Number Fields
(수체)
Version 1.0

Author : Daniel A. Marcus
Translated by Dyne

Aug 20, 2023

Contents (목차)

1 | A Special Case of Fermat's Conjecture (Fermat 가설의 특수한 경우)

대수적 수론은 근본적으로 **수체(number field)**, 즉 유리수체 $\mathbb{Q}$의 유한 확대들에 대한 연구이다. 이러한 체들은 유리수만을 수반하는 것처럼 보이는 문제들을 해결하는 데 유용하다. 예를 들어 다음 문제를 고려하자:

모든 **Pythagoras 원시 3조(primitive Pythagorean triple)**
(i.e. 공통 인수를 갖지 않는 $x^2+y^2=z^2$의 정수해)들을 찾아라.

우리가 이러한 3조를 가지고 있으며 방정식을 mod 4에서 고려한다면 z가 홀수여야 함을 즉시 알 수 있다. 이는 나중에 사용될 것이다. 이제 수체(이 경우 $\mathbb{Q}[i]=\{a+bi : a,b\in\mathbb{Q}\}$)를 이 문제에 도입하겠다: 방정식의 좌변을 인수분해하면 다음을 얻는다.

$$(x+yi)(x-yi)=z^2$$

그러므로 우리는 **Gauss 정수환(ring of Gaussian integers)** $\mathbb{Z}[i]=\{a+bi : a,b\in\mathbb{Z}\}$에서의 곱셈적 문제를 얻는다. $\mathbb{Z}[i]$가 유일 인수분해 정역임은 잘 알려져 있다(이 장의 마지막 부분의 exercise 7을 참조하라): 0이 아닌 모든 Gauss 정수는 Gauss 소수들의 곱으로 (순서 및 가역원 하에서) 유일하게 표현될 수 있다. 우리는 이 사실을 이용하여 $x+yi$가 어떠한 Gauss 정수 α와 가역 Gauss 정수 u에 대하여 $u\alpha^2$ 형태여야 함을 보이겠다. $\alpha=m+ni$로 표기하고 $\mathbb{Z}[i]$의 가역원들이 ±1과 $\pm i$뿐임을 관찰하면 (exercise 2를 참조하라) 다음을 얻는다.

$$\{x,y\}=\{\pm(m^2+n^2),\pm 2mn\} \quad , \quad z=\pm(m^2+n^2)$$

m과 n이 서로 소여야 하며 동시에 홀수이지는 않아야 함이 명백하다. (그렇지 않으면 x,y,z가 공통 인수를 가질 것이다.) 임의의 m,n과 부호의 선택에 대하여 Pythagoras 원시 3조를 얻음을 간단히 보일 수 있다. 이에 더해 양수 m,n만을 선택하더라도 등장하는 Pythagoras 원시 3조들이 줄어들지 않는다.

그러므로 임의의 원시근 $x+yi$가 $u\alpha^2$ 형태임을 보이면 문제가 해결될 것이다. 이를 위해서는 만약 π가 $x+yi$의 Gauss 소인수이면 π가 $x+yi$의 짝수 회 중복된 인수라는 사실을 보이면 충분하다: 어떠한 e에 대하여 $\pi^e|x+yi$이며 $x^{e+1}\nmid x+yi$이다. $(x+yi)(x-yi)=z^2$이며 π가 명백히 z^2의 짝수 회 중복된 인수이므로 (z에서의 중복 수의 2배) $\pi\nmid x-yi$임을 보이면 충분하다.

그러므로 π가 $x+yi$와 $x-yi$의 공통인수라 가정하고 모순을 얻자. 이들을 더하면 $\pi|2x$를 얻는다. 또한 $\pi|z$이다. 그러나 $2x$와 z는 서로 소 정수들이다. (z가 홀수라는 사실과 만약 x,z가 비자명 공통 인수를 가지면 x,y,z가 이러한 공통 인수를 가져야 한다는 사실을 상기하라.) 그러므로 정수 m,n이 존재하여 $2xm+zn=1$을 만족시킨다. 그러나 그 경우 $\mathbb{Z}[i]$에서 $\pi|1$이지만 π는 가역원이 아니라 소수이므로 이는 불가능하다.

그러므로 체 $\mathbb{Q}[i]$에서 작업하는 것으로 모든 Pythagoras 원시 3조를 결정했다.

이것이 매우 성공적이었으므로 우리는 동일한 발상을 $n>2$에 대한 방정식 $x^n+y^n=z^n$에 적용할 것이다. Fermat는 널리 알려진 방주에서 $n>2$인 경우 0이 아닌 정수해가 존재하지 않음을 증명했다 주장했다. 이는 **Fermat의 마지막 정리(Fermat's last theorem)** 또는 **Fermat 추측(Fermat's conjecture)**라 알려져 있다. 3세기가 넘는 시간 동안 이는 수학의 가장 유명한 미해결 문제였다.[1]

Pythagoras 원시 3조에 관한 우리의 결과를 이용하면 $n=4$의 경우 Fermat가 옳았으며 따라서 (자동적으로) 임의의 4의 배수에 대해서도 그러함을 알 수 있다. (exercise 15를 참조하라.) $n=p$에서 해가 존재하지 않는다면 n이 p의 배수인 경우에도 해가 존재하지 않으므로 n이 홀수 소수 p인 경우를 고려하면 충분하다. 그러므로 문제는 p가 홀수 소수인 경우 $x^p+y^p=z^p$가 0이 아닌 정수해 x,y,z를 갖지 않음을 보이는 것이다.

어떠한 홀수 소수 p에 대하여 해 $x,y,z\in\mathbb{Z}-\{0\}$가 존재한다 가정하자. 우리는 명백히 x,y,z가 공통 인수를 갖지 않는다 가정할 수 있다. (만약 공통 인수가 존재한다면 이러한 인수로 나눠라.) 우리는 모순을 얻고자 한다. 논의를 두 경우로 분할하는 것이 편리하다: p가 x,y,z 중 어떠한 것의 인수도 아닌 경우 (case

[1] Fermat의 마지막 정리는 1993-94년에 마침내 Andrew Wiles에 의해 타원곡선론의 개념들을 사용하여 증명되었다.

1), 또는 p가 이들 중 정확히 하나의 인수인 경우 (case 2). (만약 p가 이들 중 하나 초과의 인수이면 이는 3개 모두를 나눌 것이며 모순이다.)

case 1만을 고려하자. $x^3 + y^3 = z^3$이 case 1 해를 갖지 않음을 간단히 보일 수 있다: 만약 x, y, z가 3의 배수가 아니면 이들의 3승들이 $\equiv \pm 1 \pmod 9$이므로 $x^3 + y^3 \not\equiv z^3 \pmod 9$이다.

이제 $p > 3$이고 x, y, z가 p의 배수가 아니며 $x^p + y^p = z^p$라 가정하자. 좌변을 분해하면 다음을 얻는다.

$$(x + y)(x + y\omega)(x + y\omega^2) \cdots (x + y\omega^{p-1}) = z^p \tag{1.1}$$

여기에서 ω는 단위의 p승근 $e^{2\pi i/p}$이다. (이것이 왜 참인지를 보이기 위해서는 $1, \omega, \omega^2, \ldots, \omega^{p-1}$이 다항식 $t^p - 1$의 p개 근들이며 따라서 다음 항등식이 성립함을 기억해 두라.

$$t^p - 1 = (t - 1)(t - \omega)(t - \omega^2) \cdots (t - \omega^{p-1}) \tag{1.2}$$

이 방정식에서 변수 t에 수 $\frac{-x}{y}$를 대입하면 (1.1)이 따라온다.)

그러므로 수체 $\mathbb{Q}[\omega]$(사실 부분환 $\mathbb{Z}[\omega]$)에서의 곱셈적 문제를 얻는다.[2] Kummer는 $\mathbb{Z}$와 $\mathbb{Z}[i]$의 유일 인수분해 성질이 환 $\mathbb{Z}[\omega]$로 일반화되는지를 고려하는 것으로 Fermat 가설을 증명하려 시도했다. 그러나 불운하게도 유일 인수분해가 성립하지 않는다. 예를 들어 $p = 23$인 경우 $\mathbb{Z}[\omega]$의 모든 원소가 **기약원(irreducible element)**(i.e. 가역원이 아닌 원소 $\alpha \in \mathbb{Z}[\omega]$ 중 $\alpha = \beta\gamma$이면 β 또는 γ가 가역원이도록 하는 것)들로 유일하게 분해되지 않는다. (exercise 20을 참조하라.) 다른 말로 하면 $p = 23$에 대한 $\mathbb{Z}[\omega]$는 유일 인수분해 정역(UFD)이 아니다. 그러나 이는 23 미만의 모든 소수에 대하여 UFD이다. 이러한 소수에 대하여 $x^p + y^p = z^p$이 case 1 해를 갖지 않음을 간단히 보일 수 있다.

이러한 논의는 다음과 같이 체계화될 수 있다: $\mathbb{Z}[\omega]$가 UFD라 가정하면 $x + y\omega$가 어떠한 $\alpha \in \mathbb{Z}[\omega]$와 어떠한 가역원 $u \in \mathbb{Z}[\omega]$에 대하여 $u\alpha^p$ 형태임을 보일 수 있다. 그 경우 x, y가 p의 배수가 아니면 방정식 $x + y\omega = u\alpha^p$가 $x \equiv y \pmod p$임을 함의함을 보일 수 있다. (세부사항을 위해서는 exercise 16-28을 참조하라.) 마찬가지로 $x^p + (-z)^p = (-y)^p$로 표현하면 $x \equiv -z \pmod p$를 얻는다. 그러나 그 경우 다음이 성립한다.

$$2x^p \equiv x^p + y^p = z^p \equiv -x^p \pmod p$$

이는 $p | 3x^p$임을 함의한다. $p \nmid x$이며 $p \neq 3$이므로 이는 모순이다. 그러므로 Fermat 추측의 case 1이 $\mathbb{Z}[\omega]$가 UFD이도록 하는 모든 소수 p에 대하여 수립된다.

다른 소수에 대해서는 무엇을 할 수 있는가? $\mathbb{Z}[\omega]$에서의 유일 인수분해는 방정식 (1.1)에서 $x + y\omega = ua^p$임을 연역할 목적으로만 사용되었다; 이를 다른 방법으로 연역할 수도 있을까? 특정한 p의 값에 대해서는 답이 '그렇다'이며 이는 예시 $p = 23$을 포함한다. 이는 유일 인수분해의 올바른 일반화에 관한 Dedekind의 놀라운 발견에서 기인한다: $\mathbb{Z}[\omega]$의 원소들이 기약원들로 유일하게 분해되지 않을 수 있음에도 불구하고 이 환에서의 아이디얼들은 항상 소 아이디얼들로 유일하게 분해된다.[3] 이를 이용하면 주 아이디얼 $(x + y\omega)$가 어떠한 아이디얼 I의 p승임을 어렵지 않게 보일 수 있다. (exercise 19, 20을 참조하라.) (아래에서 정의할) 정칙 소수라 불리는 특정 p들에 대하여 I 자신이 주 아이디얼 (α)여야 하며 따라서 다음이 성립함이 따라온다.

$$(x + y\omega) = I^p = (\alpha)^p = (\alpha^p)$$

그러므로 우리는 다시 어떠한 가역원 u에 대하여 $x + y\omega = u\alpha^p$임을 알 수 있다. 이전과 같이 이는 $x \equiv y \pmod p$임을 함의하며 모순이 따라온다. 그러므로 Fermat 가설의 case 1이 (이제 정의할) 모든 정칙 소수에 대하여 수립된다.

$\mathbb{Z}[\omega]$의 아이디얼들의 집합에는 다음에 의해 정의된 동치 관계 $\sim$이 존재한다: 아이디얼 A, B에 대하여,

$$A \sim B \text{ iff 어떠한 } \alpha, \beta \in \mathbb{Z}[\omega] \text{에 대하여 } \alpha A = \beta B$$
(이것이 동치 관계임을 검증하라.)

$\sim$ 하에서 아이디얼들의 동치류가 유한 개만 존재함이 밝혀진다. (chapter 5를 참조하라.) 동치류의 개수는 환 $\mathbb{Z}[\omega]$의 **유수(class number)**라 불리며 문자 h로 표기된다. 그러므로 h는 p의 함수이다.

Definition. 소수 p가 **정칙(regular)**임은 $p \nmid h$인 것으로 정의된다.

---

[2] $\mathbb{Q}[\omega] = \{a_0 + a_1\omega + \cdots + a_{p-2}\omega^{p-2} : a_i \in \mathbb{Q}\ \forall i\}$;

$\mathbb{Z}[\omega] = \{a_0 + a_1\omega + \cdots + a_{p-2}\omega^{p-2} : a_i \in \mathbb{Z}\ \forall i\}$.

[3] 사실 이러한 발견은 Kummer에 의한 것이다. Bulletin of the American Mathematical Society, 2 (1980), p. 327. -Ed.의 Harold Edward의 서평을 참조하라.

p가 정칙 소수인 경우 (방정식 $x + y\omega = I^p$에서 등장하는) I가 왜 주 아이디얼이어야 하는지를 설명하자면 아이디얼류들이 자명한 방식으로 곱해질 수 있음을 먼저 언급해야 한다: 두 아이디얼류의 곱은 각 아이디얼류에서 아이디얼을 하나씩 선택하고 이들을 곱한 후 곱이 속한 아이디얼류를 취하는 것으로 정의된다. 이는 잘 정의된다: 곱의 결과로 얻어진 아이디얼류는 특정한 아이디얼의 선택에 의존하지 않으며 원래 아이디얼류에만 의존한다. (이를 증명하라.) 이러한 방식의 곱셈 하에서 아이디얼류들은 사실 군을 형성한다. 항등원은 모든 주 아이디얼들로 구성된 아이디얼류 C_0이다. (이는 실제로 아이디얼류이다; exercise 31을 참조하라.) 역원의 존재성은 chapter 3에서 수립될 것이다. 그러므로 아이디얼류들은 **아이디얼류군(ideal class group)**이라 불리는 유한 가환군을 형성한다. 만약 p가 정칙이면 이러한 군은 명백히 위수 p의 원소를 갖지 않는다. 그러므로 I^p가 주 아이디얼이면 I도 주 아이디얼임이 따라온다: I가 속한 아이디얼류를 C라 하면 C^p는 I^p가 속한 아이디얼류 C_0이다. C_0가 아이디얼류군의 항등원이고 C가 위수 p일 수 없으므로 $C = C_0$임이 따라온다. 이는 I가 주 아이디얼임을 보여준다.

