이 존재함을 증명하여라.

Solution. 각 등차수열을 $a_i, a_i+d_i, a_i+2d_i, \ldots$라 하자. 이때 당연히

$$1 + x + x^2 + \cdots = \sum_{i=1}^{n}(x^{a_i} + x^{a_i+d_i} + x^{a_i+2d_i} + \cdots)$$

가 성립한다. 따라서

$$\frac{1}{1-x} = \sum_{i=1}^{n} \frac{x^{a_i}}{1-x^{d_i}}$$

이 성립한다.

모든 등차수열이 서로 다른 공차를 가진다고 가정하고, 일반성을 잃지 않고 $d_1 > d_2 > \cdots > d_n$이라 하자. 이때

$$x^{a_1} = (1 - x^{d_1})\left(\frac{1}{1-x} - \sum_{i=2}^{n} \frac{x^{a_i}}{1 - x^{d_i}}\right)$$

이 성립한다. 여기서 $x = \zeta_{d_1}$을 대입해보자. 우선 어떤 $2 \le i \le n$에 대해서도 $1 - x^{d_i} \neq 0$이 되므로 대입하는 것은 가능하다. 우변에 있는 $1 - x^{d_1}$은 0이 될 것이므로 우변은 0이지만, x^{a_1}은 절대로 0이 될 수 없으므로 모순을 얻는다. 따라서 공차가 같은 두 등차수열이 존재한다. □

2.3 제곱근들을 더해보자

1의 n제곱근들을 모두 늘어놓은 다음, 각 수를 m승해서 더하면 아주 신기한 현상이 벌어진다.

정리 2.3.1. *양의 정수 n과 복소수 $\zeta = \zeta_n$에 대해 다음이 성립한다.*

$$1 + \zeta^m + \zeta^{2m} + \cdots + \zeta^{(n-1)m} = \begin{cases} n & \text{if } n \mid m, \\ 0 & \text{if } n \nmid m. \end{cases}$$

Proof. 만약 $\zeta^m \neq 1$이라면

$$1 + \zeta^m + \cdots + \zeta^{(n-1)m} = \frac{\zeta^{mn} - 1}{\zeta^m - 1} = \frac{1^m - 1}{\zeta^m - 1} = 0$$

이다. 한편 $\zeta^m = 1$이면

$$1 + \zeta^m + \cdots + \zeta^{(n-1)m} = 1 + 1 + \cdots + 1 = n$$

이다. □

즉, 1의 n제곱근들을 거듭제곱해서 더하는 행위는 어떤 수가 n의 배수인지 아닌지를 판별하는 역할을 수행하는 것이다. 이것을 어디에 응용할 수 있을까? 어떤 다항식

$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d$$

이 주어져 있다고 하고, 이들 중 x의 지수가 n의 배수인 것들의 항을 더한 값을 알고 싶다고 하자. 즉, $p(x)$가 주어졌을때 $a_0 + a_n + a_{2n} + \cdots$를 알고 싶은 것이다. 그러면 정리 2.3.1에 의해

$$a_0 + a_n + a_{2n} + \cdots = \frac{1}{n}\sum_{i=0}^{d} a_i(1 + \zeta_n^i + \zeta_n^{2i} + \cdots + \zeta_n^{(n-1)i}) = \frac{p(1) + p(\zeta_n) + \cdots + p(\zeta_n^{n-1})}{n}$$

로 쓸 수 있다. 이를 사용하는 대표적인 문제 하나만 살펴보자.

예제 2.3.2. 다음을 간단히 하여라.

$$\binom{2n}{0}+\binom{2n}{2}+\binom{2n}{4}+\cdots+\binom{2n}{2n-2}+\binom{2n}{2n}$$

Solution. 이항계수들은 다항식 $(1+x)^{2n}$의 계수들이다. 이 다항식의 짝수차항의 계수들을 모두 합한 값은 $((1+1)^{2n}+(1-1)^{2n})/2=2^{2n-1}$으로 계산된다. □

이번엔 조금 더 어렵지만 사실은 똑같은 문제들을 풀어보자.

연습문제 2.3.A. 다음을 간단히 하여라.

$$\binom{3n+2}{1}+\binom{3n+2}{4}+\binom{3n+2}{7}+\cdots+\binom{3n+2}{3n+1}$$

연습문제 2.3.B. 생성함수 $p(x)=a_0+a_1x+a_2x^2+\cdots$에 대해 다음을 보여라.

$$a_0+a_nx^n+a_{2n}x^{2n}+\cdots=\frac{p(x)+p(\zeta_nx)+p(\zeta_n^2x)+\cdots+p(\zeta_n^{n-1}x)}{n}$$

더 일반적으로, $0\le k<n$에 대해 다음을 보여라.

$$a_kx^k+a_{n+k}x^{n+k}+a_{2n+k}x^{2n+k}+\cdots=\frac{p(x)+\zeta_n^{-k}p(\zeta_nx)+\zeta_n^{-2k}p(\zeta_n^2x)+\cdots+\zeta_n^{-(n-1)k}p(\zeta_n^{n-1}x)}{n}$$

연습문제 2.3.C. 변수가 두 개인 경우, 생성함수 $p(x,y)=\sum_{i,j}a_{i,j}x^iy^j$이 주어져 있다고 할 때 다음을 보여라.

$$\sum_{i,j}a_{ni,nj}x^{ni}y^{nj}=\frac{1}{n^2}\sum_{s=1}^{n}\sum_{t=1}^{n}p(\zeta_n^sx,\zeta_n^ty)$$

이렇게 1의 제곱근을 이용하여, 특정한 형태의 항들만 골라내는 것이 이 장의 제목에서 말하는 필터이다. 이것을 정말 효과적으로 이용하는 문제 몇 개만 함께 살펴보자.

예제 2.3.3. 집합 $\{1,2,\ldots,2000\}$의 부분집합들 중 원소의 합이 5의 배수인 것의 개수를 구하여라.

Solution. 원소의 합이 n인 것의 개수를 a_n이라 할 때, 연습문제 2.2.B에서 a_n이 생성함수가

$$p(x)=\sum_{n=0}^{\infty}a_nx^n=(1+x)(1+x^2)\cdots(1+x^{2000})$$

이 됨을 보였다. 이제 이들 중 n이 5의 배수인 것만 골라내어 더하고 싶다. 이것은

$$\frac{1}{5}(p(1)+p(\zeta_5)+p(\zeta_5^2)+p(\zeta_5^3)+p(\zeta_5^4))$$

으로 계산할 수 있다.

이제

$$p(1)=(1+1)(1+1)\cdots(1+1)=2^{2000}$$
$$p(\zeta_5)=(1+\zeta_5)(1+\zeta_5^2)\cdots(1+1)=\big((1+1)(1+\zeta_5)\cdots(1+\zeta_5^4)\big)^{400}=2^{400}$$

이 되고, 마찬가지로 $p(\zeta_5^2) = p(\zeta_5^3) = p(\zeta_5^4) = 2^{400}$이 된다. 따라서 곧바로 집합의 개수가

$$\frac{p(1) + p(\zeta_5) + \cdots + p(\zeta_5^4)}{5} = \frac{2^{2000} + 2^{402}}{5}$$

임을 얻는다. □

예제 2.3.4 (IMO Shortlist 2007 C3)**.** 양의 정수들 $1, 2, \ldots, n$이 빨강 또는 파랑으로 색칠되어 있다. 수들 x, y, z가 같은 색으로 이루어져 있으며 $n \mid x+y+z$인 순서쌍 (x, y, z)의 개수가 2007이라고 할 때, 가능한 n의 값을 모두 구하여라.

Solution. 빨강으로 색칠된 수들의 집합을 R, 파랑으로 색칠된 수들의 집합을 B라 하자. 우선 $n \mid x+y+z$인 순서쌍 (x, y, z)를 해석할 필요가 있다. 다항식 $r(t) = \sum_{r \in R} t^r$으로 정의했을 때, $n \mid x+y+z$이며 $x, y, z \in R$인 순서쌍 (x, y, z)의 개수는 다항식 $r(t)^3$의 항들 중 t의 지수가 n의 배수인 것들의 계수의 합이 된다. 따라서 그 개수는

$$\frac{r(1)^3 + r(\zeta_n)^3 + r(\zeta_n^2)^3 + \cdots + r(\zeta_n^{n-1})^3}{n}$$

이 된다. 마찬가지로 $b(t) = \sum_{b \in B} t^b$이라 두면, x, y, z가 같은 색이며 $n \mid x+y+z$인 (x, y, z)의 개수는

$$\frac{r(1)^3 + b(1)^3 + \cdots + r(\zeta_n^{n-1})^3 + b(\zeta_n^{n-1})^3}{n}$$

으로 표현할 수 있다.

이때, $r(t) + b(t) = t + t^2 + \cdots + t^n$이다. 따라서 $0 < i < n$에 대해 $r(\zeta_n^i) + b(\zeta_n^i) = 0$이 되어 $r(\zeta_n^i)^3 + b(\zeta_n^i)^3 = 0$이다. 그러므로 순서쌍 (x, y, z)의 개수는 그냥

$$\frac{r(1)^3 + b(1)^3}{n}$$

이 된다. 여기서 $r(1) + b(1) = 1 + \cdots + 1 = n$이므로 그 개수는 $r(1)^2 - r(1)b(1) + b(1)^2$이다.

문제에서는 $r(1)^2 - r(1)b(1) + b(1)^2 = 2007$이며 $r(1) + b(1) = n$이다. 이 방정식을 풀면 $\{r(1), b(1)\} = \{33, 51\}$과 $\{18, 51\}$밖에 없다. 따라서 가능한 n은 $69, 84$이다. □

예제 2.3.5 (IMO 1995 6)**.** 홀수인 소수 p에 대해, 집합 $\{1, 2, \ldots, 2p\}$의 부분집합들 중 원소의 개수가 p이고 원소의 합이 p의 배수인 것의 개수를 구하여라.