위에서 언급한 것과 같이 이는 모순으로 이어지며 따라서 p가 정칙 소수인 경우 $x^p + y^p = z^p$가 case 1 해(i.e. $p \nmid xyz$인 해)를 갖지 않음을 보여준다. 정칙 소수의 경우 case 2 해도 존재하지 않음을 보이는 것도 (더 복잡하지만) 가능하다. (이를 위해서는 Borevich and Shafarevich - *Number Theory*, p. 378-381를 참조하라.) 그러므로 Fermat 추측은 모든 정칙 소수 p에 대하여 증명될 수 있으며 따라서 적어도 하나의 정칙 소인수를 가지는 모든 정수 n에 대하여 증명될 수 있다. 그러나 불운하게도 비정칙 소수가 무한히 많이 존재한다. (e.g. $37, 59, 67$) 반면에 무한히 많은 정칙 소수가 존재하는지는 알려져 있지 않다.

어떠한 경우에도 Fermat 추측을 증명하려는 시도는 환 $\mathbb{Z}[\omega]$에 대한 여러 문제들을 고려하는 것으로 이어진다: 이 환의 가역원들은 무엇인가? 기약원들은 무엇인가? 원소들이 유일하게 분해되는가? 그렇지 않다면, 아이디얼의 소 아이디얼로의 분해에 대하여 무엇을 말할 수 있는가? 아이디얼류가 몇 개나 존재하는가?

이러한 문제들을 조사하는 것은 고전 대수적 수론의 많은 부분을 형성한다. 더 정확히 말하자면 $\mathbb{Q}[\omega]$뿐만 아니라 임의의 수체의 부분환에 대하여 이러한 문제들을 묻는다. 모든 수체에는 $\mathbb{Z}[\omega]$와 유사한 환이 존재하며 이곳에서 흥미로운 답을 얻는다.

Exercises (연습문제)

1-9: $N : \mathbb{Z}[i] \to \mathbb{Z}$를 $N(a + bi) = a^2 + b^2$로 정의하라.

1.

2 | Number Fields and Number Rings (수체와 수환)

수체(number field)는 $\mathbb{Q}$ 상에서 유한 차수(벡터 공간으로서의 차원)를 가지는 $\mathbb{C}$의 부분체이다. 우리는 이러한 모든 체가 어떠한 대수적 수 $\alpha \in \mathbb{C}$에 대하여 $\mathbb{Q}[\alpha]$ 형태임을 알고 있다. (Appendix B를 참조하라.) 만약 α가 $\mathbb{Q}$ 상에서의 n차 기약다항식의 근이면 다음이 성립한다.

$$\mathbb{Q}[\alpha] = \left\{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_i \in \mathbb{Q}\ \forall i\right\}$$

또한 이러한 형태의 표현은 유일하다; 다른 말로 하면 $\{1, \alpha, \ldots, \alpha^{n-1}\}$은 $\mathbb{Q}$ 상에서의 벡터 공간 $\mathbb{Q}[\alpha]$의 기저이다.

우리는 이미 $\omega = e^{2\pi i/p}, p$ 소수에 대한 체 $\mathbb{Q}[\omega]$를 고려했다. 이 경우 $n = p - 1$이었음을 상기하라. 더 일반적으로 $\omega = e^{2\pi i/m}, m$이 소수일 필요는 없는 경우를 고려하자. 체 $\mathbb{Q}[\omega]$는 **m번째 원분체(mth cyclotomic field)**라 불린다. $m = 0, 1$에 대하여 각각 $\omega = 1, -1$이므로 처음의 2개 원분체는 모두 $\mathbb{Q}$이다. 3번째 원분체는 6번째 원분체와 같다: $\omega = e^{2\pi i/6}$이라 하면 $\omega = -\omega^4 = -(\omega^2)^2$이며 이는 $\mathbb{Q}[\omega] = \mathbb{Q}[\omega^2]$임을 보여준다. 일반적으로 홀수 m에 대하여 m번째 원분체는 $2m$번째 원분체와 같다. (만약 $\omega = e^{2\pi i/2m}$)이면 $\omega = -\omega^{m+1} \in \mathbb{Q}[\omega^2]$임을 보여라.) 반면에 짝수 m ($m > 0$)에 대한 원분체들이 모두 서로 다름을 보이겠다. 이는 근본적으로 (이 절에서 증명할) m번째 원분체의 $\mathbb{Q}$ 상에서의 차수가 다음 집합의 원소의 개수 $\varphi(m)$이라는 사실에서 따라온다.

$$\{k : 1 \le k \le m, (k, m) = 1\}$$

수체들의 다른 무한 족은 완전제곱수가 아닌 $m \in \mathbb{Z}$에 대한 **2차수체(quadratic field)** $\mathbb{Q}[\sqrt{m}]$들로 구성된다. 이러한 체들은 명백히 $\mathbb{Q}$ 상에서 차수 2를 가지며 기저 $\{1, \sqrt{m}\}$을 가진다. $\mathbb{Q}[\sqrt{12}] = \mathbb{Q}[\sqrt{3}]$ 등이 성립하므로 우리는 제곱 없는 수 m을 고려하면 충분하다. 제곱 없는 정수 m에 대한 $\mathbb{Q}[\sqrt{m}]$들은 모두 서로 다르다. (exercise 1을 참조하라.) $m > 0$에 대한 $\mathbb{Q}[\sqrt{m}]$은 **실 2차수체(real quadratic field)**라 불린다; $m < 0$에 대한 $\mathbb{Q}[\sqrt{m}]$은 **허 2차수체(imaginary quadratic field)**라 불린다. 그러므로 $\mathbb{Q}[i]$는 허 2차수체이며 원분체이다. $\mathbb{Q}[\sqrt{-3}]$도 원분체임을 기억해 두라. (어느 것인가?)

Chapter 1의 p번째 원분체 $\mathbb{Q}[\omega]$에서 작업하면서 환 $\mathbb{Z}[\omega]$가 어떠한 좋은 성질을 만족시킴을 보일 것이라 했다: 예를 들어 모든 아이디얼이 소 아이디얼들로 분해된다. 이는 더 일반적으로 임의의 원분체에서의 환 $\mathbb{Z}[\omega]$에 대하여 참이다. 이는 특정한 m의 값에 대한 $\mathbb{Z}[\sqrt{m}]$에서도 참이다. 그러나 이는 예를 들어 $\mathbb{Z}[\sqrt{-3}]$에서 실패한다. (exercise 2를 참조하라.) 그럼에도 불구하고 우리는 $\mathbb{Q}[\sqrt{-3}]$이 아이디얼이 소 아이디얼들로 유일하게 분해되도록 하는 다음의 환을 부분환으로 가짐을 알고 있다.

$$\mathbb{Z}\left[\frac{-1+\sqrt{3}}{2}\right] = \mathbb{Z}[\omega] \quad , \quad \omega = e^{2\pi i/3}$$

이 환은 다음의 모든 수들로 구성된다.

$$\frac{a+b\sqrt{-3}}{2} \quad , \quad a, b \in \mathbb{Z} \quad , \quad a \equiv b \pmod 2$$

(이를 검증하라; $\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$임을 상기하라.) 우리는 모든 수체가 이러한 유일 인수분해 성질을 가지는 (체가 $\mathbb{Q}$가 아닌 경우) $\mathbb{Z}$ 이외의 환을 포함함을 보일 것이다; 이는 체에 속한 대수적 정수들로 구성된다.

Definition. 복소수가 **대수적 정수(algebraic integer)**라는 것의 정의는 어떠한 $\mathbb{Z}$-**1계수(monic)**(i.e. 최고차 계수 1)다항식의 근인 것이다.

다항식이 $\mathbb{Q}$ 상에서 기약이어야 한다고 요구하지 않았음을 기억해 두라. 그러므로 우리는 $\omega = e^{2\pi i/m}$이 $x^m - 1$의 근이므로 대수적 정수임을 간단히 보일 수 있다. 그러나 모든 대수적 정수 α가 어떠한 $\mathbb{Z}$-1계수 기약다항식의 근이라는 사실이 성립한다.

Theorem 1. α가 대수적 정수이며 f가 α를 근으로 가지는 $\mathbb{Z}$-1계수다항식 중 최소 차수인 것이라 하자. 그 경우 f는 $\mathbb{Q}$ 상에서 기약이다. (이와 동치로, α를 근으로 가지는 $\mathbb{Q}$-1계수 기약다항식은 $\mathbb{Z}$-계수이다.)

Lemma. f가 $\mathbb{Z}$-1계수다항식이며 g, h가 $\mathbb{Q}$-계수 1계수다항식이고 $f = gh$라 하자. 그 경우 g, h는 사실 $\mathbb{Z}$-계수이다.

Proof. m(resp. n)이 mg(resp. nh)가 $\mathbb{Z}$-계수이도록 하는 최소 양의 정수라 하자. 그 경우 mg의 계수들은 공통 인수를 갖지 않는다. (이들이 만약 공통 인수를 가진다면 m이 더 작은 정수로 대체될 수 있음을 보여라; g가 1계수라는 사실을 사용하라.) nh의 계수들에 대해서도 같은 것이 참이다. 이를 이용하면 $m = n = 1$임을 보일 수 있다: 만약 $mn > 1$이라 하고 mn의 임의의 소인수 p를 취하고 방정식 $nmf = (mg)(nh)$를 고려하자. 계수들을 $\bmod p$로 축약하면 (축약의 결과물을 상선으로 표기할 경우) $0 = \overline{mg} \cdot \overline{nh}$를 얻는다. (환준동형사상 $\mathbb{Z}[x] \to \mathbb{Z}_p[x]$를 적용했다.) 그러나 $\mathbb{Z}_p[x]$가 정역이며 ($\mathbb{Z}[p]$가 정역이기 때문이다; 간단히 보일 수 있다) 따라서 $\overline{mg} = 0$ 또는 $\overline{nh} = 0$이다. 그러나 이 경우 p가 mg 또는 nh의 모든 계수들의 인수이다; 위에서 보인 것과 같이 이는 모순이다. 그러므로 $m = n = 1$이며 따라서 $g, h \in \mathbb{Z}[x]$이다. □

Proof of Theorem 1. 만약 f가 기약이 아니면 $\mathbb{Q}[x]$에 속한 상수가 아닌 다항식 g, h에 대하여 $f = hg$이다. 일반성을 잃지 않고 g, h가 1계수라 가정할 수 있다. 그 경우 보조정리에 의해 $g, h \in \mathbb{Z}[x]$이다. 그러나 α는 g 또는 h의 근이며 g, h가 모두 f보다 작은 차수를 가진다. 이는 모순이다. □

Corollary 1. $\mathbb{Q}$에 속한 대수적 정수들은 통상적인 정수들밖에 없다. □

Corollary 2. m이 제곱 없는 정수라 하자. 2차수체 $\mathbb{Q}[\sqrt{m}]$에서의 대수적 정수들의 집합은 다음과 같다.

$$\begin{cases} \left\{a + b\sqrt{m} : a, b \in \mathbb{Z}\right\} & (m \equiv 2 \text{ or } 3 \pmod 4) \\ \left\{\dfrac{a + b\sqrt{m}}{2} : a, b \in \mathbb{Z}, a \equiv b \pmod 2\right\} & (m \equiv 1 \pmod 4) \end{cases}$$

Proof. $\alpha = r + s\sqrt{m}, r, s \in \mathbb{Q}$라 하자. 만약 $s \neq 0$이면 α를 근으로 가지는 $\mathbb{Q}$ 상에서의 1계수 기약다항식은 다음과 같다.

$$x^2 - 2rx + r^2 - ms^2$$

그러므로 α가 대수적 정수 iff $2r$과 $r^2 - ms^2$가 모두 정수인 것이다. 이것이 위 결과를 함의함을 보이는 것은 연습문제로 남긴다. □

Corollary 2는 $\mathbb{Q}[\sqrt{m}]$에서의 대수적 정수들이 환을 형성함을 보여준다. 동일한 것이 임의의 수체에서 참이다. 이를 증명하기 위해서는 2개 대수적 정수의 합과 곱이 다시 대수적 정수임을 보이면 충분하다. 이를 위해서는 대수적 정수의 다른 특성화를 수립하는 것이 유용할 것이다.

Theorem 2. $\alpha \in \mathbb{C}$에 대하여 다음이 동치이다:

(a) α가 대수적 정수이다.
(b) 환 $\mathbb{Z}[\alpha]$의 덧셈군이 유한생성이다.
(c) α가 덧셈군이 유한생성이도록 하는 $\mathbb{C}$의 어떠한 부분환의 원소이다.
(d) 어떠한 유한생성 덧셈 부분군 $A \subset \mathbb{C}$에 대하여 $\alpha A \subset A$이다.

Proof. (1) ⇒ (2): 만약 α가 $\mathbb{Z}$ 상에서의 1계수 n차다항식의 근이면 덧셈군 $\mathbb{Z}[\alpha]$는 $1, \alpha, \ldots, \alpha^{n-1}$에 의해 생성된다.
(2) ⇒ (3) ⇒ (4)는 자명하다.
(4) ⇒ (1): $a_1, \ldots, a_n$이 A를 생성한다 하자. 각각의 αa_i를 $a_1, \ldots, a_n$의 $\mathbb{Z}$-계수 선형 결합으로 표현하면 $\mathbb{Z}$ 상에서의 어떠한 $n \times n$ 행렬 M에 대하여 다음을 얻는다.

$$\begin{pmatrix} \alpha a_1 \\ \vdots \\ \alpha a_n \end{pmatrix} = M \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

이와 동치로 다음이 0벡터이다. (여기에서 I는 $n \times n$ 항등행렬을 나타낸다.)

$$(\alpha I - M) \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

a_i들이 모두 0이지는 않으므로 $\alpha I - M$이 행렬식 0을 가짐이 따라온다. (다른 말로 하면 α가 M의 고유치임을 보였다.) 이러한 행렬식을 $\alpha I - M$의 n^2개 좌표들로 나타내면 다음을 얻는다.

$$\alpha^n + \text{저차항} = 0$$

그러므로 우리는 α를 근으로 가지는 $\mathbb{Z}$ 상에서의 1계수다항식을 만들었다. □

Corollary. 만약 α, β가 대수적 정수이면 $\alpha + \beta$와 $\alpha\beta$도 그러하다.

Proof. 우리는 $\mathbb{Z}[\alpha]$와 $\mathbb{Z}[\beta]$가 유한생성 덧셈군을 가짐을 알고 있다. 그 경우 환 $\mathbb{Z}[\alpha, \beta]$도 유한생성 덧셈군을 가진다. (만약 $\alpha_1, \ldots, \alpha_m$이 $\mathbb{Z}[\alpha]$를 생성하며 $\beta_1, \ldots, \beta_n$이 $\mathbb{Z}[\beta]$를 생성하면 mn개 곱 $\alpha_i\beta_j$들이 $\mathbb{Z}[\alpha, \beta]$를 생성해야 한다.)
마지막으로 $\mathbb{Z}[\alpha, \beta]$는 $\alpha + \beta$와 $\alpha\beta$를 원소로 가진다. 특성화 (3)에 의해 이는 이들이 대수적 정수임을 함의한다. □

Exercise. 2개의 마음에 드는 대수적 정수를 선택하고 행렬식 과정을 적용하여 이들의 합과 곱에 대한 1계수다항식을 얻어라.

이러한 결과는 $\mathbb{C}$에서의 대수적 정수들의 집합이 환을 형성함을 보여준다. 우리는 이를 기호 $\mathbb{A}$로 표기할 것이다. 특히 임의의 수체 K에 대하여 $\mathbb{A} \cap K$는 K의 부분환이다. $\mathbb{A} \cap K$를 수체 K에 대응하는 **수환(number ring)**이라 부를 것이다. 우리는 $\mathbb{Q}$와 2차수체에 대응하는 수환을 결정했다. 원분체에 대하여 $\mathbb{A} \cap \mathbb{Q}[\omega] = \mathbb{Z}[\omega]$이다; 그러나 현재로서는 ($\omega \in \mathbb{A}$이며 $\mathbb{A} \cap \mathbb{Q}[\omega]$가 환이므로) $\mathbb{A} \cap \mathbb{Q}[\omega]$이 $\mathbb{Z}[\omega]$를 포함한다는 사실만을 명확히 알 수 있다. 등식을 얻기 위해서는 $\mathbb{Q}[\omega]$에 대한 추가적인 정보가 필요하다: 구체적으로 $\mathbb{Q}$ 상에서의 차수와 판별식이 필요하다.

The Cyclotomic Fields (원분체)

$\omega = e^{2\pi i/m}$이라 하자. ω의 모든 **공액(conjugate)**($\mathbb{Q}$ 상에서의 동일한 기약다항식의 근)들도 1의 m승근들이며 어떠한 $n < m$에 대해서도 1의 n승근이 아니다. (이를 보이기 위해서는 ω의 $\mathbb{Q}$ 상에서의 기약다항식이 $x^m - 1$의 인수이지만 $n < m$에 대하여 $\omega^n \neq 1$이므로 $x^n - 1$의 인수가 아님을 기억해 두라.) 이러한 공액들로 가능한 후보는 $\omega^k, 1 \leq k \leq m, (k, m) = 1$들뿐임이 따라온다. 이러한 ω^k들이 실제로 모두 ω의 공액이다. (그러나 이는 자명하지 않다!) 이를 증명하면 $\mathbb{Q}[\omega]$가 $\mathbb{Q}$ 상에서 차수 $\varphi(m)$을 가짐을 보일 수 있으며 Galois 군을 결정할 수 있다; 이에 더해 1의 어떠한 근들이 $\mathbb{Q}[\omega]$에 속하는지를 결정할 수도 있다.

Theorem 3. 모든 $\omega^k, 1 \leq k \leq m, (k, m) = 1$들이 ω의 공액이다.

Proof. k가 위와 같은 경우 각각의 $\theta = \omega^k$와 m의 인수가 아닌 각각의 소수 p에 대하여 θ^p가 θ의 공액임을 보이면 충분하다. 공액 관계가 추이적임은 자명하므로 이러한 결과를 θ와 θ^p에 반복적으로 적용하여 요구된 결과를 얻을 수 있다: 예를 들어 $m = 35, k = 12$인 경우 (공액 관계를 $\sim$으로 나타내면) 다음이 성립한다.

$$\omega \sim \omega^2 \sim \omega^4 \sim \omega^{12}$$

그러므로 $\theta = \omega^k$이며 p가 m의 인수가 아닌 소수라 하자. f가 θ에 대한 $\mathbb{Q}$ 상에서의 1계수 기약다항식이라 하자. 그 경우 어떠한 1계수다항식 $g \in \mathbb{Q}[x]$에 대하여 $x^m - 1 = f(x)g(x)$이다. Theorem 1에 대한 Lemma는 $f, g \in \mathbb{Z}[x]$라는 사실을 보여준다. 명백히 θ^p는 $x^m - 1$의 근이므로 θ^p가 f 또는 g의 근이다; θ^p가 f의 근임을 보여야 한다. 그렇지 않다 가정하면 $g(\theta^p) = 0$이다. 그 경우 θ는 다항식 $g(x^p)$의 근이다. $g(x^p)$가 $\mathbb{Q}[x]$ 내에서 $f(x)$를 인수로 가짐이 따라온다. 다시 Lemma를 적용하면 $g(x^p)$가 $\mathbb{Z}[x]$ 내에서 $f(x)$를 인수로 가짐이 따라온다. 이제 계수들을 $\bmod p$로 축약할 수 있다: 상선이 다항식의 환 준동형사상 $\mathbb{Z}[x] \to \mathbb{Z}_p[x]$ 하에서의 상을 나타낸다 하자. $\bar{g}(x^p)$가 $\mathbb{Z}_p[x]$에서 $\bar{f}[x]$를 인수로 가진다는 사실을 얻는다. 그러나 $\bar{g}(x^p) = (\bar{g}(x))^p$이며 (exercise 5를 참조하라) $\mathbb{Z}_p[x]$가 유일 인수분해 정역이므로 (Appendix A를 참조하라) $\bar{f}$와 $\bar{g}$가 $\mathbb{Z}_p[x]$에서 공통인수 h를 가짐이 따라온다. 그 경우 $h^2 | \overline{fg} = x^m - 1$이다. 이는 h가 $x^m - 1$의 도함수 (exercise 6을 참조하라) $\bar{m}x^{m-1}$의 인수임을 함의한다. (여기에서 상선은 $\bmod p$로 축약된 m을 의미한다.) $p \nmid m$이므로 $\bar{m} \neq 0$이다; 그 경우 $h(x)$는 단항식이다. (다시 $\mathbb{Z}_p[x]$의 유일 인수분해를 사용했다.) 그러나 $h | x^m - 1$이므로 이는 불가능하다. 이는 증명을 완료한다. □

Corollary 1. $\mathbb{Q}[\omega]$는 $\mathbb{Q}$ 상에서 차수 $\varphi(m)$을 가진다.

Proof. ω가 공액들을 $\varphi(m)$개 가지며 따라서 ω의 $\mathbb{Q}$ 상에서의 기약다항식은 차수 $\varphi(m)$을 가진다. □

Corollary 2. $\mathbb{Q}[\omega]$의 $\mathbb{Q}$ 상에서의 Galois 군은 다음의 $\bmod m$ 정수 곱셈군과 동형이다.

$$\mathbb{Z}_m^* = \{k : 1 \le k \le m, (k, m) = 1\}$$

각각의 $k \in \mathbb{Z}_m^*$에 대하여 Galois 군에서 대응하는 자기동형사상은 ω를 ω^k로 대응시킨다. (따라서 모든 $g \in \mathbb{Z}[x]$에 대하여 $g(\omega)$를 $g(\omega^k)$로 대응시킨다.)

Proof. $\mathbb{Q}[\omega]$의 자기동형사상은 ω의 상에 의해 유일하게 결정되며 Theorem 3은 ω가 임의의 $\omega^k, (k, m) = 1$로 대응될 수 있다 말해준다. (명백히 이는 다른 곳으로 대응될 수 없다.) 이는 Galois 군과 $\bmod m$ 곱셈군 간의 1-1 대응을 수립한다. 자기동형사상의 합성이 $\bmod m$ 곱셈에 대응되는지를 확인하는 것만이 남아있으며, 이를 연습문제로 남기겠다. □

Corollary 2의 응용으로 $\mathbb{Z}_m^*$의 부분군들에 대응하는 $\mathbb{Q}[\omega]$의 부분체들을 찾을 수 있다. 특히 p가 소수인 경우 p번째 원분체는 ($\mathbb{Z}_p^*$가 위수 $p-1$의 순환군이므로) $p-1$의 각각의 인수 차수마다 유일한 부분체를 가진다. 그러므로 각각의 홀수 소수 p에 대하여 p번째 원분체는 유일한 2차수체를 포함한다. 이는 p에 의존하는 부호를 가지는 $\mathbb{Q}(\sqrt{\mp p})$로 밝혀진다. (exercise 8을 참조하라.) 우리는 chapter 4에서 2차상호법칙을 증명하기 위해 이 사실을 사용할 것이다.

Corollary 3. $\omega = e^{2\pi i/m}$이라 하자. 만약 m이 짝수이면 $\mathbb{Q}[\omega]$에 속한 1의 근은 1의 m승근들뿐이다. 만약 m이 홀수이면 1의 $2m$승근들뿐이다.

Proof. 홀수 m에 대하여 m번째 원분체가 $2m$번째 원분체와 동일함을 알고 있으므로 짝수 m에 대하여 진술을 증명하면 충분하다. 그러므로 m이 짝수이며 θ가 $\mathbb{Q}[\omega]$에 속한 1의 **원시(primitive)** k승근이라 하자. (i.e. 1의 k승근이며 $n < k$에 대하여 1의 n승근이 아니다.) 그 경우 r이 k와 m의 최소공배수라 하면 $\mathbb{Q}[\omega]$는 1의 원시 r승근을 포함한다. (exercise 9를 참조하라.) 그러나 그 경우 $\mathbb{Q}[\omega]$는 r번째 원분체를 포함하며 이는 $\phi(r) \le \phi(m)$을 함의한다. 이는 $r = m$이 아닌 한 모순이다. (exercise 10을 참조하라.) 그러므로 $k|m$이며 θ가 1의 m승근이다. □

Corollary 3은 다음을 함의한다:

Corollary 4. 짝수 m에 대한 m번째 원분체들은 모두 서로 다르며 이들 중 어떠한 2개도 동형이 아니다.

우리는 이제 임의의 수체에 관한 이론으로 넘어가겠다. 궁극적으로 우리는 원분체로 돌아와 $\mathbb{A} \cap \mathbb{Q}[\omega] = \mathbb{Z}[\omega]$임을 보일 것이다.

Embeddings in $\mathbb{C}$ ($\mathbb{C}$로의 매장)

K가 $\mathbb{Q}$ 상에서의 n차수체라 하자. 우리는 K에서 $\mathbb{C}$로의 매장이 정확히 n개 존재함을 알고 있다. (Appendix B를 참조하라.) 이들은 어떠한 α에 대하여 $K = \mathbb{Q}[\alpha]$로 표현하고 α가 $\mathbb{Q}$ 상에서의 n개 공액들 중 임의의 것으로 대응될 수 있음을 관찰하면 간단히 기술할 수 있다. 각각의 공액 β는 K의 $\mathbb{C}$로의 유일한 매장 ($g(\alpha) \mapsto g(\beta)\ \forall g \in \mathbb{Q}[x]$)를 결정하며 α가 공액들 중 하나로 대응되어야 하므로 모든 매장은 이러한 방식으로 등장해야만 한다.

Example. 제곱 없는 정수 m에 대한 2차수체 $\mathbb{Q}[\sqrt{m}]$은 $\mathbb{C}$로의 매장을 2개 가진다: ($\sqrt{m}$과 $-\sqrt{m}$이 $\sqrt{m}$의 2개 공액들이므로) 항등함수 및 $a + b\sqrt{m} \mapsto a - b\sqrt{m}$ $(a, b \in \mathbb{Q})$. m번째 원분체는 $\mathbb{C}$로의 $\varphi(m)$개 매장, 즉 $\varphi(m)$개 자기동형사상들을 가진다. 반면에 체 $\mathbb{Q}[\sqrt[3]{2}]$는 $\mathbb{C}$로의 매장을 3개 가지며 하나만 (항등함수) 자기동형사상에 대응하고 다른 두 매장은 ($\omega = e^{2\pi i/3}$이라 하면) $\sqrt[3]{2}$의 공액 $\omega\sqrt[3]{2}$ 및 $\omega^2\sqrt[3]{2}$에 대응한다. 이들은 실수가 아니므로 명백히 $\mathbb{Q}[\sqrt[3]{2}]$에 속하지 않는다.

더 일반적으로, 만약 K, L이 수체이며 $K \subset L$이면 K의 $\mathbb{C}$로의 임의의 매장이 L의 $\mathbb{C}$로의 정확히 $[L : K]$개 매장으로 확장됨을 알고 있다. (Appendix B) 특히 L은 K의 각 점을 고정하는 $\mathbb{C}$로의 매장을 $[L : K]$개 가진다.

$\mathbb{C}$로의 매장 대신 체의 자기동형사상을 가지고 작업하는 것이 선호될 때가 있다. (특히 이들을 서로 합성하고자 하는 경우에 그렇다.) 수체 K의 매장을 자기동형사상으로 대체하는 유용한 방법은 K를 $\mathbb{Q}$의 정규확대 L로 확대하는 것이다. (이는 항상 가능하다; Appendix B를 참조하라.) K의 각각의 매장은 L의 $[L : K]$개 매장들로 확장되며, L이 정규이므로 이들은 모두 L의 자기동형사상들이다. 예를 들어 체 $K = \mathbb{Q}[\sqrt[3]{2}]$는 $\mathbb{Q}$ 상에서 정규인 $L = \mathbb{Q}[\sqrt[3]{2}, \omega], \omega = e^{2\pi i/3}$으로 확대될 수 있다. K의 각각의 매장은 L의 2개 자기동형사상들로 확장된다. (Exercise: L의 6개 자기동형사상들을 $\sqrt[3]{2}$와 ω를 무엇으로 대응시키는지에 따라 기술하라.)

The Trace and the Norm (자취와 노름)

K가 수체라 하자. K에서의 함수 T와 N을 다음과 같이 정의할 것이다: $\sigma_1, \dots, \sigma_n$이 K의 $\mathbb{C}$로의 매장을 나타내며 $n = [K : \mathbb{Q}]$라 하자. 각각의 $\alpha \in K$에 대하여 다음과 같이 정의한다.

$$\mathrm{T}(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) + \cdots + \sigma_n(\alpha)$$
$$\mathrm{N}(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha)\cdots\sigma_n(\alpha)$$

명백히 $\mathrm{T}(\alpha)$와 $\mathrm{N}(\alpha)$는 α뿐만 아니라 체 K에도 의존한다. 하나 초과의 체를 다룰 경우 혼동을 피하기 위해 $\mathrm{T}^K(\alpha)$과 $\mathrm{N}^K(\alpha)$로 표기하겠다.