Solution. 원소의 개수가 p의 배수이고, 원소의 합도 p의 배수인 집합의 개수를 구해보자. 이것은 다항식

$$f(x, y) = (1 + xy)(1 + x^2 y)(1 + x^3 y) \cdots (1 + x^{2p} y)$$

에서 x와 y의 지수가 모두 p의 배수인 항들의 계수의 합과 같다. (x의 지수는 원소의 합을 나타내고, y의 지수는 원소의 개수를 나타낸다.) 따라서 우리가 구하고자 하는 값은

$$\frac{1}{p^2} \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} f(\zeta_p^i, \zeta_p^j)$$

으로 쉽게 나타낼 수 있다.

만약 $0 < i < p$라면, p가 소수이므로 $f(\zeta_p^i, \zeta_p^j) = (1+1)^2(1+\zeta_p)^2 \cdots (1+\zeta_p^{p-1})^2 = 2^2 = 4$가 된다. 만약 $i = 0$이라면, $f(0, \zeta_p^j) = (1+\zeta_p^j)^{2p}$이다. 따라서 우리가 구하는 값은

$$\frac{4p(p-1)}{p^2} + \frac{1}{p^2}\sum_{j=0}^{p-1}(1+\zeta_p^j)^{2p} = \frac{4p-4}{p} + \frac{p + p\binom{2p}{p} + p}{p^2} = \frac{\binom{2p}{p} + 4p - 2}{p}$$

가 된다. 여기서 원소의 개수가 0인 집합 1개, 원소의 개수가 $2p$인 집합 1개를 추가로 세어주었으므로 빼주면 답은 $(\binom{2p}{p} + 2p - 2)/p$가 될 것이다. $\square$

물론 이러한 방법을 사용하지 않고도 조합적으로 풀 수 있는 문제들이다. 하지만 1의 원시근을 사용하면서 이 문제들이 얼마나 기계적인 계산 문제가 되는지를 느낄 수 있을 것이다.

종종 1의 제곱근이 타일링 문제에서 사용되는 경우도 있는데, 이것에 관하여 한 문제만 보고 넘어가고 싶다.

예제 2.3.6. 양의 정수 a, b, n에 대해, $a \times b$ 크기의 직사각형이 $1 \times n$ 크기의 직사각형들로 분할될 수 있다고 한다. 이때 $n \mid a$이거나 $n \mid b$임을 증명하여라.

Solution. i행 j열의 칸에 ζ_n^{i+j}의 가중치를 부여하자. 이때 각 직사각형이 덮는 n개의 칸에 있는 가중치를 모두 합하면 $\zeta_n + \zeta_n^2 + \cdots + \zeta_n^n = 0$이 된다. 따라서 $a \times b$ 크기의 직사각형을 $1 \times n$ 크기의 직사각형들로 분할할 수 있다면 $a \times b$의 모든 칸의 가중치의 합이 0이 되어야 할 것이다. 그 합은

$$\sum_{i=1}^{a}\sum_{j=1}^{b}\zeta_n^{i+j} = (\zeta_n + \zeta_n^2 + \cdots + \zeta_n^a)(\zeta_n + \zeta_n^2 + \cdots + \zeta_n^b)$$

이므로 둘 중 하나는 0이 되어야 한다. 일반성을 잃지 않고 $\zeta_n + \zeta_n^2 + \cdots + \zeta_n^a = 0$이라 하면 여기에 $\zeta_n - 1$을 곱했을 때 $\zeta_n^{a+1} - \zeta_n = 0$이므로 a는 n의 배수임을 얻는다. $\square$

2.4 이산 푸리에 변환과 푸리에 급수

1의 원시근들을 합했을 때 사라진다는 것은 해석학 중 푸리에 이론과 아주 밀접한 관련을 가진다. 이 절에서는 푸리에 변환 중 적분을 이용하지 않는 이산적인 푸리에 이론에 대해 알아보자.

수열 $a_0, a_1, a_2, \ldots, a_{n-1}$이 주어져 있다고 하자. 이 수열은 n개의 항만을 갖지만, 모든 첨자는 $\bmod n$으로 보는 수열이다. 즉, $a_n = a_0$이고 $a_{-1} = a_{n-1}$이다. 이제 이 수열의 **이산 푸리에 변환**(**discrete Fourier transform**)을

$$\hat{a}_k = a_0 + a_1\zeta_n^{-k} + a_2\zeta_n^{-2k} + \cdots + a_{n-1}\zeta_n^{-(n-1)k}$$

로 정의하자. 이 수열 $\hat{a}_0, \hat{a}_1, \ldots, \hat{a}_{n-1}$도 첨자를 $\bmod n$으로 본다는 사실을 눈치챌 수 있을 것이다.

흥미롭게도 푸리에 변환 $\hat{a}$로부터 a를 구할 수 있고, 그 공식이 a_k로부터 $\hat{a}_k$를 만드는 것과 아주 유사하다.

정리 2.4.1 (푸리에 반전 공식). *수열 $\{a_k\}$의 푸리에 변환을 $\{\hat{a}_k\}$라 하고 $\zeta = \zeta_n$이라 하자. 이때 다음이 성립한다.*

$$a_k = \frac{1}{n}(\hat{a}_0 + \hat{a}_1\zeta^k + \hat{a}_2\zeta^{2k} + \cdots + \hat{a}_{n-1}\zeta^{(n-1)k})$$

Proof. 그냥 $\hat{a}_l$에 정의를 대입해주면

$$\frac{1}{n}\sum_{l=0}^{n-1}\hat{a}_l\zeta^{lk} = \frac{1}{n}\sum_{l=0}^{n-1}\sum_{m=0}^{n-1}a_m\zeta^{-lm}\zeta^{lk} = \sum_{m=0}^{n-1}a_m\left(\frac{1}{n}\sum_{m=0}^{n-1}\zeta^{l(k-m)}\right) = a_k$$

임을 확인할 수 있다. □

이것이 의미하는 것은, $\hat{a}$들이 사실은 a_k를 ζ^k라는 함수들의 합으로 표현할 때의 계수들이 된다는 것이다. 또한 이 변환은 수열 a와 $\hat{a}$ 사이에 일대일 대응을 만들어주므로 a의 성질을 필요충분조건인 $\hat{a}$의 성질로 바꿀 수 있다. 예를 들어 다음이 성립한다.

명제 2.4.2. *수열 a의 이산 푸리에 변환을 $\hat{a}$이라 하자. 이때 $a_0 = a_1 = \cdots = a_{n-1}$일 필요충분조건은 $\hat{a}_1 = \hat{a}_2 = \cdots = \hat{a}_{n-1} = 0$인 것이다.*

Proof. 우선 $a_0 = \cdots = a_{n-1}$이라면 임의의 $1 \le k \le n-1$에 대해

$$\hat{a}_k = a_0(1 + \zeta^{-k} + \zeta^{-2k} + \cdots + \zeta^{-(n-1)k}) = 0$$

이다. 반대로 $\hat{a}_1 = \cdots = \hat{a}_{n-1} = 0$이라면

$$a_k = \frac{1}{n}(\hat{a}_0 + 0 + \cdots + 0) = \frac{\hat{a}_0}{n}$$

로 일정하다. □

연습문제 2.4.A. 수열 a의 이산 푸리에 변환을 $\hat{a}$라 하자. 이때 $a_1 = \cdots = a_{n-1}$일 필요충분조건은 $\hat{a}_1 = \cdots = \hat{a}_{n-1}$임을 보여라.

연습문제 2.4.B. 두 수열 a와 b에 대해 그들의 **합성곱(convolution)** $a * b$를

$$(a * b)_k = a_k b_0 + a_{k-1}b_1 + \cdots + a_{k-n+1}b_{n-1}$$

으로 정의하자. 이때 $\widehat{(a * b)}_k = \hat{a}_k \cdot \hat{b}_k$임을 보여라.

푸리에 변환을 올림피아드에서 직접적으로 사용해야할 일은 없겠지만, 이렇게 원래 수열과 그것에 1의 제곱근들을 곱한 후 합해 얻어진 수열 사이에 어떤 대응 관계가 있다는 사실을 알면 편한 경우는 많다. 아래 문제를 풀어보며 이 개념이 어떻게 문제에 녹아 들어가 있는지 살펴보자.

예제 2.4.3 (Leningrad 1991). 유한수열 $\{a_1, \dots, a_n\}$에 대해, 모든 $1 \le k \le p$에 대해

$$s(k,p) = a_k + a_{k+p} + a_{k+2p} + \dots$$

의 값이 같다면, 수열 $\{a_i\}$를 p-*balanced*라 하자. 만약 길이 50이 수열이 $3, 5, 7, 11, 13, 17$-balanced라면, 모든 항이 0이어야 함을 증명하여라.

Solution. 수열 $\{a_i\}$가 p-balanced라는 이야기는 $s(\cdot, p)$가 일정하다는 것인데, 이것은 푸리에 변환 $\widehat{s(\cdot, p)}$의 $1, 2, \dots, p-1$번째 항이 모두 0이라는 것이다. 잘 생각해보면, 이것은 복소수 $\zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1}$이 다항식

$$f(x) = a_1 + a_2x + a_3x^2 + \cdots + a_nx^{n-1}$$

의 근이 되는 것과 동치이다.