정의로부터 즉시 모든 $\alpha, \beta \in K$에 대하여 $\mathrm{T}(\alpha+\beta) = \mathrm{T}(\alpha) + \mathrm{T}(\beta)$이며 $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)$임을 알 수 있다. 이에 더해 $r \in \mathbb{Q}$에 대하여 $\mathrm{T}(r) = nr, \mathrm{N}(r) = r^n$이다. 또한 $r \in \mathbb{Q}$와 $\alpha \in K$에 대하여 $\mathrm{T}(r\alpha) = r\,\mathrm{T}(\alpha)$이며 $\mathrm{N}(r\alpha) = r^n\,\mathrm{N}(\alpha)$이다.

우리는 자취 및 노름에 대한 다른 공식을 수립하고 이들의 값이 항상 유리수임을 보일 것이다: α가 $\mathbb{Q}$ 상에서 차수 d를 가진다 하자. (i.e. α에 대한 $\mathbb{Q}$ 상에서의 기약다항식이 d차이다; 이와 동치로 α의 $\mathbb{Q}$ 상에서의 공액이 d개이다; 이와 동치로 $\mathbb{Q}[\alpha]$가 $\mathbb{Q}$ 상에서 d차이다.) $t(\alpha)$와 $n(\alpha)$가 각각 α의 $\mathbb{Q}$ 상에서의 d개 공액들의 합과 곱이라 하자. 그 경우 다음이 성립한다:

Theorem 4.

$$\mathrm{T}(\alpha) = \frac{n}{d}t(\alpha)$$
$$\mathrm{N}(\alpha) = (n(\alpha))^{n/d}$$

여기에서 $n = [K : \mathbb{Q}]$이다. ($\frac{n}{d}$가 정수임을 기억해 두라: 사실 이는 차수 $[K : \mathbb{Q}[\alpha]]$이다.)

Proof. $t(\alpha)$와 $n(\alpha)$는 α의 자취와 노름 $\mathrm{T}^{\mathbb{Q}[\alpha]}$ 및 $\mathrm{N}^{\mathbb{Q}[\alpha]}$이다. $\mathbb{Q}[\alpha]$의 $\mathbb{C}$로의 각각의 매장은 정확히 $\frac{n}{d}$개의 K의 $\mathbb{C}$로의 매장으로 확장된다. 이는 위 공식들을 수립한다. □

Corollary 1. $\mathrm{T}(\alpha)$와 $\mathrm{N}(\alpha)$가 유리수이다.

Proof. $t(\alpha)$와 $n(\alpha)$가 유리수임을 보이면 충분하다. α에 대한 $\mathbb{Q}$ 상에서의 1계수 기약다항식의 둘째 계수가 $-t(\alpha)$이고 상수항 계수가 $\pm n(\alpha)$이므로 이는 자명하다. □

만약 α가 대수적 정수이면 α의 $\mathbb{Q}$ 상에서의 1계수 기약다항식이 $\mathbb{Z}$-계수이며 따라서 다음이 성립한다.

Corollary 2. 만약 α가 대수적 정수이면 $\mathrm{T}(\alpha)$와 $\mathrm{N}(\alpha)$가 정수이다.

Example. 2차수체 $K = \mathbb{Q}[\sqrt{m}]$에서 $a, b \in \mathbb{Q}$에 대하여 다음이 성립한다.

$$\mathrm{T}(a + b\sqrt{m}) = 2a$$
$$\mathrm{N}(a + b\sqrt{m}) = a^2 - mb^2$$

이 경우 α가 대수적 정수 iff 노름과 자취가 모두 정수인 것이다. (물론 이는 일반적으로는 참이 아니다: 예를 들어 $x^3 + \frac{1}{2}x + 1$의 임의의 근을 고려하라.)

Some Applications (응용)

K에서의 대수적 정수들의 환 $\mathbb{A} \cap K$에서의 가역원들을 결정하고자 한다고 하자. 위의 Corollary 2와 노름이 곱셈적이라는 사실을 이용하면 모든 가역원이 노름 ± 1을 가짐을 간단히 보일 수 있다. 그 후 Theorem 4는 (α의 공액들이 대수적 정수이므로) $\frac{1}{\alpha}$도 대수적 정수임을 보여준다. 이는 $\mathbb{A} \cap K$의 가역원들이 노름 ± 1을 가지는 원소들임을 보여준다. 그러므로 예를 들어 $\mathbb{Z}[\sqrt{-2}]$에 속한 가역원들은 ± 1뿐이다. 유사한 결과가 2개를 제외한 모든 허 2차수체에 대하여 성립한다. (exercise 13)을 참조하라. 반면에 $\mathbb{Z}[\sqrt{2}]$의 가역원들은 방정식 $a^2 - 2b^2 = \pm 1$의 정수해들에 대응한다; 이들은 무한히 많다. (exercise 14를 참조하라.)

노름은 어떠한 원소들이 $\mathbb{A} \cap K$에서 (chapter 1에서 정의된 것과 같이) 기약임을 보이기 위해 사용될 수도 있다. 명백히 $\alpha \in \mathbb{A} \cap K$의 노름이 $\mathbb{Z}$에서의 소수이면 α가 기약이다. (그러나 역이 성립할 필요는 없다.) 그러므로 예를 들어 $9 + \sqrt{10}$은 $\mathbb{Z}[\sqrt{10}]$에서 기약이다.

자취의 응용으로, 우리는 특정 체가 특정 원소를 포함하지 못함을 보일 수 있다. 예를 들어 $\sqrt{3} \notin \mathbb{Q}[\sqrt[4]{2}]$이다. (exercise 16을 참조하라.) 자취는 또한 다음 절에서 정의할 판별식과 밀접한 관련이 있ㅌ다. 그러나 먼저 우리는 $\mathbb{Q}$를 임의의 수체로 대체하는 것으로 자취와 노름을 일반화할 것이다:

K와 L이 수체이며 $K \subseteq L$이라 하자. K를 점별 고정하는 L의 $\mathbb{C}$로의 $n = [L : K]$개 매장들을 $\sigma_1, \dots, \sigma_n$으로 표기하자. 각각의 $\alpha \in L$에 대하여 **상대자취(relative trace)**와 **상대노름(relative norm)**을 다음과 같이 정의한다.

$$\mathrm{T}_K^L(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) + \cdots + \sigma_n(\alpha)$$
$$\mathrm{N}_K^L(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha)\cdots\sigma_n(\alpha)$$

그러므로 이러한 표기법 하에서 $\mathrm{T}^K = \mathrm{T}_{\mathbb{Q}}^K$이며 $\mathrm{N}^K = \mathrm{N}_{\mathbb{Q}}^K$이다. 다시 모든 $\alpha, \beta \in L$에 대하여 $\mathrm{T}_K^L(\alpha+\beta) = \mathrm{T}_K^L(\alpha) + \mathrm{T}_K^L(\beta)$이며 $\mathrm{N}_K^L(\alpha\beta) - \mathrm{N}_K^L(\alpha)\,\mathrm{N}_K^L(\beta)$이다; 모든 $\delta \in K$에 대하여 $\mathrm{T}_K^L(\delta) = n\delta$이며 $\mathrm{N}_K^L(\delta) = \delta^n$이다; $\delta \in K$와 $\alpha \in L$에 대하여 $\mathrm{T}_K^L(\delta\alpha) = \delta\,\mathrm{T}_K^L(\alpha)$이며 $\mathrm{N}_K^L(\delta\alpha) = \delta^n\,\mathrm{N}_K^L(\alpha)$이다. 이전과 같이 다음을 보일 수 있다.

Theorem 4′. $\alpha \in L$이며 d가 α의 K 상에서의 차수라 하자. $t(\alpha)$와 $n(\alpha)$가 α의 K 상에서의 d개 공액들의 합과 곱이라 하자. 그 경우 다음이 성립한다.

$$\mathrm{T}_K^L(\alpha) = \frac{n}{d}t(\alpha)$$
$$\mathrm{N}_K^L(\alpha) = (n(\alpha))^{n/d}$$

□

Corollary. $\mathrm{T}_K^L(\alpha)$와 $\mathrm{N}_K^L(\alpha)$가 K에 속한다. 만약 $\alpha \in \mathbb{A} \cap L$이면 이들은 $\mathbb{A} \cap K$에 속한다. □

3개 서로 다른 체가 존재하는 경우 상대자취와 상대노름은 다음과 같이 연관된다:

Theorem 5. K, L, M이 수체이며 $K \subset L \subset M$이라 하자. 그 경우 모든 $\alpha \in M$에 대하여 다음이 성립한다.

$$\mathrm{T}_K^L(\mathrm{T}_L^M(\alpha)) = \mathrm{T}_K^M(\alpha)$$
$$\mathrm{N}_K^L(\mathrm{N}_L^M(\alpha)) = \mathrm{N}_K^M(\alpha)$$

(이는 **추이성(transitivity)**이라 불린다.)

Proof. $\sigma_1, \dots, \sigma_n$이 K를 점별 고정하는 L의 $\mathbb{C}$로의 매장이며 $\tau_1, \dots, \tau_m$이 L을 점별 고정하는 M의 $\mathbb{C}$로의 매장이라 하자. 우리는 σ_i와 τ_j를 합성하고 싶지만 아직은 할 수 없다; 먼저 이러한 매장들을 모두 어떠한 체의 자기동형사상으로 확장해야 한다. 그러므로 $M \subset N$인 $\mathbb{Q}$의 정규 확대 N을 고정하자. 그 경우 모든 σ_i와 τ_j는 N의 자기동형사상으로 확장될 수 있다; 이들의 한 가지 확장을 고정하고 이러한 확장들을 다시 σ_i, τ_j라 부르자. (이는 혼동을 유발하지 않는다.) 이제 함수들을 합성할 수 있으며 다음을 얻는다.

$$\mathrm{T}_K^L(\mathrm{T}_L^M(\alpha)) = \sum_{i=1}^{n} \sigma_i \left(\sum_{j=1}^{m} \tau_j(\alpha) \right) = \sum_{i,j} \sigma_i\tau_j(\alpha)$$
$$\mathrm{N}_K^L(\mathrm{N}_L^M(\alpha)) = \prod_{i=1}^{n} \sigma_i \left(\prod_{j=1}^{m} \tau_j(\alpha) \right) = \prod_{i,j} \sigma_i\tau_j(\alpha)$$

mn개 함수 $\sigma_i\tau_j$들의 M으로의 제한이 K를 점별 고정하는 M의 $\mathbb{C}$로의 매장을 제공함을 보이는 것만이 남아있다. 모든 $\sigma_i\tau_j$들이 K를 점별 고정하며 이들이 올바른 개수만큼 존재하므로 ($mn = [M : L][L : K] = [M : K]$) 이들의 M으로의 제한이 모두 서로 다름을 보이면 충분하다. 이를 독자에게 연습문제로 남기겠다. (exercise 18) □

The Discriminant of an n-tuple (순서 n조의 판별식)

K가 $\mathbb{Q}$ 상에서의 n차수체라 하자. $\sigma_1, \dots, \sigma_n$이 n개 매장 $K \subset \mathbb{C}$를 나타낸다 하자. K의 원소들의 임의의 순서 n조 $\alpha_1, \dots, \alpha_n \in K$에 대하여 $\alpha_1, \dots, \alpha_n$의 **판별식(discriminant)**을 다음과 같이 정의하자.

$$\mathrm{disc}(\alpha_1, \dots, \alpha_n) = |\sigma_i(\alpha_j)|^2$$

i.e. i행 j열 성분이 $\sigma_i(\alpha_j)$인 행렬의 행렬식의 제곱이다. (표기법: i행 j열 성분이 a_{ij}인 행렬을 $[a_{ij}]$로 나타내며 그 행렬식을 $|a_{ij}|$로 나타낸다.) 제곱으로 인해 행렬식이 σ_i 및 α_j들의 순서에 독립적이게 됨을 기억해 두라.

노름과 자취에서와 마찬가지로 $\mathbb{Q}$를 임의의 수체로 대체하는 것으로 판별식의 개념을 일반화할 수 있다. (exercise 23을 참조하라.)

판별식을 자취 $\mathrm{T} = \mathrm{T}^K$를 통해 나타낼 수 있다:

Theorem 6. $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = |\,\mathrm{T}(\alpha_i\alpha_j)|$

Proof. 이는 다음의 행렬방정식

$$[\sigma_j(\alpha_i)][\sigma_i(\alpha_j)] = [\sigma_1(\alpha_i\alpha_j) + \cdots + \sigma_n(\alpha_i\alpha_j)] = [\mathrm{T}(\alpha_i\alpha_j)]$$

및 다음과 같은 행렬식의 친숙한 성질에서 즉시 따라온다.

$$|a_{ij}| = |a_{ji}| \quad , \quad \text{행렬 } A, B\text{에 대하여 } |AB| = |A||B|$$

□

Corollary. $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) \in \mathbb{Q}$이다; 만약 모든 α_i들이 대수적 정수이면 $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}$이다.

특히 판별식은 α_j들이 선형 종속인지를 결정한다:

Theorem 7. $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = 0$ iff $\alpha_1, \ldots, \alpha_n$이 $\mathbb{Q}$ 상에서 선형 종속인 것이다.