따라서 수열 $a_1, \dots, a_{50}$이 $3, 5, 7, 11, 13, 17$-balanced인 것은 ζ_p^k이 $p = 3, 5, 7, 11, 13, 17$과 $1 \le k \le p-1$에 대해 모두 $f(x)$의 근이 된다는 뜻이다. 즉, $f(x)$는 서로 다른 근을 $2+4+6+10+12+16 = 50$개 갖는다. 하지만 $f(x)$는 49차 다항식이므로 항등적으로 0이 되어야만 한다. 따라서 수열 a의 모든 항은 0이다. □

적분을 아는 학생들에게 잠깐 연속적인 푸리에 변환도 소개하고자 한다. 우선 연속적인 경우에 1의 제곱근을 더했을 때 0이 된다는 사실이 어떤 식으로 나타날 것인지 살펴보아야 한다. 수를 연속적으로 더하는 것은 적분의 개념이고, 1의 제곱근을 더하는 상황이므로 정수 n에 대해

$$\int_{x=0}^{1} e^{2\pi inx}dx = \begin{cases} 0 & \text{if } n \neq 0 \\ 1 & \text{if } n = 0 \end{cases}$$

와 같은 식을 이론을 전개하는데 원형으로 삼을 수 있을 것이다.

무한수열 $\dots, a_{-1}, a_0, a_1, \dots$이 있을 때, 이 수열의 **푸리에 변환**(**Fourier transform**)을 주기가 1인 함수

$$\hat{a}(x) = \sum_{n=-\infty}^{\infty} a_n e^{-2\pi inx}$$

로 정의하자. 여기서 주의해야할 점이 있다. $\hat{a}(x)$는 실제로 함수여야 하므로 우변의 무한급수가 임의의 x에 대해 수렴해야 한다. 따라서 적어도 $\sum_{n=-\infty}^{\infty} |a_n|$이 수렴하는 경우에만 푸리에 변환을 정의한다. 이때 푸리에 역변환은

$$a_n = \int_{x=0}^{1} \hat{a}(x)e^{2\pi inx}dx$$

로 주어질 것이다.

연습문제 2.4.C. 양의 실수 a와 b에 대해, $a \times b$ 크기의 직사각형을 작은 직사각형들로 분할하여 각 작은 직사각형이 길이가 정수인 변을 갖도록 할 수 있다고 한다. 이때 a 또는 b가 정수임을 보여라.[7]

[7]이 문제는 예제 2.3.6의 연속적인 버전이라고 생각할 수 있다.

이 성질을 필터로 사용하려면 다음과 같이 하면 된다. 다항식 $p(x) = a_0 + a_1x + \cdots$ 에서 x^k의 계수 a_k를 구하고 싶다면,

$$a_k = \int_{x=0}^{1} p(e^{2\pi ix})e^{-2\pi ikx}dx$$

와 같이 계산할 수 있다. 이 방법은 해석적 정수론에서 많이 사용하는 방법이다. 예를 들어 임의의 k에 대해 어떤 $G(k)$가 존재하여, 충분히 큰 임의의 정수는 $G(k)$개의 완전 k제곱수들의 합으로 표현 가능함을 증명하고 싶다고 하자. 이때 사용하는 방법은 함수

$$f(x) = x^{0^k} + x^{1^k} + x^{2^k} + x^{3^k} + \cdots$$

를 정의한 후, 충분히 큰 G를 잡으면 모든 양의 정수 n에 대해

$$\int_{x=0}^{1} f(x)^G e^{-2\pi inx}dx > 0$$

이 됨을 해석적으로 보이는 것이다. 최근에 Helfgott에 의해 완전히 증명된 약한 골드바흐의 추측도 이와 같은 방법을 사용하여 해결되었다.

2.5 모듈러로 작동하는 다른 종류의 필터들

이 통신강좌는 물론 1의 제곱근들이 만드는 필터에 대해 다루고 있다. 하지만 이 통신강좌가 올림피아드 전부가 아닌 만큼, 이외에 어떤 필터가 있는지도 소개하고자 한다. 이 절은 순수하게 다른 것들을 보여주기 위한 용도로 작성한 것이니 두 발 뻗고 편하게 읽어주길 바란다. 먼저 소개할 것은 조합론을 공부하면서 한 번 쯤은 들어봤을 법한 Chevalley-Warning theorem이다.

예제 2.5.1 (Chevalley-Warning theorem)**.** 소수 p, 양의 정수 n과 $x_1, \ldots, x_n$을 변수로 가지는 정수계수 다항식 $f_1, \ldots, f_m$이 있다. 만약 $\deg f_1 + \cdots + \deg f_m < n$이라면,[8]

$$\begin{cases} f_1(x_1, \ldots, x_n) \equiv 0 \pmod{p} \\ \quad\vdots \\ f_m(x_1, \ldots, x_n) \equiv 0 \pmod{p} \end{cases}$$

를 동시에 만족시키는 $(x_1, \ldots, x_n) \in \{0, \ldots, p-1\}^n$의 개수가 p의 배수임을 증명하여라.

Solution. 해의 개수를 mod$p$로 세는 방법이 무엇이 있을까? 이 문제에서는 $p \mid x$라면 $x^{p-1} \equiv 0 \pmod{p}$이고 $p \nmid x$라면 $x^{p-1} \equiv 1 \pmod{p}$임을 이용할 것이다. 그렇다면 $(x_1, x_2, \ldots, x_n)$이 저 방정식들의 공통근이 되는지 판별할 수 있는 방법에 대해 한 번 더 생각해볼 필요가 있다. 다항식

$$A(x_1, \ldots, x_n) = \prod_{i=1}^{m}(1 - f_i(x_1, \ldots, x_n)^{p-1})$$

[8] 여기서 deg는 항의 차수의 합들 중 최댓값으로 정의된다. 예를 들어 $\deg(x_1 + x_2^3 + x_1^2x_3^2) = 4$이다.

을 정의하면, $(x_1, \ldots, x_n)$이 공통근이 맞다면 $A \equiv 1 \pmod p$가 되고, 아니라면 $A \equiv 0 \pmod p$가 된다. 즉, A라는 다항식은 공통근만 골라내서 더하는 필터의 역할을 하는 것이다.

이제 남은 일은 $A(x_1, \ldots, x_n)$들을 합한 값인

$$\sum_{x_1=0}^{p-1} \sum_{x_2=0}^{p-1} \cdots \sum_{x_n=0}^{p-1} A(x_1, \ldots, x_n)$$

을 계산하는 것이다. $A(x_1, \ldots, x_n)$은 몇 개의 단항식의 합으로 이루어져 있고, $\deg A < (p-1)n$이므로 각 단항식의 차수는 $(p-1)n$보다 작을 것이다. 한 단항식 $x_1^{d_1} x_2^{d_2} \cdots x_n^{d_n}$에 대해서만 먼저 살펴보자.

$$\sum_{x_1=0}^{p-1} \cdots \sum_{x_n=0}^{p-1} x_1^{d_1} \cdots x_n^{d_n} = \left(\sum_{x_1=0}^{p-1} x_1^{d_1} \right) \cdots \left(\sum_{x_n=0}^{p-1} x_n^{d_n} \right)$$

인데, 연습문제 2.1.G에 의해 $d_i < p-1$이라면 $\sum_{x_i=0}^{p-1} x_i^{d_i} = 0$이다. (여기서 $0^0 = 1$로 간주되기 때문에 $d_i = 0$일 때에도 합은 0이 된다.) 전체 차수가 $d_1 + \cdots + d_n < (p-1)n$이므로 $d_i < p-1$인 i가 존재하고, 따라서 임의의 단항식에 대해 그 합은 0이 된다. 그러므로 $A(x_1, \ldots, x_n)$의 합도 0이 되고 이것으로 증명이 끝난다. □

이 문제에서 사용한 필터를 되짚어보자. 어떤 수가 0인지 아닌지를 판별하기 위해 $p-1$승을 해주었고, 여기에 조건들이 동시에 만족되는지를 확인하기 위해 1에서 빼 곱해주었다. 이번엔 조금 다른 형태의 필터를 사용하는 문제를 살펴보자.

예제 2.5.2 (USA TST 2010 6)**.** 1보다 큰 정수들의 유한집합 S가 주어져 있다. 이 집합의 부분집합 $T \subseteq S$들 중, 임의의 $s \in S$에 대해 $\gcd(s,t) > 1$인 $t \in T$가 존재하게 되는 것의 개수가 홀수임을 증명하여라.

Solution. 부분집합 $T \subseteq S$가 주어져 있을 때,

$$N(T) = \{s \in S : \gcd(s,t) > 1\text{인 } t \in T\text{가 존재}\}$$

를 정의하자. 이 집합은 S들의 원소들 사이에서 gcd가 1보다 큰 원소들을 이은 그래프에서, T와 이웃하는 집합 정도로 해석할 수 있겠다.

우리가 관심있는 것은 $N(T) = S$인 $T \subseteq S$의 개수의 기우성이다. 즉, $N(T) = S$인 것을 판단할 수 있는 필터를 만들어야 한다. 이번 문제에서는 $n = 0$이면 $2^n = 1$은 홀수이지만 $n > 0$이면 2^n이 짝수가 된다는 점을 이용할 것이다. 모든 것을 mod2로 본다면, 2^n은 $n = 0$인 경우에만 0이 아닌 값으로 살아남는 것이다. 우리가 원하는 것은 $S - N(T)$의 원소의 개수가 0인 T의 개수를 세는 것이므로 $S - N(T)$의 부분집합의 개수를 계산하면서 필터를 사용하면 좋을 것 같다.