Proof. α_j들이 $\mathbb{Q}$ 상에서 선형 종속이면 행렬 $[\sigma_i(\alpha_j)]$의 열들도 선형 종속이다; 따라서 행렬식이 0이다. 역으로 $\mathrm{disc}(\alpha_1, \ldots, \alpha_n) = 0$이면 행렬 $[\mathrm{T}(\alpha_i\alpha_j)]$의 행 R_i들이 선형 종속이다. $\alpha_1, \ldots, \alpha_n$이 $\mathbb{Q}$ 상에서 선형 독립이라 가정하자. $a_1R_1 + \cdots + a_nR_n$이 0벡터이도록 하는 (모두 0이지는 않은) 유리수 $a_1, \ldots, a_n$들을 고정하자. $\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n$을 고려하자. $\alpha \neq 0$이어야 한다. 이에 더해 각 행의 j번째 좌표만 고려하면 각각의 j에 대하여 $\mathrm{T}(\alpha\alpha_j) = 0$이라는 사실을 얻는다. α_j들이 $\mathbb{Q}$ 상에서 선형 독립이라 가정했으므로 이들은 $\mathbb{Q}$ 상에서의 K의 기저를 형성한다; ($\alpha \neq 0$이므로) $\alpha\alpha_j$들도 기저를 형성함이 따라온다. 그러나 그 경우 모든 $\beta \in K$에 대하여 $\mathrm{T}(\beta) = 0$이다. (왜 그런가?) 예를 들어 $\mathrm{T}(1) = n$이므로 이는 명백히 모순이다. □

Theorem 7은 K의 $\mathbb{Q}$ 상에서의 모든 기저가 0이 아닌 판별식을 가짐을 보여준다. 하나의 원소의 멱들로 구성된 기저의 경우 판별식에 대한 상대적으로 간단한 공식을 얻는다:

Theorem 8. $K = \mathbb{Q}[\alpha]$이며 $\alpha_1, \ldots, \alpha_n$이 α의 $\mathbb{Q}$ 상에서의 공액들을 나타낸다 하자. 그 경우 다음이 성립한다.

$$\mathrm{disc}(1, \alpha, \ldots, \alpha^{n-1}) = \prod_{1 \leq r < s \leq n} (\alpha_r - \alpha_s)^2 = \pm\,\mathrm{N}^K(f'(\alpha))$$

여기에서 f는 α의 $\mathbb{Q}$ 상에서의 1계수 기약다항식이다; $+$ 부호가 성립할 필요충분조건은 $n \equiv 0$ 또는 $1 \pmod 4$인 것이다.

Proof. 첫째 부등식은 (σ_i들이 적절한 순서를 가진 경우) 다음 식

$$|\sigma_i(\alpha^{j-1})| = |(\sigma_i(\alpha))^{j-1}| = |\alpha_i^{j-1}|$$

이 Vandermonde 행렬식이라는 사실에서 즉시 따라온다: 일반적으로 임의의 가환환 상에서 다음의 잘 알려진 식이 성립한다. (exercise 19를 참조하라.)

$$|a_i^{j-1}| = \prod_{1 \leq r < s \leq n} (a_s - a_r)$$

두 번째 등식에 대해서는 먼저 다음이 성립한다.

$$\prod_{r<s} (\alpha_r - \alpha_s)^2 = \pm \prod_{r \neq s} (\alpha_r - \alpha_s)$$

여기에서 우변의 합은 2개의 서로 다른 성분을 가지는 $n(n-1)$개 순서쌍 전체에 대하여 취한다. $+$ 부호가 등장할 필요충분조건이 $n \equiv 0$ 또는 $1 \pmod 4$임을 검증하는 것은 독자에게 남기겠다. 그러므로 이러한 마지막 합이 $\mathrm{N}^K(f'(\alpha))$와 동일함을 보이는 것이 남아있다. f'이 $\mathbb{Q}$-계수라는 사실을 이용하면 다음이 성립한다.

$$\mathrm{N}^K(f'(\alpha)) = \prod_{r=1}^{n} \sigma_r(f'(\alpha)) = \prod_{r=1}^{n} f'(\sigma_r(\alpha)) = \prod_{r=1}^{n} f'(\alpha_r)$$

마지막으로 각각의 r에 대하여 다음이 성립함을 보이는 것을 연습문제로 남기겠다.

$$f'(\alpha_r) = \prod_{s \neq r} (\alpha_r - \alpha_s)$$

곱은 $n-1$개 지표 $s, s \neq r$에 대하여 취한다. (exercise 20을 참조하라.) □

이것의 응용으로 p가 홀수 소수인 경우 $\omega^{2\pi i/p}$에 대한 $\mathrm{disc}(1, \omega, \ldots, \omega^{p-2})$를 계산하겠다. 우리는 $f(x) = 1 + x + x^2 + \cdots + x^{p-1}$임을 알고 있다. $f'(\omega)$를 계산하는 가장 간단한 방법은 $x^p - 1 = (x-1)f(x)$로 표현하고 미분하여 $px^{p-1} = f(x) + (x-1)f'(x)$를 얻는 것이다. 이는 $f'(\omega) = \frac{p}{\omega(\omega-1)}$을 제공한다. 노름을 취하면 다음을 얻는다.

$$\mathrm{N}(f'(\omega)) = \frac{\mathrm{N}(p)}{\mathrm{N}(\omega)\,\mathrm{N}(\omega - 1)}$$

$\mathrm{N}(p) = p^{p-1}$이며 $\mathrm{N}(\omega) = 1$임을 간단히 보일 수 있다; 이에 더해 chapter 1의 exercise 16은 $\mathrm{N}(1-\omega) = p$임을 보여준다. 이는 $\mathrm{N}(\omega - 1)$과 같다. (왜인가?) 그러므로 우리는 $\mathrm{N}(f'(\omega)) = p^{p-2}$를 얻는다.

우리는 $\mathbb{Q}$ 상에서의 임의의 대수적 수 α에 대하여 α의 차수가 n인 경우 $\mathrm{disc}(1, \alpha, \ldots, \alpha^{n-1})$을 $\mathrm{disc}(\alpha)$로 표기할 것이다. 체 K는 $\mathbb{Q}[\alpha]$인 것으로 간주한다. 그러므로 우리는 p 소수, $\omega = e^{2\pi i/p}$에 대하여 $\mathrm{disc}(\omega) = \pm p^{p-2}$임을 보였다. 더 일반적으로 만약 $\omega = e^{2\pi i/n}$이면 $\mathrm{disc}(\omega)$에 대한 복잡한 표현이 존재한다. (exercise 23(c)를 참조하라.) 그러나 우리는 매우 간단히 $\mathrm{disc}(\omega)$이 $m^{\varphi(m)}$의 인수임을 보일 수 있으며 이는 우리의 목적을 위해서는 충분하다: f가 ω의 $\mathbb{Q}$ 상에서의 1계수 기약다항식이라 하면 어떠한 $g \in \mathbb{Z}[x]$에 대하여 $x^m - 1 = f(x)g(x)$임을 알고 있다. 미분하고 x에 ω를 대입하면 $m = \omega f'(\omega)g(\omega)$를 얻는다. 노름을 취하면 다음을 얻는다.

$$m^{\varphi(m)} = \pm\,\mathrm{disc}(\omega)\,\mathrm{N}(\omega g(\omega))$$

$\mathrm{N}(\omega g(\omega)) \in \mathbb{Z}$이므로 (왜 그런가?) 이는 요구된 식을 수립한다.

The Additive Structure of a Number Ring (수환의 덧셈적 구조)

K가 $\mathbb{Q}$ 상에서의 n차수체이며 R이 K에서의 대수적 수환 $\mathbb{A} \cap K$라 하자. 우리는 판별식을 이용하여 R의 덧셈적 구조를 결정할 것이다. 구체적으로는 R이 계수 n의 자유가환군임을 보일 것이다.

유한 **계수(rank)** n의 **자유가환군(free abelian group)**은 $\mathbb{Z}$와 동형인 n개 부분군들의 직접합이다; 이와 동치로 이는 n-공간의 격자점들의 덧셈군 $\mathbb{Z}^n$과 동형이다. 서로 다른 n에 대한 $\mathbb{Z}^n$들이 동형이 아니므로 이러한 군의 계수는 잘 정의된다. (이를 보이는 가장 간단한 방법은 $\mathbb{Z}^n/2\mathbb{Z}^n$이 2^n개 원소를 가짐을 관찰하는 것이다.)

자유가환군에 대하여 알아야 하는 유일한 사실은 계수 n의 자유가환군의 모든 부분군이 다시 계수 n 이하의 자유가환군이라는 것이다. (증명을 위해서는 exercise 24를 참조하라.) 이로부터 어떠한 군이 동일한 계수의 2개 자유가환군에 의해 조여지면 이 군도 해당 계수의 자유가환군이어야 함이 즉시 따라온다: 만약 $A \subset B \subset C$이며 A, C가 모두 계수 n의 자유가환군이면 B도 그러하다. 우리는 이것을 이용하여 R에 대한 결과를 수립할 것이다.

우리는 먼저 대수적 정수들로만 구성된 K의 $\mathbb{Q}$ 상에서의 기저가 존재함을 주장하겠다; 사실 임의의 기저가 주어진 경우 모든 구성원에 고정된 정수를 곱하는 것으로 이러한 기저를 얻을 수 있다. 이는 각각의 $\alpha \in K$에 대하여 정수 $m \in \mathbb{Z}$가 존재하여 $m\alpha$가 대수적 정수이도록 한다는 사실에서 즉시 따라온다. (exercise 25를 참조하라.)

이러한 K의 $\mathbb{Q}$ 상에서의 기저 $\{\alpha_1, \ldots, \alpha_n\} \subset R$을 고정하면 R에 포함된 계수 n의 자유가환군인 α_i들에 의해 생성된 덧셈군을 얻는다.

$$A = \{m_1\alpha_1 + \cdots + m_n\alpha_n : m_i \in \mathbb{Z}\ \forall i\}$$

이는 다음과 같은 직접합으로 표현 가능하다.

$$\mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$$

각각의 합인자가 $\mathbb{Z}$와 동형이므로 이는 명백히 계수 n의 자유가환군이다.

$A \subset R$이 성립한다. 조임의 다른 쪽 방향에 대해서는 어떠한가? 이곳이 바로 판별식이 사용되는 곳이다:

Theorem 9. $\{\alpha_1, \ldots, \alpha_n\}$이 대수적 정수들로 구성된 K의 $\mathbb{Q}$ 상에서의 기저이며 $d = \mathrm{disc}(\alpha_1, \ldots, \alpha_n)$이라 하자. 그 경우 모든 $\alpha \in R$은 각각의 j에 대하여 $d | m_j^2$를 만족시키는 어떠한 $m_j \in \mathbb{Z}$들에 의해 다음 형태로 표현될 수 있다.

$$\frac{m_1\alpha_1 + \cdots + m_n\alpha_n}{d}$$

(Note: α_i들이 기저를 형성하므로 $d \neq 0$이며 α_i들이 대수적 정수이므로 $d \in \mathbb{Z}$임을 알고 있다.)

Proof. $x_j \in \mathbb{Q}$들에 대하여 $\alpha = x_1\alpha_1 + \cdots + x_n\alpha_n$으로 표현하자. $\sigma_1, \ldots, \sigma_n$이 K의 $\mathbb{C}$로의 매장을 나타낸다 하고 위 방정식에 각각의 σ_i들을 적용하면 다음의 연립방정식을 얻는다.

$$\sigma_i(\alpha) = x_i\sigma_i(\alpha_1) + \cdots + x_n\sigma_i(\alpha_n) \qquad (i = 1, \ldots, n)$$

Cramer 규칙을 이용하여 x_j들에 대하여 해결하면 판별식 $\delta = |\sigma_i(\alpha_j)|$와 j열을 $\sigma_i(\alpha)$로 대체하여 얻은 행렬식 y_j들에 대하여 $x_j = y_j/\delta$임을 알 수 있다. 명백히 y_j들과 δ는 대수적 정수이며, $\delta^2 = d$이다. 그러므로 $dx_j = \delta y_j$이고 이는 유리수 dx_j가 대수적 정수임을 보여준다. 우리가 보인 것과 같이 이는 $dx_j \in \mathbb{Z}$를 함의한다. 이를 m_j라 부르자.
$m_j^2/d \in \mathbb{Z}$임을 보이는 것이 남아있다. 이는 유리수이므로 이것이 대수적 정수임을 보이면 충분하다. 사실 $m_j^2/d = y_j^2$임을 확인하는 것을 독자에게 남기겠다. □

Theorem 9는 R이 다음의 자유가환군에 포함됨을 보여준다.

$$\frac{1}{d}A = \mathbb{Z}\frac{\alpha_1}{d} \oplus \cdots \oplus \mathbb{Z}\frac{\alpha_n}{d}$$

그러므로 R은 계수 n의 자유가환군을 포함하며 계수 n의 자유가환군에 포함된다. 앞에서 관찰한 것과 같이 이는 다음을 함의한다.

Corollary. R은 계수 n의 자유가환군이다.

이와 동치로, R이 $\mathbb{Z}$ 상에서 기저를 가진다: $\beta_1, \ldots, \beta_n \in R$이 존재하여 모든 $\alpha \in R$이 다음 형태로 유일하게 표현된다.

$$m_1\beta_1 + \cdots + m_n\beta_n \qquad (m_i \in \mathbb{Z})$$

$\{\beta_1, \ldots, \beta_n\}$은 R에 대한 **정수적 기저(integral basis)** 또는 R에 대한 $\mathbb{Z}$ 상에서의 기저라 불린다. 명백히 $\{\beta_1, \ldots, \beta_n\}$은 K의 $\mathbb{Q}$ 상에서의 기저도 된다.

Example. 제곱 없는 정수 m에 대한 2차수체 $\mathbb{Q}[\sqrt{m}]$에서 $R = \mathbb{A} \cap \mathbb{Q}[\sqrt{m}]$에 대한 정수적 기저는 $m \equiv 2$ 또는 $3 \pmod 4$인 경우 $1, \sqrt{m}$으로, $m \equiv 1 \pmod 4$인 경우 $1, (1+\sqrt{m})/2$로 구성된다. (Theorem 1의 Corollary 2에 주어진 R의 기술을 사용하여 이를 검증하라.)

앞에서 말한 것과 같이 m번째 원분체에서의 대수적 정수환은 단지 $\mathbb{Z}[\omega]$이며 따라서 정수적 기저는 $1, \omega, \ldots, \omega^{\varphi(m)-1}$로 구성된다. 이제 우리는 m이 소수의 멱인 경우에 대하여 이를 증명할 수 있다:

Theorem 10. 소수 p와 $m = p^r$에 대하여 $\omega = e^{2\pi i/m}$이라 하자. 그 경우 $\mathbb{A} \cap \mathbb{Q}[\omega] = \mathbb{Z}[\omega]$이다.

두 가지 보조정리가 필요하다:

Lemma 1. (모든 $m \geq 3$에 대하여 유효함): $\mathbb{Z}[1-\omega] = \mathbb{Z}[\omega]$이며 다음이 성립한다.

$$\operatorname{disc}(1-\omega) = \operatorname{disc}(\omega)$$

Proof. $\omega = 1 - (1-\omega)$이므로 $\mathbb{Z}[1-\omega] = \mathbb{Z}[\omega]$임은 자명하다. 이 사실은 그 자체로 판별식이 동일함을 함의한다. (exercise 26을 참조하라.) 그러나 Theorem 8을 사용하는 것이 더 간단할 수도 있다: α_i들이 ω의 공액들을 범위로 가지는 경우 $1-\alpha_i$들은 $1-\omega$의 공액들을 범위로 가진다. 따라서 다음이 성립한다.

$$\operatorname{disc}\omega = \prod_{1 \leq r < s \leq n} (\alpha_r - \alpha_s)^2 = \prod_{1 \leq r < s \leq n} ((1-\alpha_r) - (1-\alpha_s))^2 = \operatorname{disc}(1-\omega)$$

□

Lemma 2. ($m = p^r$에 대하여) 다음이 성립한다.

$$\prod_k (1 - \omega^k) = p$$

여기에서 곱은 $1 \leq k \leq m, p \nmid k$인 모든 k에 대하여 취한다.

Proof. 다음과 같다 하자.

$$f(x) = \frac{x^{p^r} - 1}{x^{p^{r-1}} - 1} = 1 + x^{p^{r-1}} + x^{2p^{r-1}} + \cdots + x^{(p-1)p^{r-1}}$$

그 경우 (위와 같은 k에 대한) 모든 ω^k들은 $x^{p^r} - 1$의 근이지만 $x^{p^{r-1}-1}$의 근이 아니므로 f의 근이다. k의 값이 정확히 $\varphi(p^r) = (p-1)p^{r-1}$개 존재하므로 다음이 성립한다.

$$f(x) = \prod_k (x - \omega^k)$$

마지막으로 $x = 1$을 대입하라. □

Proof of Theorem 10. Theorem 9에 의해 모든 $\alpha \in R = \mathbb{A} \cap \mathbb{Q}[\omega]$는 다음 형태로 표현될 수 있다.

$$\alpha = \frac{m_1 + m_2(1-\omega) + \cdots + m_n(1-\omega)^{n-1}}{d}$$

여기에서 $n = \varphi(p^r)$이고 모든 $m_i \in \mathbb{Z}$이며 $d = \operatorname{disc}(1-\omega) = \operatorname{disc}(\omega)$이다. 우리는 이미 (임의의 m에 대하여) $\operatorname{disc}(\omega)$가 $m^{\varphi(m)}$의 인수임을 보였으며 따라서 이 경우 d는 p의 멱이다. $R = \mathbb{Z}[1-\omega]$임을 보이겠다; 그 경우 Lemma 1에서 정리가 따라올 것이다.
만약 $R \neq \mathbb{Z}[1-\omega]$일 경우 모든 m_i가 d를 인수로 갖지는 않도록 하는 어떠한 α가 존재해야 한다. R이 다음 형태의 원소를 포함함이 따라온다.

$$\beta = \frac{m_i(1-\omega)^{i-1} + m_{i+1}(1-\omega)^i + \cdots + m_n(1-\omega)^{n-1}}{p}$$

여기에서 $i \leq n$이고 $m_j \in \mathbb{Z}$들이 정수이며 $p \nmid m_i$이다. (왜 그런가?) $1 - \omega^k$가 ($\mathbb{Z}[\omega]$에서) $1 - \omega$를 인수로 가짐을 간단히 보일 수 있으므로 Lemma 2는 $p/(1-\omega)^n \in \mathbb{Z}[\omega]$임을 보여준다. 그 경우 $p/(1-\omega)^i \in \mathbb{Z}[\omega]$이며 따라서 $\beta p/(1-\omega)^i \in R$이다. 명백히 R에 속하는 항들을 제외하면 $m_i/(1-\omega) \in R$을 얻는다. $\mathrm{N} = \mathrm{N}^{\mathbb{Q}[\omega]}$에 대하여 $\mathrm{N}(1-\omega) | \mathrm{N}(m_i)$임이 따라온다. 그러나 $\mathrm{N}(m_i) = m_i^n$이지만 Lemma 2에 의해 $\mathrm{N}(1-\omega) = p$이므로 이는 불가능하다. □

수환은 1개 초과의 정수적 기저를 가질 수 있으며 이들 중 자명한 한 가지 선택이 항상 존재하는 것도 아니다. 그러나 이들은 모두 같은 판별식을 가진다.

Theorem 11. $\{\beta_1, \ldots, \beta_n\}$과 $\{\gamma_1, \ldots, \gamma_n\}$이 $R = \mathbb{A} \cap K$에 대한 2개의 정수적 기저라 하자. 그 경우 $\operatorname{disc}(\beta_1, \ldots, \beta_n) = \operatorname{disc}(\gamma_1, \ldots, \gamma_n)$이다.

Proof. β들을 γ들로 표현하면 다음을 얻는다.

$$\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = M \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix}$$

여기에서 M은 $\mathbb{Z}$ 상에서의 $n \times n$ 행렬이다.
각각의 σ_j를 각각의 n개 방정식에 적용하면 행렬방정식 $[\sigma_j(\beta_i)] = M[\sigma_j(\gamma_i)]$를 얻는다. 행렬식을 취하고 제곱하면 다음을 얻는다.

$$\operatorname{disc}(\beta_1, \ldots, \beta_n) = |M|^2 \operatorname{disc}(\gamma_1, \ldots, \gamma_n)$$

M이 $\mathbb{Z}$ 상에서의 행렬이므로 명백히 $|M| \in \mathbb{Z}$이다; 이는 $\operatorname{disc}(\gamma_1, \ldots, \gamma_n)$이 $\operatorname{disc}(\beta_1, \ldots, \beta_n)$의 인수이며 이들이 같은 부호를 가짐을 보여준다. (β_i들과 γ_i들이 모두 대수적 정수이므로 이러한 판별식들이 정수임을 기억해 두라.) 반면에 유사한 논의는 $\operatorname{disc}(\beta_1, \ldots, \beta_n)$이 $\operatorname{disc}(\gamma_1, \ldots, \gamma_n)$의 인수임을 보여준다. 판별식들이 같다고 결론지을 수 있다. □

그러므로 정수적 기저의 판별식은 환 R의 불변량으로 간주될 수 있다. 이를 $\operatorname{disc}(R)$로 표기하자. 우리는 또한 $R = \mathbb{A} \cap K$인 경우 이를 $\operatorname{disc}(K)$로도 표기할 것이다.
예를 들어 m이 제곱 없는 정수라 가정하면 다음이 성립한다.

$$\operatorname{disc}(\mathbb{A} \cap \mathbb{Q}[\sqrt{m}]) = \begin{cases} \operatorname{disc}(\sqrt{m}) = 4m & (m \equiv 2 \text{ 또는 } 3 \pmod 4) \\ \operatorname{disc}\left(\dfrac{1+\sqrt{m}}{2}\right) = 4m & (m \equiv 1 \pmod 4) \end{cases}$$

(Exercise: 지금까지 수립한 여러 공식들을 이용하여 이러한 계산을 4가지 방법으로 검증하라.)

판별식의 한 가지 응용은 정수적 기저들을 판별하는 것이다: $\alpha_1, \ldots, \alpha_n \in R$이면 이들이 R에 대한 정수적 기저를 형성할 필요충분조건은 $\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \operatorname{disc}(R)$인 것이다. (exercise 27(d)를 참조하라.)

다른 응용으로 우리는 Theorem 10을 임의의 원분체에 대하여 일반화할 것이다. 이는 K와 L의 합성체 KL에서의 대수적 정수들을 K와 L에서의 대수적 정수들과 연관짓는 더 일반적인 결과에서 따라올 것이다. 우리는 K, L이 수체이면 (K와 L을 포함하는 $\mathbb{C}$의 최소 부분체로 정의된) **합성(composite)** KL이 다음의 모든 유한합들로 구성됨을 알고 있다. (Appendix B를 참조하라.)

$$\alpha_1\beta_1 + \cdots + \alpha_r\beta_r \qquad (\alpha_i \in K, \beta_i \in L \ \forall i)$$

R, S, L가 각각 K, L, KL에서의 대수적 정수환이라 하면 T가 다음 환을 포함함은 명백하다.

$$RS = \{\alpha_1\beta_1 + \cdots + \alpha_r\beta_r : \alpha_i \in R, \beta_i \in S \ \forall i\}$$

등호가 성립하는지를 묻는 것은 자연스럽다. 일반적으로는 그렇지 않다. (exercise 31을 참조하라.) 그러나 (편리하게도 원분체에서 성립하는) 특정 조건 하에서는 $T = RS$임을 보일 수 있다.

m, n이 각각 K, L의 $\mathbb{Q}$ 상에서의 차수라 하자. d가 다음의 최대공약수를 나타낸다 하자.

$$\gcd(\operatorname{disc} R, \operatorname{disc} S)$$

Theorem 12. $[KL : \mathbb{Q}] = mn$이라 가정하자. 그 경우 $T \subset \frac{1}{d}RS$이다.

그러므로 특히 다음이 성립한다.

Corollary 1. 만약 $[KL : \mathbb{Q}] = mn$이며 $d = 1$이면 $T = RS$이다.

Theorem 12를 증명하기 위해 체론에서의 보조정리가 필요하다:

Lemma 1. $[KL : \mathbb{Q}] = mn$이라 가정하자. σ가 K의 $\mathbb{C}$로의 매장이며 τ가 L의 $\mathbb{C}$로의 매장이라 하자. 그 경우 K로의 제한이 σ이며 L로의 제한이 τ이도록 하는 KL의 $\mathbb{C}$로의 매장이 존재한다.

Proof. σ의 KL의 $\mathbb{C}$로의 매장으로의 서로 다른 n가지 확장이 존재함을 알고 있다(Appendix B를 참조하라); 이들 중 어떠한 2개도 L에서 일치하지 않으며 따라서 L로의 서로 다른 n가지 제한이 존재한다. L이 $\mathbb{C}$로의 매장을 n개만 가지므로 이들 중 하나는 τ여야 한다. □

Proof of Theorem 12. $\{\alpha_1, \ldots, \alpha_n\}$이 R의 $\mathbb{Z}$ 상에서의 기저(i.e. R에 대한 정수적 기저)이며 $\{\beta_1, \ldots, \beta_n\}$이 S의 $\mathbb{Z}$ 상에서의 기저라 하자. 그 경우 mn개 곱 $\alpha_i\beta_j$들은 RS의 $\mathbb{Z}$ 상에서의 기저를 형성하며 이는 동시에 KL의 $\mathbb{Q}$ 상에서의 기저이다. (왜 그런가?) 임의의 $\alpha \in T$는 다음 형태로 표현될 수 있다.

$$\alpha = \sum_{i,j} \frac{m_{ij}}{r}\alpha_i\beta_j$$

여기에서 r과 모든 m_{ij}들은 $\mathbb{Z}$에 속하고 이러한 $mn + 1$개 정수들은 1 초과의 공통인수를 갖지 않는다: $\gcd(r, \gcd(m_{ij})) = 1$.
정리를 증명하기 위해 우리는 임의의 이러한 α에 대하여 $r|d$임을 보여야 한다. 명백히 $r|\operatorname{disc}(R)$임을 보이면 충분하다; 대칭성에 의해 r은 $\operatorname{disc}(S)$의 인수도 될 것이며 증명이 완료될 것이다.
보조정리는 K의 $\mathbb{C}$로의 임의의 매장 σ가 L의 각 점을 고정하는 KL의 $\mathbb{C}$로의 매장(여전히 σ로 표기하겠다)으로 확장됨을 보여준다. 따라서 각각의 σ에 대하여 다음이 성립한다.

$$\sigma(\alpha) = \sum_{i,j} \frac{m_{ij}}{r}\sigma(\alpha_i)\beta_j$$

각각의 $i = 1, \ldots, m$에 대하여 다음과 같이 설정하면,

$$x_i = \sum_{j=1}^{n} \frac{m_{ij}}{r}\beta_j$$

각각의 σ마다 하나씩 m개 방정식을 얻는다.

$$\sum_{i=1}^{m} \sigma(\alpha_i)x_i = \sigma(\alpha)$$

이제 Cramer 규칙에 의해 x_i들에 대하여 해결하자: 계수 $\sigma(\alpha_i)$들에 의해 형성된 행렬식을 δ라 하고 δ에서 i열을 $\sigma(\alpha)$로 대체하여 얻어진 행렬식을 y_i라 하면 $x_i = y_i/\delta$이다. 모든 $\sigma(\alpha_i)$들과 $\sigma(\alpha)$가 대수적 정수이므로 δ와 모든 γ_i들이 대수적 정수임을 자명하다; 이에 더해 $\delta^2 = \mathrm{disc}(R)$이다. $e = \mathrm{disc}(R)$이라 하면 $ex_i = \delta\gamma_i \in \mathbb{A}$를 얻는다; 그 경우 사실 다음이 성립한다.

$$ex_i = \sum_{j=1}^{n} \frac{em_{ij}}{r}\beta_j \in \mathbb{A} \cap L = S$$

β_j들이 S에 대한 정수적 기저를 형성함을 상기하면 유리수 em_{ij}/r들이 모두 정수여야 한다 결론지을 수 있다: 그러므로 r은 모든 em_{ij}들의 인수이다. 가정에 의해 r이 $\gcd(m_{ij})$와 서로 소이므로 $r|e = \mathrm{disc}(R)$이다. □

Corollary 1을 이용하여 다음을 증명할 수 있다.

Corollary 2. $K = \mathbb{Q}[\omega], \omega = e^{2\pi i/m}, R = \mathbb{A} \cap K$라 하자. 그 경우 $R = \mathbb{Z}[\omega]$이다.