지금까지 한 논의를 바탕으로, 우선

$$\#\{T \subseteq S : N(T) = S\} \equiv \#\{(T_1, T_2) : N(T_1) \cap T_2 = \emptyset\} \pmod 2$$

임을 알 수 있다. 그렇다면 우변은 왜 홀수가 되는 것일까? $N(T_1) \cap T_2 = \emptyset$이라는 조건을 다시 해석하면, T_1과 T_2가 공통 원소를 가지지 않고 T_1의 원소와 T_2의 원소가 절대 이웃하지 않는 것이다. 즉 $N(T_1) \cap T_2 = \emptyset$은 사실 T_1과 T_2에 대해 대칭인 조건이다. 따라서 (T_1, T_2)가 조건을 만족한다면 (T_2, T_1)도 조건을 만족하므로 $T_1 \neq T_2$라면 두 순서쌍이 자연스럽게 짝지어진다. 남는 것은 $T_1 = T_2$인 경우인데, $T_1 \subseteq N(T_1)$이므로 $T_1 = T_2 = \emptyset$인 경우밖에 없다. 순서쌍들이 둘 씩 짝지어진 이후에 단 하나의 순서쌍이 남으므로 그 개수는 홀수라는 결론을 내릴 수 있다. □

연습문제로 Chevalley-Warning theorem을 사용하는 문제를 하나 남겨놓겠다. 어려운 문제이지만, 주어진 상황에 맞게 다항식을 인위적으로 조작하는 방법을 익힐 수 있는 문제라 생각한다.

연습문제 2.5.A (Erdős-Ginzberg-Ziv theorem)**.** 양의 정수 n과 $2n-1$개의 정수 $a_1, a_2, \ldots, a_{2n-1}$이 있을 때, 이 중 n개의 수를 적당히 골라 더해서 n의 배수를 만들 수 있음을 증명하여라.[9]

2.6 연습문제 모음

연습문제 2.6.A. 양의 정수 a, b, n에 대해, $n \times n$ 크기의 격자판을 $a \times a$ 크기의 정사각형들과 $b \times b$ 크기의 정사각형들로 분할할 수 있다고 한다. 이때 n은 a의 배수가 되거나 b의 배수가 됨을 증명하여라.

연습문제 2.6.B (USAMO 1976 5)**.** 다항식 P, Q, R, S가

$$P(x^5) + xQ(x^5) + x^2R(x^5) = (x^4 + x^3 + x^2 + x + 1)S(x)$$

을 만족시킨다고 할 때, $x - 1$이 $P(x)$를 나눔을 증명하여라.

연습문제 2.6.C. 소수 p와 서로소인 양의 정수 n이 있다. 이때 순서쌍 $(a_1, \ldots, a_{p-1})$ 중 $0 \leq a_1, \ldots, a_{p-1} \leq n-1$이고 $a_1 + 2a_2 + \cdots + (p-1)a_{p-1}$이 p의 배수인 것의 개수를 구하여라.

연습문제 2.6.D (IMO Shortlist 2002 N5)**.** 양의 정수 $m, n \geq 2$와 m^{n-1}의 배수가 아닌 정수 $a_1, \ldots, a_n$이 있다. 이때 모두 0은 아니며 $|e_i| < m$인 정수 $e_1, \ldots, e_n$이 존재하여 $e_1a_1 + e_2a_2 + \cdots + e_na_n$이 m^n의 배수가 됨을 증명하여라.

연습문제 2.6.E (Kömal B.4401)**.** 소수 $p = 3n + 1$에 대해 $1^3, 2^3, \ldots, n^3$을 p로 나눈 나머지들이 모두 다를 수 있는가?

[9] 힌트: 우선 n이 소수인 경우에만 증명하여도 됨을 보여라. 그 다음 $p \mid x_1 + \cdots + x_{2n-1}$과 $p \mid x_1a_1 + \cdots + x_{2n-1}a_{2n-1}$이 각 x_i가 0 또는 1이지만 모두 0은 아닌 공통근을 가짐을 증명하여라.

연습문제 2.6.F. 양의 정수 n과 $a_1, a_2, \dots, a_m$이 주어져 있다. 정수 k에 대해, $f(k)$를 $1 \le c_i \le a_i$이며 $c_1 + \cdots + c_m \equiv k \pmod n$인 순서쌍 $(c_1, \dots, c_m)$의 개수로 정의하자. 이때 함수 f가 상수함수일 필요충분조건은 $a_1, \dots, a_m$ 중 n의 배수가 있는 것임을 보여라.

연습문제 2.6.G (USA TST 2004 2)**.** 양의 정수 n에 대해, 수열 $a_0, a_1, a_2, \dots, a_n$들 중 $a_0, \dots, a_n \in \{1, 2, \dots, n\}$이며 $a_n = a_0$인 것들을 생각하자.

(a) n이 홀수라고 가정하자. 수열들 중 $a_i - a_{i-1} \not\equiv i \pmod n$인 것의 개수를 구하여라.
(b) n이 홀수인 소수라고 가정하자. 수열들 중 $a_i - a_{i-1} \not\equiv i, 2i \pmod n$인 것의 개수를 구하여라.

연습문제 2.6.H (Vietnam TST 2008 6)**.** 집합 $M = \{1, 2, \dots, n\}$의 각 원소는 빨강, 노랑, 파랑 중 하나로 색칠되어 있다. 두 집합

$$S_1 = \{(x, y, z) \in M^3 : x, y, z\text{는 서로 같은 색으로 칠해져 있으며 } n \mid x + y + z\}$$
$$S_2 = \{(x, y, z) \in M^3 : x, y, z\text{는 서로 다른 색으로 칠해져 있으며 } n \mid x + y + z\}$$

을 정의하자. 이때 $2|S_1| \ge |S_2|$임을 증명하여라.

연습문제 2.6.I (IMO Shortlist 1999 C7)**.** 소수 $p > 3$이 있다. 공집합이 아닌 임의의 부분집합 $T \subset \{0, 1, \dots, p-1\}$에 대해,

$$E(T) = \{(x_1, \dots, x_{p-1}) : x_1, \dots, x_{p-1} \in T,\ p \mid x_1 + 2x_2 + \cdots + (p-1)x_{p-1}\}$$

을 정의하자. 이때, $|E(\{0, 1, 2\})| \le |E(\{0, 1, 3\})|$이며 등호가 성립할 필요충분조건은 $p = 5$임을 증명하여라.

연습문제 2.6.J (Miklós Schweitzer 1991 2)**.** 단위원 위에 n개의 점이 놓여있어 그 위의 임의의 점에서 n개의 점들까지의 거리의 곱이 항상 2 이하라 한다. 이때 n개의 점들은 정n각형을 이루어야 함을 증명하여라.

연습문제 2.6.K (Saint-Petersburg 2003)**.** 소수 p, 정수 $n \ge p$와 $a_1, \dots, a_n$이 있다. 각각의 $0 \le k \le n$에 대해, $\{1, \dots, n\}$의 크기 k 부분집합들 $\{s_1, \dots, s_k\}$ 중 $p \mid a_{s_1} + \cdots + a_{s_k}$인 것들의 개수라 하자. 이때

$$p \mid f_0 - f_1 + f_2 - f_3 + \cdots + (-1)^n f_n$$

임을 증명하여라. (여기서 $f_0 = 1$이다.)

연습문제 2.6.L (Crittenden-Vanden Eynden, 1970)**.** 정수 $a_1, \dots, a_n$과 양의 정수 $b_1, \dots, b_n$이 주어져 있다. 임의의 $1 \le x \le 2^n$에 대해 $x \equiv a_i \pmod{b_i}$인 i가 존재한다고 할 때, 임의의 정수 x에 대해서도 $x \equiv a_i \pmod{b_i}$인 i가 존재함을 증명하여라.

연습문제 2.6.M (IMO Shortlist 2012 N8)**.** 임의의 소수 $p > 100$과 정수 r에 대해, p가 $a^2 + b^5 - r$을 나누게 되는 정수 a와 b가 존재함을 증명하여라.

3 1의 제곱근들이 가지는 정수론적 성질

대수적 정수론은 쉽게 말해서 우리가 '수'의 개념을 실수에서 복소수로 확장했듯이, '정수'와 '유리수'의 개념을 확장하는 것이다. 올림피아드 공부를 하면서 가장 많이 볼 수 있는 예는 $\mathbb{Z}[i]$ 위에서의 정수론일 것이다. 복소수들의 집합 $\mathbb{Z}[i]$는

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$

으로 정의된다. 즉 실수부와 허수부가 모두 정수인 복소수들의 집합이다. 이 집합은 덧셈, 뺄셈, 그리고 곱셈에 대해 닫혀있다. 하지만 정수들의 집합 $\mathbb{Z}$와 같이 나눗셈에 대해서는 닫혀있지 않다. 따라서 나누어떨어짐이라는 관계가 의미를 갖는다. 만약 $(a+bi)(x+yi) = c + di$인 정수 x, y가 존재한다면 $a + bi \mid c + di$라고 할 수 있다.

여기서 더 나아가 소수를 정의할 수도 있다. $p \in \mathbb{Z}[i]$가 소수라 함은 $a, b \in \mathbb{Z}[i]$이며 $p = ab$이라면 a나 b 중 $1, -1, i, -i$가 있는 것이다. $\mathbb{Z}$와 조금 차이가 있다면 $\mathbb{Z}[i]$에는 음수, 양수라는 개념이 모호해지기 때문에 $1 + i$도 소수, $-1 - i$도 소수로 간주한다는 것이다. 그러면 $\mathbb{Z}[i]$ 위에서 소인수분해의 유일성도 논할 수 있다.

이렇게 정수나 유리수의 개념을 조금 확장해서 특정한 복소수도 포함하게 만드는 것이 대수적 정수론의 시작이다. 이 장에서는 대수적 정수론에 관한 이야기를 조금 하고 싶다.

3.1 대수적 수와 대수적 정수

대수적 정수론은 다루고자 하는 수를 확장하는 것으로 시작한다. 앞서 복소수를 실계수 다항식의 근으로서 실수에서부터 확장했었다. 이번에는 유리수를 같은 방법으로 확장해 보자.

정의 3.1.1. 어떤 복소수 $\alpha \in \mathbb{C}$에 대해, 0이 아닌 유리계수 다항식 $p(x)$가 존재하여 $p(\alpha) = 0$이 된다면 α를 **대수적 수(algebraic number)**라 부르자. 대수적 수들의 집합은 $\overline{\mathbb{Q}}$라고 표기한다.

실수와 유리수와 가장 큰 차이점은 i를 하나 추가함으로써 실수의 확장은 끝났지만, 유리수에서는 그렇지 않다는 것이다.

연습문제 3.1.A. 집합 $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$에서 방정식 $x^3 = 1$은 근을 $x = 1$ 하나밖에 갖지 않음을 보여라.

즉 i를 추가한 이후에도 추가해야 할 수들이 많다는 이야기이다. 이쯤에서 표기법에 관련하여 짚고 넘어갈 점이 있다. 대수적 수 α에 대해

$$\mathbb{Q}(\alpha) = \{p(\alpha) : p\text{는 유리계수 다항식}\}$$

으로 정의한다.[10] 두 유리계수 다항식의 합, 차, 곱은 다시 유리계수 다항식으므로 $\mathbb{Q}(\alpha)$는 당연히 합, 차, 곱에 대해 닫혀 있다. 그런데 나눗셈에 대해서도 닫혀 있을까?

정리 3.1.2. *임의의 대수적 수 α에 대해 $\mathbb{Q}(\alpha)$는 0이 아닌 수에 의한 나눗셈에 대해 닫혀 있다. 즉, $x, y \in \mathbb{Q}(\alpha)$이고 $x \neq 0$이라면 $y/x \in \mathbb{Q}(\alpha)$이다.*

이 정리는 절대로 당연한 정리가 아니다. 예를 들어 $1/(1+2\sqrt[3]{2}+3\sqrt[3]{4})$를 $\sqrt[3]{2}$에 대한 정수계수 다항식의 형태로 표현할 수 있겠는가? 설령 할 수 있다고 해도 그 방법을 일반화하는 것은 쉽지 않을 것이다. 이 정리를 증명하기 위해서는 다항식에 관한 논의가 선행되어야 한다. 정수론을 잘 공부한 학생에게는 복습과 같이 느껴질 정도로 유리계수 다항식들과 정수 사이에는 공통점이 많다.

변수가 x뿐인 유리계수 다항식들의 집합을 $\mathbb{Q}[x]$로 표기하자. 이때 $\mathbb{Q}[x]$는 당연히 덧셈, 뺄셈, 곱셈에 대해 닫혀있다. 따라서 앞에서 $\mathbb{Z}[i]$에 했던 것처럼 나누어떨어짐이나 소수에 관한 이야기를 할 수 있다.

만약 두 다항식 f, g에 대해 $f(x) = g(x)h(x)$인 $h(x) \in \mathbb{Q}[x]$가 존재한다면, g가 f를 나눈다고 하고 $g \mid f$라고 표기하자. $\mathbb{Q}[x]$에서 1을 나누는 다항식들은 0이 아닌 상수들일 것이다. 즉, $\mathbb{Q} - \{0\}$의 원소들은 모두 1을 나눈다. 이것들이 어떤 의미에서는 가장 '작은' 다항식인 셈이다.

정리 3.1.3 (나머지 정리)**.** *다항식 $f, g \in \mathbb{Q}[x]$이 있고, $g \neq 0$이라 하자. 이때 다음을 만족하며 $\deg r < \deg g$인 다항식 $q, r \in \mathbb{Q}[x]$가 유일하게 존재한다. (단, 편의상 $\deg 0 = -\infty$라 한고, 0이 아닌 상수함수는 $\deg$가 0이라고 한다.)*

$$f(x) = g(x)q(x) + r(x)$$

연습문제 3.1.B. 정리 3.1.3를 증명하여라.

나머지 정리가 있다면, 항상 유클리드 알고리즘을 시행할 수 있게 되어 최대공약수의 개념이 생긴다. 둘 다 0은 아닌 다항식 $f, g \in \mathbb{Q}[x]$가 있다고 하자. 이때 집합

$$S = \{fa + gb : a, b \in \mathbb{Q}[x]\}$$

를 생각할 수 있고, $f = g = 0$은 아니므로 이 집합은 0이 아닌 다항식을 적어도 하나 포함한다. 이제 S에 있는 0이 아닌 다항식들 중 차수가 최소인 다항식 $d_0 = fa_0 + gb_0$를 생각하자. 나머지 정리에 의해 $f = q_1 d_0 + r_1$이며 $\deg r_1 < \deg d_0$인 다항식 $q_1, r_1 \in \mathbb{Q}[x]$가 있고, 이때 $r_1 = f - q_1 d_0 = (1 - q_1 a_0)f - (q_1 b_0)g$이므로 $r_1 \in S$이다. 하지만 d_0가 0이 아닌 S의 원소 중 차수가 최소인 원소이므로 $r_1 = 0$이라는 결론을 얻는다. 따라서 $f = q_1 d_0$이다. 마찬가지로 $g = q_2 d_0$꼴로 표현 가능할 것이다.

이제 $d_0 = fa_0 + gb_0$에 어떠한 유리계수 다항식을 곱해도 다시 S의 원소가 될 것이므로 $\{d_0 a : a \in \mathbb{Q}[x]\} \subseteq S$를 얻는다. 반면 $fa + gb = (q_1 a + q_2 b)d_0$이므로 $fa + gb$는

[10] 사실 올바른 정의는 아니지만, 편의상 이렇게 정의하도록 하겠다.

항상 d_0의 배수이다. 따라서 $S \subseteq \{d_0 a : a \in \mathbb{Q}[x]\}$이다. 두 포함관계에서

$$S = \{d_0 a : a \in \mathbb{Q}[x]\}$$

임이 유도된다. 이때 d_0에 0이 아닌 상수를 곱하여 최고차항의 계수가 1이 되도록 만든 다항식을 d_1이라 하자. 상수는 역수를 취할 수 있으므로 $S = \{d_1 a : a \in \mathbb{Q}[x]\}$도 성립한다. 이때 d_1을 f와 g의 **최대공약수**(**greatest common divisor**)이라고 부르고 $d_1 = \gcd(f, g)$로 표기하자. 정의 상에서 곧바로 도출되는 몇 가지 성질이 있다. 증명은 독자에게 맡기겠다.

명제 3.1.4. *둘 다 0은 아닌 다항식 $f, g \in \mathbb{Q}[x]$가 있다. 이때 다음이 성립한다.*

(i) $\gcd(f, g) \mid f$, $\gcd(f, g) \mid g$
(ii) $fa + gb = \gcd(f, g)$*인* $a, b \in \mathbb{Q}[x]$*가 존재*
(iii) *임의의* $p \in \mathbb{Q}[x]$*에 대해* $\gcd(f + gp, g) = \gcd(f, g)$

다항식 f가 $\deg f \geq 1$이고 $f = gh$로 나타내는 모든 방법에 대해 $\deg g = 0$이거나 $\deg h = 0$이라면, f를 **기약다항식**(**irreducible polynomial**)이라 부르자. 정수에서의 소수와 대응되는 개념이다. 항상 $\deg f = \deg g + \deg h$이므로 당연히 $\deg f = 1$이라면 f는 기약다항식일 것이다.

정리 3.1.5. *만약 f가 기약다항식이고 $f \mid gh$이라면 $f \mid g$이거나 $f \mid h$이다.*

Proof. 최대공약수의 정의에 의해 $\gcd(f, g) = fa_1 + gb_1$이고 $\gcd(f, h) = fa_2 + hb_2$인 $a_1, b_1, a_2, b_2 \in \mathbb{Q}[x]$가 존재할 것이다. 이때

$$\gcd(f, g)\gcd(f, h) = (fa_1 + gb_1)(fa_2 + hb_2) = f(fa_1a_2 + gb_1a_2 + ha_1b_2) + gh(b_1b_2)$$

이므로 f가 $\gcd(f, g)\gcd(f, h)$를 나눔을 확인할 수 있다. 한편 $\gcd(f, g)$는 f를 나누는데 f는 기약다항식이므로 $\gcd(f, g)$는 상수이거나 f에 0이 아닌 상수를 곱한 다항식이 되어야 한다. 마찬가지로 $\gcd(f, h)$도 상수이거나 f에 상수를 곱한 다항식이 될 것이다. 하지만 $f \mid \gcd(f, g)\gcd(f, h)$이므로 $\gcd(f, g)$와 $\gcd(f, h)$가 둘 다 상수가 되는 것은 불가능하다. 따라서 $\gcd(f, g)$와 $\gcd(f, h)$ 중 f에 상수를 곱한 다항식이 존재한다. 일반성을 잃지 않고 $\gcd(f, g) = cf$라 한다면, $cf = \gcd(f, g) \mid g$이므로 $f \mid g$이다. □

두 다항식 f와 g의 근에 대해 알고 있다면, 그 최대공약수에 대해서도 쉽게 알 수 있다.

연습문제 3.1.C. 두 다항식 $f, g \in \mathbb{Q}[x]$가 $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$와 음 아닌 정수 $d_1, \ldots, d_n, e_1, \ldots, e_n$에 대해

$$f(x) = (x - \alpha_1)^{d_1} \cdots (x - \alpha_n)^{d_n}, \quad g(x) = (x - \alpha_1)^{e_1} \cdots (x - \alpha_n)^{e_n}$$

으로 주어져 있다고 하자. 이때

$$\gcd(f,g)(x) = (x-\alpha_1)^{\min\{d_1,e_1\}} \cdots (x-\alpha_n)^{\min\{d_n,e_n\}}$$

이 됨을 증명하여라.

연습문제 3.1.D. 두 다항식 $x^n - 1$과 $x^m - 1$의 최대공약수를 계산하여라.

연습문제 3.1.E (USAMO 1977 1)**.** 다항식 $1+x^n+x^{2n}+\cdots+x^{mn}$이 $1+x+x^2+\cdots+x^m$의 배수가 되는 양의 정수의 순서쌍 (m,n)을 모두 구하여라.