Proof. m이 소수의 멱인 경우 이는 이미 증명되었다. 만약 m이 소수의 멱이 아닌 경우 서로 소 정수 $m_1, m_2 > 1$에 대하여 $m = m_1m_2$로 표현할 수 있다. 우리는 m_1과 m_2에 대한 결과가 m에 대한 결과를 함의함을 보일 것이다. (그러므로 m에 대한 귀납법에 의해 $R = \mathbb{Z}[\omega]$를 증명할 것이다.) 다음과 같다 하면,

$$\begin{aligned} \omega_1 &= e^{2\pi i/m_1} \quad & \omega_2 &= e^{2\pi i/m_2} \\ K_1 &= \mathbb{Q}[\omega_1] \quad & K_2 &= \mathbb{Q}[\omega_2] \\ R_1 &= \mathbb{A} \cap K_1 \quad & R_2 &= \mathbb{A} \cap K_2 \end{aligned}$$

$R_1 = \mathbb{Z}[\omega_1], R_2 = \mathbb{Z}[\omega_2]$라 가정하자. (귀납가정) Corollary 1을 적용하기 위해 우리는 $K = K_1K_2$이며 차수와 판별식 조건이 성립함을 보여야 한다. 명백히 $\omega^{m_1} = \omega_2, \omega^{m_2} = \omega_1$이다. 어떠한 $r, s \in \mathbb{Z}$에 대하여 $\omega = \omega_1^r\omega_2^s$이며 (왜 그런가?) 따라서 $K = K_1K_2$이다. 이에 더해 이는 $\mathbb{Z}[\omega] = \mathbb{Z}[\omega_1]\mathbb{Z}[\omega_2]$임을 보여준다. 차수 조건이 성립한다: m_1, m_2가 서로 소이므로 $\varphi(m) = \varphi(m_1)\varphi(m_2)$이다. 판별식 조건을 보이기 위해 $\mathrm{disc}(\omega_1)$이 m_1의 멱의 인수이며 $\mathrm{disc}(\omega_2)$가 m_2의 멱의 인수임을 보였음을 상기하라. 이제 다음이 성립한다 결론지을 수 있다.

$$R = R_1R_2 = \mathbb{Z}[\omega_1]\mathbb{Z}[\omega_2] = \mathbb{Z}[\omega]$$

□

만약 모든 수환이 어떠한 α에 대하여 $\mathbb{Z}[\alpha]$ 형태라면 좋을 것이다. 불운하게도 이는 항상 성립하지는 않는다. (exercise 30을 참조하라.) 이와 동치로 $1, \alpha, \ldots, \alpha^{n-1}$ 형태의 정수적 기저가 존재하지 않을 수도 있다. 이는 다음의 모호한 문제를 제기한다: 구성원들이 하나의 원소에 의해 표현될 수 있도록 하는 정수적 기저가 항상 존재하는가? 물론 어떠한 α에 대하여 $K = \mathbb{Q}[\alpha]$이며 따라서 K의 모든 원소가 α에 대한 $\mathbb{Q}$-계수 다항식 표현을 가지므로 답은 '그렇다'이다. 이는 그다지 흥미롭지 않다. 그러나 이러한 다항식들이 특정한 형태를 가져야 한다고 요구한다면 어떻겠는가? 해답이 다음 결과에 의해 제시된다:

Theorem 13. $\alpha \in R$이며 α가 $\mathbb{Q}$ 상에서 차수 n을 가진다 하자. 그 경우 $d_1|d_2|\cdots|d_{n-1}$을 만족시키는 $d_i \in \mathbb{Z}$들과 차수 i의 $\mathbb{Z}$-1계수다항식 f_i들에 대하여 다음과 같은 형태의 정수적 기저가 존재한다.

$$1, \frac{f_1(\alpha)}{d_1}, \ldots, \frac{f_{n-1}(\alpha)}{d_{n-1}}$$

d_i들은 유일하게 결정된다.

Proof. $d = \mathrm{disc}(\alpha)$라 하고 각각의 $k, 1 \le k \le n$에 대하여 F_k가 $1/d, \alpha/d, \ldots, \alpha^{k-1}/d$에 의해 생성된 계수 k의 자유가환군이며 $R_k = R \cap F_k$라 하자. 그러므로 $R_1 = \mathbb{Z}$이며 $R_n = R$이다. (왜 그런가?) d_i들과 f_i들을 적절히 정의하여 각각의 $k, 1 \le k \le n$에 대하여 다음이 R_k의 $\mathbb{Z}$ 상에서의 기저이도록 할 것이다.

$$1, \frac{f_1(\alpha)}{d_1}, \ldots, \frac{f_{k-1}(\alpha)}{d_{k-1}}$$

$k = 1$의 경우 이는 명백히 참이다. 그러므로 $k < n$을 고정하고 정리에서와 같은 f_i, d_i들에 대하여 $\{1, f_1(\alpha)/d_1, \ldots, f_{k-1}(\alpha)/d_{k-1}\}$이 R_k의 $\mathbb{Z}$ 상에서의 기저라 가정하자. f_k와 d_k를 정의하여 $f_k(\alpha)/d_k$를 추가하면 R_{k+1}의 기저를 얻음을 보여야 한다.
π가 다음 환에서 마지막 인자로의 정준 사영이라 하자.

$$F_{k+1} = \mathbb{Z}\frac{1}{d} \oplus \cdots \oplus \frac{\alpha^k}{d}$$

즉 π는 차수 k의 항을 선택한다. 그 경우 $\pi(R_{k+1})$은 다음의 무한 순환군의 부분군이다.

$$\mathbb{Z}\frac{\alpha^k}{d} = \left\{ \frac{m\alpha^k}{d} : m \in \mathbb{Z} \right\}$$

이는 $\pi(R_{k+1})$ 자신이 무한 순환군임을 함의한다. $\pi(\beta)$가 $\pi(R_{k+1})$을 생성하도록 하는 임의의 $\beta \in R_{k+1}$을 고정하자. $\{1, f_1(\alpha)/d_1, \ldots, f_{k-1}(\alpha)/d_{k-1}, \beta\}$가 R_{k+1}의 $\mathbb{Z}$ 상에서의 기저임을 보이는 것을 독자에게 남기겠다. (exercise 36)
β가 올바른 형태를 가짐을 보이는 것이 남아있다. 다음이 성립한다.

$$\frac{\alpha^k}{d_{k-1}} = \pi\left(\frac{\alpha f_{k-1}(\alpha)}{d_{k-1}}\right)$$

또한 이는 $\pi(R_{k+1})$에 속한다. (왜 그런가?) 어떠한 $m \in \mathbb{Z}$에 대하여 $\alpha^k/d_{k-1} = m\pi(\beta)$임이 따라온다. $d_k = md_{k-1}$으로 정의하면 $\pi(\beta) = \alpha^k/d_k$이며 이는 어떠한 $f_k(\alpha) = \alpha^k$+저차항에 대하여 $\beta = f_k(\alpha)/d_k$임을 함의한다. 그러나 f_k가 정수계수인지는 아직 알 수 없다; df_k/d_k가 정수계수라는 사실만 알 수 있다. 그러나 $f_k(\alpha)/d_{k-1} = m\beta \in R$이므로 다음이 성립한다.

$$\frac{f_k(\alpha) - \alpha f_{k-1}(\alpha)}{d_{k-1}} = \gamma \in R$$

사실 이는 $\gamma \in R_k$이도록 선택되었다. R_k에 대한 우리의 기저를 사용하여 어떠한 k차 미만의 $g \in \mathbb{Z}[x]$에 대하여 $\gamma = g(\alpha)/d_{k-1}$로 표현하자. 이것이 다항식 $f_k(x) - xf_{k-1}(x)$가 $g(x)$와 동일함을 함의함을 보이는 것은 독자에게 남기겠다. (exercise 37을 참조하라.) 따라서 $f_k \in \mathbb{Z}[x]$이다.
마지막으로 d_i들이 유일하게 결정됨을 보이기 위해서는 (증명이 아니라 정리에서) d_i에 대한 조건이 d_k가 $mR_{k+1} \subset \mathbb{Z}[\alpha]$을 만족시키는 최소 정수임을 함의함을 관찰하라. (이를 검증하라; exercise 38을 참조하라.) □

우리는 이를 2차수체에 대하여 이미 보였다: 제곱 없는 정수 m에 대하여 $\alpha = \sqrt{m}$으로 선택하면 $m \equiv 2$ 또는 $3 \pmod 4$인 경우 정수적 기저 $\{1, \alpha\}$를, $m \equiv 1 \pmod 4$인 경우 정수적 기저 $\{1, (\alpha+1)/2\}$를 얻는다. 다른 좋은 예시들은 3승 없는 정수 m에 대한 **순수3차수체(pure cubic field)** $\mathbb{Q}[\sqrt[3]{m}]$들에 의해 제공된다. $\alpha = \sqrt[3]{m}$이라 하면 다음 결과를 얻는다:

만약 m이 제곱 없는 정수이면 $R = \mathbb{A} \cap \mathbb{Q}[\alpha]$에 대한 기저는 다음 원소들로 구성된다.

$$\begin{cases} 1, \alpha, \alpha^2 & (m \not\equiv \pm 1 \pmod 9) \\ 1, \alpha, \dfrac{\alpha^2 \pm \alpha + 1}{3} & (m \equiv \pm 1 \pmod 9) \end{cases}$$

$\pm$ 부호들은 자명하게 대응된다. 만약 m이 제곱 없는 정수가 아니면 k가 m의 2회 중복된 모든 소인수들의 곱이라 하자. (그러므로 $m = hk^2$이고 h, k가 제곱 없는 정수이며 서로 소이다.) 그 경우 R에 대한 정수적 기저는 다음 원소들로 구성된다.

$$\begin{cases} 1, \alpha, \dfrac{\alpha^2}{k} & (m \not\equiv \pm 1 \pmod 9) \\ 1, \alpha, \dfrac{\alpha^2 \pm k^2\alpha + k^2}{3k} & (m \equiv \pm 1 \pmod 9) \end{cases}$$

이들은 모두 exercise 41에서 증명된다.

Exercises (연습문제)

1.

3 | Prime Decomposition in Number Rings (수환에서의 소 아이디얼 분해)

우리는 수환이 항상 유일 인수분해 정역이지는 않음을 보였다: 원소들은 기약원들로 유일하게 분해되지 않을 수 있다. (비유일 인수분해의 예시를 위해서는 exercise 29, chapter 1 및 exercise 15, chapter 2를 참조하라.) 그러나 우리는 수환의 0이 아닌 아이디얼이 항상 소 아이디얼들로 유일하게 분해됨을 증명할 것이다. 이는 아이디얼들이 주 아이디얼 (n)뿐이고 소 아이디얼들이 소수 p에 대한 (p)들인 $\mathbb{Z}$에서의 유일 인수분해의 일반화로 간주될 수 있다.

우리는 수환이 3가지 특수한 성질들을 가짐을 보이고 이러한 성질들을 가지는 임의의 정역이 아이디얼에 대한 유일 인수분해 성질을 가짐을 보이겠다. 그러므로 다음과 같이 정의할 것이다:

Definition. Dedekind 정역(Dedekind domain)은 다음을 만족시키는 정역 R이다:

(1) 모든 아이디얼이 유한생성이다.
(2) 0이 아닌 모든 소 아이디얼이 극대 아이디얼이다.
(3) 다음과 같은 R의 분수체 내에서 R이 **정수적으로 닫혀 있다(integrally closed)**.

$$K = \{\alpha/\beta : \alpha, \beta \in R, \beta \neq 0\}$$

이러한 마지막 조건은 만약 $\alpha/\beta \in K$가 R 상에서의 어떠한 1계수다항식의 근이면 $\alpha/\beta \in R$임을 의미한다; 즉 R 내에서 $\beta|\alpha$이다.
조건 (1)이 다음의 각 조건과 동치임을 일러두겠다.

(1′) 아이디얼들의 임의의 증가 열이 궁극적으로 상수가 된다: $I_1 \subset I_2 \subset I_3 \subset \cdots$는 충분히 큰 n에 대하여 I_n들이 모두 서로 같음을 함의한다.
(1″) 아이디얼들의 공집합이 아닌 임의의 집합 S는 (유일할 필요는 없는) 극대원을 가진다: $\exists M \in S$ s.t. $M \subset I \in S \Rightarrow M = I$.

이러한 세 조건의 동치를 증명하는 것은 독자에게 남긴다. (exercise 1) 이들을 만족시키는 환은 **Noether 환(Noetherian ring)**이라 불린다.

Theorem 14. 모든 수환은 Dedekind 정역이다.

Proof. 우리는 이미 모든 수환이 (덧셈 하에서) 유한 계수의 자유가환군임을 보였다. (Chapter 2, Theorem 9의 Corollary) 아이디얼 I는 덧셈적 부분군이며 따라서 이는 유한 계수의 자유가환군이다. (Chapter 2, exercise 24) I가 임의의 $\mathbb{Z}$-기저에 생성되며 따라서 아이디얼로서 유한생성임이 따라온다. 이는 (1)을 수립한다.
0이 아닌 모든 소 아이디얼 P가 극대임을 보이기 위해서는 정역 R/P가 사실 체임을 보이면 충분하다. (Appendix A를 참조하라.) 우리는 R/P가 유한집합임을 보일 것이다; 모든 유한 정역이 체이므로 (exercise 2) 결과가 따라올 것이다.
더 일반적으로, 만약 I가 수환의 임의의 0이 아닌 아이디얼이면 R/I가 유한집합이다: α가 I의 임의의 0이 아닌 원소이며 K가 R에 대응하는 수체이고 $m = \mathrm{N}^K(\alpha)$라 하자. 우리는 $m \in \mathbb{Z}$임을 알고 있으며 노름의 정의로부터 $m \neq 0$임을 간단히 보일 수 있다. 이에 더해 $m \in I$이다: 노름의 정의에 의해 β가 α의 공액들의 곱이라 하면 $m = \alpha\beta$이다. 이러한 공액들은 R에 속하지 않을 수 있지만 $\beta = m/\alpha \in K$이며 $\beta \in \mathbb{A}$임을 간단히 보일 수 있으므로 $\beta \in R$이다. 그러므로 우리는 I가 0이 아닌 정수 m을 원소로 가짐을 보였다. 명백히 $R/(m)$은 유한집합이다: 사실 그 위수는 정확히 m^n이다. (이를 증명하라; exercise 3을 참조하라.) $(m) \subset I$이므로 우리는 R/I가 유한집합이라 결론지을 수 있다; 사실 그 위수는 m^n의 인수이다.
마지막으로 R이 K에서 정수적으로 닫혀 있음을 관찰하자: 만약 α/β가 R 상에서의 1계수다항식의 근이면 Chapter 2, exercise 4에 의해 α/β가 대수적 정수이다. 따라서 $\alpha/\beta \in K \cap \mathbb{A} = R$이다. □

우리는 임의의 Dedekind 정역에서의 유일 인수분해 결과를 증명할 것이다. 논의에서 '아이디얼'은 항상 '0이 아닌 아이디얼'을 의미한다.

다음의 중요한 사실이 필요하다:

Theorem 15. I가 Dedekind 정역 R에서의 아이디얼이라 하자. 그 경우 IJ가 주 아이디얼이도록 하는 아이디얼 J가 존재한다.

Proof. α가 I의 0이 아닌 임의의 원소이며 $J = \{\beta \in R : \beta I \subset (\alpha)\}$이라 하자. 그 경우 J가 아이디얼이며 ($\alpha \in J$이므로 0이 아니다.) $IJ \subset (\alpha)$임을 간단히 보일 수 있다. 등호가 성립함을 보이겠다.

두 가지 보조정리가 필요하다:

Lemma 1. Dedekind 정역에서 모든 아이디얼은 소 아이디얼들의 곱을 포함한다.