다시 대수적 수에 대한 논의로 돌아가자. α가 대수적 수라고 한다면, 다음과 같은 집합을 생각할 수 있다.

$$S = \{f \in \mathbb{Q}[x] : f(\alpha) = 0\}$$

이 집합은 다행히 α가 대수적 수이므로 0이 아닌 다항식을 포함한다. 따라서 최대공약수를 정의할 때와 마찬가지로 0이 아니며 deg가 최소인 다항식 p_0를 생각할 수 있다. 임의의 $f \in S$에 대해, 나머지 정리에 의해 $f = qp_0 + r$이며 $\deg r < \deg p_0$인 $q, r \in \mathbb{Q}[x]$가 존재하는데, 이 식에 $x = \alpha$를 대입하면 $0 = f(\alpha) = q(\alpha)p_0(\alpha) + r(\alpha) = r(\alpha)$이 되어 $r \in S$임을 알 수 있다. 여기서 또 p_0의 최소성에 의해 $r = 0$이 되고 따라서 f는 p_0의 배수이다. 즉, S는 $\{p_0a : a \in \mathbb{Q}[x]\}$의 부분집합이다. 반대로 p_0의 배수에 α를 대입하면 당연히 0이 될 것이므로 $\{p_0a : a \in \mathbb{Q}[x]\}$는 S의 부분집합이다. 따라서

$$S = \{p_0a : a \in \mathbb{Q}[x]\}$$

를 얻는다. 마찬가지로 p_0에 0이 아닌 상수를 곱해 최고차항의 계수가 1인 다항식 p_1를 만들 수 있고, 이 다항식을 α의 **최소다항식(minimal polynomial)**이라 부른다. 정의에 의해 $f(\alpha) = 0$인 것과 $p_1 \mid f$인 것은 동치가 된다.

이렇게 만들어진 다항식 p_1은 항상 기약다항식이다. 만약 $p_1 = ab$라면, $0 = p_1(\alpha) = a(\alpha)b(\alpha)$이므로 $a(\alpha) = 0$이거나 $b(\alpha) = 0$이 되어야 하는데, 최소성에 의해 a 또는 b가 p_1의 상수배가 되어야 한다. 따라서 p_1는 항상 기약다항식임을 알 수 있다.

연습문제 3.1.F. 복소수 $\alpha = i$와 $\beta = \zeta_3$의 최소다항식을 각각 구하여라.

이제 정리 3.1.2을 증명할 힘이 생겼다.

Proof of Theorem 3.1.2. 집합 $\mathbb{Q}(\alpha)$는 곱셈에 대해 닫혀 있으므로 나눗셈에 대해 닫혀 있음을 보이기 위해서는 역수에 대해 닫혀 있음을 보이면 충분하다. 이제 $f \in \mathbb{Q}[x]$에 대해 $f(\alpha) \neq 0$이라면 $1/f(\alpha) \in \mathbb{Q}(\alpha)$임을 증명하자.

α의 최소다항식을 p라 하자. 그러면 p는 기약다항식이고 $f(\alpha) \neq 0$이므로 $p \nmid f$이다. 두 다항식 p와 f의 최대공약수는 p를 나누어야 하는데, p의 상수배가 될 수는 없으므로 1이 되어야 한다. 즉, $\gcd(p,f) = 1$이고 $1 = pa + fb$인 $a, b \in \mathbb{Q}[x]$가 존재하게 된다.

이제 이 식에 α를 대입하면 $1 = p(\alpha)a(\alpha) + f(\alpha)b(\alpha) = f(\alpha)b(\alpha)$가 되므로 $1/f(\alpha) = b(\alpha)$이다. 따라서 $1/f(\alpha) \in \mathbb{Q}(\alpha)$이다. □

대수적 수가 유리수의 확장이라면, 이번에는 정수의 확장인 대수적 정수를 정의해 보자.

정의 3.1.6. 대수적 수 α에 대해, 그의 최소다항식이 정수계수 다항식이라면, α를 **대수적 정수**(**algebraic integer**)라고 부른다.

연습문제 3.1.G. 유리수들 중 대수적 정수들은 정수($\mathbb{Z}$의 원소)밖에 없음을 보여라.

연습문제 3.1.H. 집합 $\mathbb{Q}(i)$의 원소들 중 대수적 정수를 모두 구하여라.

연습문제 3.1.I. 만약 최고차항의 계수가 1인 정수계수 다항식 p에 대해 $p(\alpha)$라면, α는 대수적 수임을 증명하여라.

따라서 1의 제곱근들은 모두 대수적 정수이다. 대수적 수와 대수적 정수에 관한 가장 놀라운 사실은 다음 정리이다. 조금 더 좋은 증명이 있지만, 그 증명은 선형대수를 사용하기 때문에 대칭다항식을 사용하는 증명을 적어놓았다.

정리 3.1.7. *대수적 수들의 집합 $\overline{\mathbb{Q}}$는 덧셈, 뺄셈, 곱셈, 나눗셈에 대해 닫혀 있다. 또한 대수적 정수들의 집합은 덧셈, 뺄셈, 곱셈에 대해 닫혀 있다.*

Proof. 대수적 수 α에 대해 $1/\alpha$도 대수적 수라는 사실은 쉽게 확인할 수 있고, 대수적 (정)수 α에 대해 $-\alpha$도 대수적 (정)수라는 사실은 더욱 쉽게 확인할 수 있다. 따라서 대수적 수들의 집합과 대수적 정수들의 집합 모두 덧셈, 곱셈에 대해 닫혀 있음을 증명해도 충분하다.

두 대수적 (정)수 α_1과 β_1을 생각하자. 각각의 최소다항식을 p와 q라 하자. 이때 대수학의 기본 정리에 의해 p와 q를

$$p(x) = (x - \alpha_1) \cdots (x - \alpha_n), \quad q(x) = (x - \beta_1) \cdots (x - \beta_m)$$

으로 인수분해할 수 있을 것이다.

다항식

$$F(x) = \prod_{i=1}^{n} \prod_{j=1}^{m} (x - \alpha_i - \beta_j), \quad G(x) = \prod_{i=1}^{n} \prod_{j=1}^{m} (x - \alpha_i \beta_j)$$

를 생각하자. 다항식 F를 전개했을 때 각 항 x^k의 계수는 α_i들과 β_j들로 이루어진 다항식이 될 것이다. 여기서 이 다항식은 정수계수를 갖고, $\alpha_1, \ldots, \alpha_n$에 대해 대칭이며, $\beta_1, \ldots, \beta_m$에 대해서도 대칭이다. 따라서 기본대칭다항식들 $e_k = \sum_{i_1 < \cdots < i_k} \alpha_{i_1} \cdots \alpha_{i_k}$와 $f_k = \sum_{j_1 < \cdots < j_k} \beta_{i_1} \cdots \beta_{i_k}$에 대한 정수계수 다항식으로 표현 가능할 것이다. (이것은 이 통신강좌에서는 다루지 않은 대칭다항식에 관한 이론이다.) 이때 $p(x)$의 계수들이 e_k들이며 $q(x)$의 계수들이 f_k들이다. 그러므로 만약 α와 β가 대수적 정수라면 e_k와 f_k가 모두 정수가 되어 F가 정수계수 다항식이 될 것이고, 만약 α와 β가 단지 대수적 수라면 F는 유리계수 다항식이 될 것이다. 마찬가지로 α와 β가 대수적 정수라면 G도 정수계수 다항식이 되고 대수적 수라면 유리계수 다항식이 된다.

따라서 α와 β가 대수적 (정)수라면 $\alpha + \beta$와 $\alpha\beta$도 대수적 (정)수가 된다. □

이 정리에서 곧바로 알 수 있는 사실은 α가 대수적 수라면 $\mathbb{Q}(\alpha)$의 원소들은 모두 대수적 수라는 것이다. 마찬가지로 대수적 정수 α에 대해

$$\mathbb{Z}[\alpha] = \{p(\alpha) : p\text{는 정수계수 다항식}\}$$

이라 정의하면 $\mathbb{Z}[\alpha]$의 모든 원소도 대수적 정수가 된다.

연습문제 3.1.J. 임의의 대수적 수 α에 대해, 어떤 양의 정수 n이 존재하여 $n\alpha$가 대수적 정수가 됨을 보여라.

3.2 사이클로토믹 다항식

모든 정리를 하나하나 증명하며 헤쳐 나가야 하니 힘든 여정이 아닐 수 없다. 하지만 지루한 부분은 거의 다 지나갔으니 힘을 내보자.

한 번 $x^6 - 1$의 근들을 죽 적어보자. 앞에서 언젠가 말했듯이, 이들 중 몇 개는 1의 3제곱근이기도 하고, 몇 개는 1의 2제곱근이기도 하다. 이것을 그림 3와 같이 묶어서 표현할 수 있다.

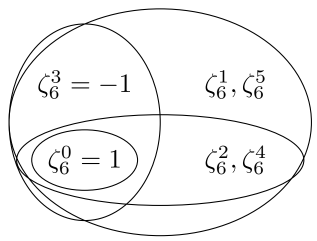

Figure 3: 1의 6제곱근들의 분류

각각의 묶음에 대해, 그들을 근으로 갖는 다항식을 생각해보자. 왼쪽 아래 있는 묶음은 $x-1$의 근이고, 왼쪽 두 묶음은 x^2-1의 근들이므로 왼쪽 위 묶음은 $(x^2-1)/(x-1) = x+1$의 근이다. 아래 두 묶음은 $x^3 - 1$의 근이므로 오른쪽 아래 묶음은 $(x^3 - 1)/(x - 1) = x^2 + x + 1$의 근들이다. 네 묶음은 $x^6 - 1$의 근들이므로 오른쪽 위 묶음은 $(x^6 - 1)/(x - 1)(x+1)(x^2+x+1) = x^2 - x + 1$의 근들이 될 것이다. 이렇게 다항식의 근들을 분류하는 사이에 우리는

$$x^6 - 1 = (x - 1)(x + 1)(x^2 + x + 1)(x^2 - x + 1)$$

으로 다항식을 인수분해하였다.

이것이 사이클로토믹 다항식의 정의이다. 양의 정수 n에 대해 n번째 **사이클로토믹 다항식(cyclotomic polynomial)**을

$$\Phi_n(x) = \prod_{\substack{0 \le k < n \\ \gcd(k,n)=1}} (x - \zeta_n^k)$$

으로 정의하자. 이때

$$x^n - 1 = \prod_{k=0}^{n-1}(x-\zeta_n^k) = \prod_{d|n} \prod_{\substack{0\le k<n \\ \gcd(k,n)=d}} (x-\zeta_n^k) = \prod_{d|n} \prod_{\substack{0\le k/d<n/d \\ \gcd(k/d,n/d)=1}} (x-\zeta_{n/d}^{k/d}) = \prod_{d|n} \Phi_d(x)$$

이 된다. 앞서 살펴본 x^6-1의 인수분해는 $x^6-1 = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x)$였던 것이다.

연습문제 3.2.A. 소수 p에 대해 $\Phi_p(x)$를 구하여라.

정리 3.2.1. *양의 정수 n에 대해 Φ_n은 정수계수 다항식이다.*

Proof. n에 대한 귀납법으로 증명하자. $n=1$인 경우에는 $\Phi_1(x) = x-1$이므로 성립한다. 만약 $n \ge 2$라면

$$x^n - 1 = \Phi_n(x) \prod_{d|n, d<n} \Phi_d(x)$$

이므로 귀납가설에 의해 x^n-1은 $\Phi_n(x)$와 최고차항의 계수가 1인 정수계수 다항식의 곱이다. 즉, $\Phi_n(x)$는 x^n-1을 최고차항의 계수가 1인 정수계수 다항식으로 나눈 다항식인데, 최고차항의 계수가 1이므로 나누는 과정에서 분수가 생길 일이 없다. (이 부분은 학생 여러분들이 스스로 생각해보길 바란다.) 따라서 $\Phi_n(x)$도 정수계수 다항식이 된다. □

정의상 사이클로토믹 다항식은 뫼비우스 μ 함수를 이용하여 쉽게 표현할 수 있게 생겼다.

정의 3.2.2. 뫼비우스 μ 함수(**Möbius μ function**)을 다음과 같이 정의하자.

$$\mu(n) = \begin{cases} 0 & \text{if } p^2 \mid n\text{인 소수 } p \text{ 존재} \\ (-1)^k & \text{if } n = p_1p_2\cdots p_k \end{cases}$$

이 함수의 대표적인 성질은 임의의 양의 정수 $n>1$에 대해 $\sum_{d|n}\mu(d) = 0$ 이라는 것이다. 어렵지 않게 증명할 수 있으니 스스로 해보길 바란다. 참고로 $n=1$이면 좌변의 값은 1이 된다.

연습문제 3.2.B. 사이클로다항식을 $\Phi_n(x) = \prod_{d|n}(x^d-1)^{\mu(n/d)}$ 으로 표현할 수 있음을 보여라.

연습문제 3.2.C. 양의 정수 n에 대해, 1의 원시n제곱근들을 모두 합한 값은 $\mu(n)$임을 보여라.

연습문제 3.2.D. 소수 p의 양의 원시근들 중 p보다 작은 것들의 합을 p로 나눈 나머지를 구하여라.

연습문제 3.2.E. 소수 p와 그의 배수가 아닌 정수 n이 있다. 이때 $x^a \equiv 1 \pmod p$인 최소의 양의 정수 a가 n일 필요충분조건은 $p \mid \Phi_n(x)$인 것임을 보여라.

연습문제 3.2.F. 만약 $x^a \equiv 1 \pmod p$인 최소의 양의 정수 a가 n이라면 $p = nk+1$ 꼴임을 이용하여, $nk+1$꼴의 소수가 무한히 많음을 증명하여라.

연습문제 3.2.G. $p_1, p_2, \ldots, p_n$은 3보다 큰 서로 다른 소수이다. 이때 $2^{p_1 p_2 \cdots p_n} + 1$은 적어도 2^n개의 소인수를 가짐을 증명하여라.

이제 정말 어려운 정리로 이 절을 마무리하자.

정리 3.2.3. *임의의 양의 정수 n에 대해 Φ_n은 기약다항식이다.*

Proof. ζ_n의 최소다항식을 $f(x)$라 하자. 정의에 의해 $\Phi_n(\zeta_n) = 0$이므로 f는 Φ_n을 나눈다. 그러므로 $f(x) = (x - \zeta_n^{i_1}) \cdots (x - \zeta_n^{i_k})$ 형태로 쓸 수 있을 것이다.

$f(\zeta) = 0$인 임의의 ζ와 n의 소인수가 아닌 임의의 소수 p를 생각하자. 우리의 목표는 ζ^p도 f의 근이 된다는 것을 증명하는 것이다. 결론을 부정하여 $f(\zeta^p) \neq 0$이라 가정하자. 우선

$$\prod_{0 \le i \neq j < n} (\zeta_n^i - \zeta_n^j) = \pm \left(\prod_{i=1}^{n-1} (1 - \zeta^i) \right)^n = \pm n^n$$

이 되므로 $f(\zeta^p) = (\zeta^p - \zeta_n^{i_1}) \cdots (\zeta^p - \zeta_n^{i_k})$에 어떤 대수적 정수를 곱하면 n^n을 만들 수 있을 것이다. 즉, $n^n / f(\zeta^p)$는 대수적 정수이다.

한편 $f(x^p) - f(x)^p$를 전개하면, 모든 항에 p가 생기므로 $f(x^p) - f(x)^p = pg(x)$인 정수계수 다항식 g가 존재한다. 여기에 $x = \zeta$를 대입하면 $f(\zeta) = 0$이므로 $f(\zeta^p) = pg(\zeta)$임을 알 수 있다. 그런데 $n^n/(pg(\zeta))$는 대수적 정수이고, $g(\zeta)$도 대수적 정수이므로 두 수의 곱인 n^n/p도 대수적 정수가 되어야 한다. 하지만 p가 n을 나누지 않으므로 모순이다.

따라서 $f(\zeta) = 0$이고 $p \nmid n$이라면 $f(\zeta^p) = 0$이라는 결론을 얻는다. 임의로 $\gcd(n, k) = 1$인 k를 골랐을 때, $k = p_1 p_2 \cdots p_t$로 소인수분해할 수 있다. 이때 $f(\zeta_n) = 0$이고 각각의 p_i는 n을 나누지 않으므로 귀납적으로 $f(\zeta_n^{p_1}) = 0, f(\zeta_n^{p_1 p_2}) = 0, \ldots, f(\zeta_n^k) = 0$을 얻는다. 그러므로 f는 모든 1의 원시n제곱근들을 근으로 가지게 되어 $f = \Phi_n$이다. 따라서 Φ_n은 기약다항식이다. □

연습문제 3.2.H (China TST 2007 1)**.** 소수 $p > 2$이 있다. 모든 내각이 같고 각 변의 길이가 유리수인 p각형은 반드시 정p각형임을 보여라.

3.3 $\mathbb{Q}(\zeta_n)$ 위의 갈루아 이론

복소수를 처음 설명하면서 갈루아 이론의 핵심은 i와 $-i$ 같이 구별이 불가능한 수가 있다는 사실에 있다고 언급했었다. 이제는 이것이 무슨 뜻인지 조금 더 풀어 설명할 필요가 있다.

임의의 $\gcd(n, k) = 1$인 k에 대해, 함수 $\sigma_k : \mathbb{Q}(\zeta_n) \to \mathbb{Q}(\zeta_n)$을 정의할 것이다. 임의의 $x \in \mathbb{Q}(\zeta_n)$은 유리수 $a_0, a_1, \ldots, a_{n-1}$에 대해 $x = a_0 + a_1\zeta_n + a_2\zeta_n^2 + \cdots + a_{n-1}\zeta_n^{n-1}$의 형태로 표현 가능하다. 이 수의 함숫값을

$$\sigma_k(a_0 + a_1\zeta_n + \cdots + a_{n-1}\zeta_n^{n-1}) = a_0 + a_1\zeta_n^k + \cdots + a_{n-1}\zeta_n^{(n-1)k}$$

로 정의하자. 첫 번째로 확인해야 할 것은 이 함수가 잘 정의되었는가이다. 만약 $a_0+\cdots+a_{n-1}\zeta_n^{n-1}=b_0+\cdots+b_{n-1}\zeta_n^{n-1}$인데 $a_0+\cdots+a_{n-1}\zeta_n^{(n-1)k}\neq b_0+\cdots+b_{n-1}\zeta_n^{(n-1)k}$라면 이 함수는 잘 정의되지 못한 것이다. 따라서 이런 일이 발생하지 않음을 증명해주어야 한다.

만약 $a_0+\cdots+a_{n-1}\zeta_n^{n-1}=b_0+\cdots+b_{n-1}\zeta_n^{(n-1)}$이라면 ζ_n은 다항식 $(a_0-b_0)+(a_1-b_1)x+\cdots+(a_{n-1}-b_{n-1})x^{n-1}$의 근이 된다. 따라서 $\Phi_n(x)$의 기약성에 의해 $\Phi_n(x)$은 $(a_0-b_0)+\cdots+(a_{n-1}-b_{n-1})x^{n-1}$을 나누어야 한다. 그러면 ζ_n^k도 $\Phi_n(x)$의 근이므로 $(a_0-b_0)+\cdots+(a_{n-1}-b_{n-1})x^{n-1}$의 근이 되고, $a_0+\cdots+a_{n-1}\zeta_n^{(n-1)k}=b_0+\cdots+b_{n-1}\zeta_n^{(n-1)k}$임을 얻는다. 그러므로 이 함수 σ_k는 잘 정의된 함수이다.

이 함수들은 몇 가지 성질을 갖는다. 증명은 어렵지 않으므로 학생 여러분에게 맡기겠다.

명제 3.3.1. *함수들 $\sigma_k:\mathbb{Q}(\zeta_n)\to\mathbb{Q}(\zeta_n)$은 다음 성질을 갖는다.*

(i) 함수 σ_1은 항등함수이다. (즉, $\sigma_1(x)=x$이다.)
(ii) 만약 $k\equiv k' \pmod n$이라면 $\sigma_k=\sigma_{k'}$이다.
(iii) 두 함수 σ_k와 σ_l을 합성하면 $\sigma_l\circ\sigma_k=\sigma_{kl}$이 된다.
(iv) 임의의 k에 대해 σ_k는 전단사함수이다. (즉, 역함수가 존재한다.)
(v) 임의의 k에 대해 σ_k는 $\mathbb{Z}[\zeta_n]$을 $\mathbb{Z}[\zeta_n]$으로 보낸다.
(vi) 임의의 k와 $x\in\mathbb{Q}$에 대해 $\sigma_k(x)=x$이다.
(vii) 임의의 k와 $x,y\in\mathbb{Q}(\zeta_n)$에 대해 $\sigma_k(x+y)=\sigma_k(x)+\sigma_k(y)$이고 $\sigma_k(xy)=\sigma_k(x)\sigma_k(y)$이다.

앞에서 말한 '구별 불가능함'은 (vi)과 (vii)를 의미하는 것이다. 함수 σ_k가 유리수를 보존하고, 합과 곱도 보존하므로 ζ_n이 ζ_n^k로 움직여도 사실상 아는 것이 유리수밖에 없는 상태에서는 감지해낼 수 없다.

첨자가 $\bmod n$으로 같으면 같은 함수가 되므로, 함수가 $0\le k<n$이며 $\gcd(k,n)=1$인 k에 대해서 총 $\phi(n)$개 있다고 생각해도 무방하다. 또 한 가지 흥미로운 사실은 (vi)의 역이 성립한다는 것이다.

정리 3.3.2. *어떤 $x\in\mathbb{Q}(\zeta_n)$이 $\phi(n)$개의 $0\le k<n$에 대해 모두 $\sigma_k(x)=x$를 만족한다고 하면, $x\in\mathbb{Q}$이다.*

Proof. 정의상 어떤 유리계수 다항식 p가 존재하여 $x=p(\zeta_n)$이 된다. 이때 p를 Φ_n로 나눈 나머지를 r이라 할 때 $p(\zeta_n)=r(\zeta_n)$이므로 $\deg p<\deg\Phi_n=\phi(n)$이라 가정할 수 있다.

편의상 $m=\phi(n)$으로 두자. 앞서 한 논의에 의해 유리수 $a_0,\ldots,a_{m-1}$에 대해 $x=a_0+a_1\zeta_n+a_2\zeta_n^2+\cdots+a_{m-1}\zeta_n^{m-1}$이라 할 수 있다. 그러면 우리가 가진 조건은 임의의 $\gcd(k,n)=1$인 k에 대해

$$(a_0-x)+a_1\zeta_n^k+a_2\zeta_n^{2k}+\cdots+a_{m-1}\zeta_n^{(m-1)k}=0$$

으로 쓸 수 있다. 생각해보면 이것은 1차 연립방정식일 뿐이므로 다음과 같이 행렬로 표기할 수 있다.

$$\begin{pmatrix} 1 & \zeta_n^{k_1} & \cdots & \zeta_n^{(m-1)k_1} \\ 1 & \zeta_n^{k_2} & \cdots & \zeta_n^{(m-1)k_2} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta_n^{k_m} & \cdots & \zeta_n^{(m-1)k_m} \end{pmatrix} \begin{pmatrix} a_0 - x \\ a_1 \\ \vdots \\ a_{m-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

왼쪽에 있는 $m \times m$ 행렬은 반데몬드 행렬의 형태를 가짐을 확인할 수 있다. 따라서 그 행렬식은

$$\prod_{1 \le i < j \le m} (\zeta_n^{k_j} - \zeta_n^{k_i}) \neq 0$$

이 되어 이 행렬은 역행렬을 가짐을 알 수 있다. 역행렬을 왼쪽에 곱해주면 $a_0 - x = a_1 = \cdots = a_{m-1} = 0$을 얻는다. 따라서 $x = a_0$는 유리수이다. $\square$

방금 증명한 정리는 보기와는 다르게 아주 높은 활용도를 가지고 있다. 한 가지 간단한 예를 들어보자. 임의의 $x \in \mathbb{Q}(\zeta_n)$에 대해

$$A = \prod_{\substack{0 \le k < n \\ \gcd(k,n)=1}} \sigma_k(\zeta_n)$$

을 생각하자. 이 수에 σ_l을 씌우면

$$\sigma_l(A) = \sigma_l\left(\prod_{\substack{0 \le k < n \\ \gcd(k,n)=1}} \sigma_k(\zeta_n) \right) = \prod_{\substack{0 \le k < n \\ \gcd(k,n)=1}} \sigma_l(\sigma_k(\zeta_n)) = \prod_{\substack{0 \le k < n \\ \gcd(k,n)=1}} \sigma_{lk}(\zeta_n) = A$$

으로 바뀌지 않는다. 따라서 정리 3.3.2에 의해 이 수는 유리수가 된다.

조금 더 흥미로운 예시를 들어보겠다. 다항식

$$\prod_{i=0}^{n-1} (a_0 + a_1\zeta_n^i + a_2\zeta_n^{2i} + \cdots + a_{n-1}\zeta_n^{(n-1)i})$$

를 전개해보려는 생각을 한 적이 한 번쯤은 있을 것이다. $n = 2$일 때는 $a_0^2 - a_1^2$이 되고, $n = 3$일 때는 $a_0^3 + a_1^3 + a_2^3 - 3a_0a_1a_2$가 되는 다항식이다. 이때 이 다항식의 모든 계수가 정수임을 보이고 싶다.

우선 각 계수들에 σ_k를 취해보자. σ_k는 곱과 합을 보존하므로

$$\begin{aligned} \sigma_k\left(\prod_{i=0}^{n-1} (a_0 + a_1\zeta_n^i + \cdots + a_{n-1}\zeta_n^{(n-1)i}) \right) &= \prod_{i=0}^{n-1} (a_0 + a_1\zeta_n^{ki} + \cdots + a_{n-1}\zeta_n^{(n-1)ki}) \\ &= \prod_{i=0}^{n-1} (a_0 + a_1\zeta_n^i + \cdots + a_{n-1}\zeta_n^{(n-1)i}) \end{aligned}$$

가 된다. 따라서 이 다항식의 계수는 모두 유리수이다. 한편 ζ_n^{ki}들은 모두 대수적 정수이고, 고작 이들을 곱하고 더했을 뿐이므로 모든 계수는 대수적 정수여야 한다. 계수들이 유리수이며 대수적 정수이므로 정수여야 한다는 결론을 얻을 수 있다.

예제 3.3.3. 양의 정수 n과 복소수 z_1, z_2, z_3, z_4, z_5이 $z_1^n = z_2^n = z_3^n = z_4^n = z_5^n = 1$을 만족시킨다. 만약 $z_1 + z_2 + z_3 + z_4 + z_5 \neq 0$이라면 $|z_1 + z_2 + z_3 + z_4 + z_5| > 5^{-n}$임을 증명하여라.

Solution. 각각의 z_i는 1의 n제곱근이므로 당연히 $\mathbb{Z}[\zeta_n] \subset \mathbb{Q}(\zeta_n)$에 속한다. 따라서 각각의 $\gcd(k, n) = 1$인 k에 대해 $\sigma_k(z_1 + z_2 + z_3 + z_4 + z_5) \in \mathbb{Z}[\zeta_n]$이다.

이제 이들을 모두 곱한

$$A = \prod_{\substack{0 \leq k < n \\ \gcd(k,n)=1}} \sigma_k(z_1 + z_2 + z_3 + z_4 + z_5)$$

를 생각하자. 앞서 설명한 것과 같은 이유로 A는 σ_l의 고정점이 되어 유리수이다. 또한 A는 $\mathbb{Z}[\zeta_n]$의 원소들의 곱이므로 대수적 정수이다. 따라서 A는 정수가 된다. 한편 σ_k는 전단사함수이고 $\sigma_k(0) = 0$이므로 $\sigma_k(z_1 + \cdots + z_5) \neq 0$이고, 따라서 $A \neq 0$이다.

A의 절댓값을 계산해보면

$$1 \leq |A| = \prod_{\substack{0 \leq k < n \\ \gcd(k,n)=1}} |\sigma_k(z_1 + z_2 + z_3 + z_4 + z_5)|$$

인데, 각각의 $\sigma_k(z_1 + \cdots + z_5)$는 다섯개의 1의 제곱근의 합이므로 절댓값은 5 이하다. 그러므로

$$|z_1 + z_2 + z_3 + z_4 + z_5| = |\sigma_1(z_1 + z_2 + z_3 + z_4 + z_5)| \geq 5^{-\phi(n)+1} > 5^{-n}$$

이다. □

마지막으로 지금까지 배운 내용을 종합하는 문제 하나를 남겨놓겠다.

연습문제 3.3.A. 소수 p, q와 양의 정수 r은 $q \mid p-1$, $q \nmid r$과 $p > r^{q-1}$을 만족시킨다. 정수 $a_1, a_2, \ldots, a_r$에 대해

$$a_1^{(p-1)/q} + a_2^{(p-1)/q} + \cdots + a_r^{(p-1)/q}$$

가 p의 배수라면, $a_1, \ldots, a_r$ 중 p의 배수가 적어도 하나 존재함을 증명하여라.