Proof. 그렇지 않다 가정하자; 그 경우 이러한 곱을 포함하지 않는 아이디얼들의 집합은 공집합이 아니고 결과적으로 조건 $(1'')$에 의해 극대원 M을 가진다. M은 소 아이디얼들의 곱을 포함하지 않으므로 자명하게 소 아이디얼이 아니며, 따라서 $\exists r, s \in R - M$ s.t. $rs \in M$이다. 아이디얼 $M+(r)$과 $M+(s)$는 M보다 강하게 크며 따라서 소 아이디얼들의 곱을 포함해야 한다; 그러나 그 경우 $(M + (r))(M + (s)) \subset M$도 그러하다. 이는 모순이다. □

Lemma 2. A가 분수체 K를 가지는 Dedekind 정역 R에서의 진 아이디얼이라 하자. 그 경우 원소 $\gamma \in K - R$이 존재하여 $\gamma A \subset R$을 만족시킨다.

Proof. 0이 아닌 원소 $a \in A$를 고정하자. Lemma 1에 의해 주 아이디얼 (a)는 소 아이디얼들의 곱을 포함한다; $(a) \supset P_1P_2 \cdots P_r$을 만족시키며 r이 최소이도록 하는 소 아이디얼 $P_1, P_2, \ldots, P_r$들을 고정하자. 모든 진 아이디얼은 극대 아이디얼에 포함되며 이는 반드시 소 아이디얼이어야 한다. (Appendix A를 참조하라.) 따라서 어떠한 소 아이디얼 P에 대하여 $A \subset P$이다. 그 경우 P는 곱 $P_1P_2 \cdots P_r$을 포함한다. P가 어떠한 P_i를 포함함이 따라온다. (만약 그렇지 않다면 원소 $a_i \in P_i - P$를 고정하자; P는 곱 $a_1a_2 \cdots a_r$을 원소로 가지며 따라서 P는 어떠한 a_i를 원소로 가져야 하고 모순이다.) 일반성을 잃지 않고 $P \supset P_1$이라 가정하자. Dedekind 정역의 조건 (2)에 의해 $P = P_1$이어야 한다.
마지막으로 (a)가 r개 미만의 곱을 포함할 수 없음을 상기하라; 특히 $\exists b \in (P_2P_3 \cdots P_r) - (a)$이다. 그 경우 $\gamma = b/a \in K - R$이며 $\gamma A \subset R$이다. (이러한 마지막 주장을 증명하라.) □

Proof of Theorem 15 (Continued). 집합 $A = \frac{1}{\alpha}IJ$를 고려하자. 이는 R에 포함된다. ($IJ \subset (\alpha)$임을 상기하라.) 또한 사실 A는 아이디얼이다. (이를 검증하라.) 만약 $A = R$이면 $IJ = (\alpha)$이며 증명이 완료된다; 그렇지 않은 경우 A는 진 아이디얼이며 Lemma 2를 적용 가능하다. 그러므로 $\gamma A \subset R, \gamma \in K - R$이다. 우리는 여기에서 모순을 얻을 것이다. R이 K에서 정수적으로 닫혀 있으므로 γ가 R 상에서의 1계수 다항식의 근임을 보이면 충분하다.
$\alpha \in I$이므로 $A = \frac{1}{\alpha}IJ$가 J를 포함함을 관찰하라; 그러므로 $\gamma J \subset \gamma A \subset R$이다. $\gamma J \subset J$임이 따라온다; 이것이 왜 참인지를 보이기 위해서는 J의 정의로 돌아가 γJ와 γA가 모두 R에 포함된다는 사실을 사용하라. 세부사항을 채우는 것은 독자에게 남긴다.
마지막으로 아이디얼 J의 생성자 $\alpha_1, \ldots \alpha_m$들을 고정하고 관계 $\gamma J \subset J$를 이용하여 다음의 행렬방정식을 얻자.

$$\gamma \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} = M \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix}$$

여기에서 M은 R 상에서의 $m \times m$ 행렬이다. Theorem 2의 증명에서와 마찬가지로 (행렬식을 통해) γ를 근으로 가지는 R 상에서의 1계수다항식을 얻는다. 이는 증명을 완료한다. □

다음은 Theorem 15의 직접적인 결과이다.

Corollary 1. Dedekind 정역의 아이디얼류들은 군을 형성한다. (Chapter 1, exercise 32를 참조하라.) □

Theorem 15의 2가지 따름정리가 더 존재하여 유일 인수분해를 증명할 수 있게 해 준다:

Corollary 2 (Cancellation Law (소거 법칙))**.** 만약 A, B, C가 Dedekind 정역에서의 아이디얼들이며 $AB = AC$이면 $B = C$이다.

Proof. AJ가 주 아이디얼이도록 하는 아이디얼 J가 존재한다; $AJ = (\alpha)$라 하자. 그 경우 $\alpha B = \alpha C$이며 이로부터 $B = C$임이 간단히 따라온다. □

Corollary 3. 만약 A, B가 Dedekind 정역 R에서의 아이디얼들이면 $A|B$ iff $A \supset B$이다.

Proof. 한쪽 방향은 자명하다: $A|B \Rightarrow A \supset B$이다. 역으로 $A \supset B$라 가정하고 $AJ = (\alpha)$이도록 하는 J를 고정하자. $C = \frac{1}{\alpha}JB$가 R에서의 아이디얼이며 $AC = B$임을 보이는 것은 독자에게 남기겠다. (먼저 $C \subset R$임을 보여라.) □

이러한 결과들을 이용하여 다음을 증명할 수 있다.

Theorem 16. Dedekind 정역 R에서의 모든 아이디얼은 소 아이디얼들의 곱으로 유일하게 표현 가능하다.

Proof. 먼저 우리는 모든 아이디얼이 소 아이디얼들의 곱으로 표현 가능함을 보이겠다: 만약 그렇지 않다면 표현 불가능한 아이디얼들의 집합이 공집합이 아니며 따라서 조건 $(1'')$에 의해 극대원 M을 가진다. R이 빈 곱이며 아이디얼들의 반군의 항등원이 된다는 관습에 의해 $M \neq R$이다. (만약 이러한 관습이 마음에 들지 않는다면 이를 잊어버리고 진 아이디얼들만 고려하라.) M이 어떠한 소 아이디얼 P에 포함됨이 따라온다. (Theorem 15의 Lemma 2의 증명을 참조하라.) 그 경우 위 Corollary 3에 의해 어떠한 아이디얼 I에 대하여 $M = PI$이다. I는 M을 포함하며 소거 법칙에 의해 이것이 진 포함 관계임을 알 수 있다: 만약 $I = M$이면 $RM = PM$이고 $R = P$이며 모순이다. 그러므로 I는 M보다 강하게 크며 따라서 I는 소 아이디얼들의 곱이다. 그러나 그 경우 M도 소 아이디얼들의 곱이므로 가정에 모순이다.
이러한 표현이 유일함을 보이는 것이 남아있다. $P_1P_2\cdots P_r = Q_1Q_1\cdots Q_s$이며 P_i, Q_i들이 (서로 다를 필요는 없는) 소 아이디얼들이라 하자. 그 경우 $P_1 \supset Q_1Q_2\cdots Q_r$이며 이는 $P_1 \supset$ 어떠한 Q_i임을 함의한다. (Theorem 15의 Lemma 2의 증명을 참조하라.) 필요하다면 Q_i들을 재배열하는 것으로 $P_1 \supset Q_1$이라 가정할 수 있다; 그 경우 조건 (2)에 의해 사실 $P = Q$이다. 소거 법칙을 사용하면 $P_2\cdots P_r = Q_2\cdots Q_s$를 얻는다. 이러한 방식으로 계속하면 궁극적으로 $r = s$를 얻으며 (재배열 이후) 모든 i에 대하여 $P_i = Q_i$를 얻는다. □

Theorem 14와 16을 조합하면 다음을 얻는다.

Corollary. 수환의 아이디얼들은 소 아이디얼들로 유일하게 분해된다.

이것의 예시로 수환 $\mathbb{Z}[\sqrt{-5}]$에서의 아이디얼 (2)와 (3)을 고려하자. 다음을 즉시 보일 수 있다.

$$(2) = (2, 1+\sqrt{-5})^2$$
$$(3) = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$$

(이를 검증하라; 곱 $(\alpha,\beta)(\gamma,\delta)$가 $\alpha\gamma, \beta\gamma, \alpha\delta, \beta\delta$에 의해 생성됨을 기억해 두라.) 이에 더해 우변의 모든 아이디얼들이 소 아이디얼이다: 이는 $|R/(2)| = 4$이며 따라서 $R/(2, 1+\sqrt{-5})$가 4의 인수 위수를 가짐을 관찰하는 것으로 보일 수 있다. $(2, 1+\sqrt{-5})$가 (2)를 진 포함하며 R 전체일 수 없으므로 (만약 그렇다면 그 제곱도 R일 것이다) 유일한 가능성은 2이다. 이는 $(2, 1+\sqrt{-5})$가 덧셈 부분군으로서 극대이며 따라서 극대 아이디얼이고 그러므로 소 아이디얼임을 보여준다. 마찬가지로 (3)의 인자들도 소 아이디얼이다.

이는 Chapter 2, exercise 15에서 주어진 비유일 인수분해의 예시에 새로운 실마리를 제공한다: $(2)(3) = (1+\sqrt{-5})(1-\sqrt{-5})$이다. $(1+\sqrt{-5}) = (2, 1+\sqrt{-5})(3, 1+\sqrt{-5})$이며 $(1-\sqrt{-5}) = (2, 1+\sqrt{-5})(3, 1-\sqrt{-5})$임을 검증하라. 그러므로 모든 원소들(더 엄밀히는 대응하는 주 아이디얼들)이 소 아이디얼들로 분해될 경우 6의 두 가지 분해가 동일해진다.

Theorem 16의 관점에서 우리는 소 아이디얼 분해를 통해 자명한 방법으로 임의의 두 아이디얼의 최대공약수 $\gcd(I, J)$와 최소공배수 $\mathrm{lcm}(I, J)$를 정의할 수 있다. 용어 '최소'나 '최대'는 사실 이곳에서 반대 의미를 가진다: Theorem 15의 Corollary 3은 '배수'가 부분아이디얼을, '인수'가 확대아이디얼을 의미함을 보여준다; 그러므로 $\gcd(I, J)$는 사실 I와 J를 모두 포함하는 최소 아이디얼이며 $\mathrm{lcm}(I, J)$는 두 아이디얼에 모두 포함된 최대 아이디얼이다. 따라서 다음이 성립한다.

$$\gcd(I, J) = I + J$$
$$\mathrm{lcm}(I.J) = I \cap J$$

이러한 관찰을 이용하면 Dedekind 정역의 모든 아이디얼이 2개 이하의 원소들에 의해 아이디얼로서 생성됨을 보일 수 있다; 사실 이들 중 하나는 임의로 선택될 수 있다.

Theorem 17. I가 Dedekind 정역 R에서의 아이디얼이라 하고 α가 I의 임의의 0이 아닌 원소라 하자. 그 경우 $\beta \in I$가 존재하여 $I = (\alpha, \beta)$를 만족시킨다.

Proof. 위 관찰에 의해 $I = \gcd((\alpha), (\beta))$를 만족시키는 $\beta \in R$을 구축하면 충분하다. (β는 자동으로 I에 속하게 될 것이다; 왜 그러한가?)

(서로 다른 P_i들에 대하여) $P_1^{n_1}P_2^{n_2}\cdots P_r^{n_r}$이 I의 소 아이디얼 분해라 하자. 그 경우 (α)는 모든 $P_i^{n_i}$를 인수로 가진다. $Q_1,\ldots,Q_s$가 (α)의 인수인 다른 소 아이디얼들을 나타낸다 하자. 어떠한 Q_j도 (β)의 인수가 아니며 각각의 i에 대하여 $P_i^{n_i}$가 (β)의 인수인 P_i의 최고차 멱이도록 하는 β를 구축해야 한다. 이와 동치로,

$$\beta \in \bigcap_{i=1}^{r}(P_i^{n_i} - P_i^{n_i+1}) \cap \bigcap_{j=1}^{s}(R - Q_j)$$

이는 중국인의 나머지 정리에 의해 달성될 수 있다 (Appendix A를 참조하라): $\beta_i \in P_i^{n_i} - P_i^{n_i+1}$(유일 인수분해에 의해 이는 공집합이 아니어야 한다)을 고정하고 β가 다음의 합동식을 만족시킨다 하자.

$$\begin{aligned} \beta &\equiv \beta_i \pmod{P_i^{n_i+1}}, \quad i = 1,\ldots,r \\ \beta &\equiv 1 \pmod{Q_j}, \qquad j = 1,\ldots,s \end{aligned}$$

(이러한 β가 존재함을 보이기 위하여 우리는 P_i의 멱들과 Q_j들이 쌍마다 서로 극대임을 보여야 한다: 이들 중 임의의 2개의 합이 R이다. 합을 최대공약수로 해석하면 이를 간단히 보일 수 있다. 이를 보이는 다른 방법이 exercise 7에 주어져 있다.) □

우리는 모든 주 아이디얼 정역(PID)이 유일 인수분해 정역(UFD)임을 알고 있다. (Appendix A를 참조하라.) 일반적으로 역은 거짓이다: $\mathbb{Z}[x]$는 UFD이지만 PID는 아니다. (exercise 8) 그러나 Dedekind 정역의 경우에는 역이 성립한다:

Theorem 18. Dedekind 정역이 UFD일 필요충분조건은 PID인 것이다.

Proof. 위에서 언급한 것과 같이 PID는 항상 UFD를 함의한다; Dedekind 정역의 경우 Theorem 16을 사용하는 것으로 이러한 결과를 얻을 수도 있다. 역으로 Dedekind 정역 R이 UFD이며 I가 R의 임의의 아이디얼이라 하자. Theorem 15에 의해 I는 어떠한 주 아이디얼 (a)의 인수이다. 원소 a는 R에 속한 소원들의 곱이며 각각의 소원 p가 주 소 아이디얼 (p)를 생성함을 간단히 보일 수 있다: 만약 $ab \in (p)$이면 $p|ab$이며 따라서 $p|a$ 또는 $p|b$이고 이는 $a \in (p)$ 또는 $b \in (p)$임을 함의한다. 그러므로 I는 주 소 아이디얼들의 곱을 인수로 가진다. R의 아이디얼들의 유일 인수분해에 의해 I 자신이 주 소 아이디얼들의 곱이며 따라서 주 아이디얼임을 알 수 있다. □

Splitting of Primes in Extensions (확대에서의 소 아이디얼의 분리)

우리는 $\mathbb{Z}$의 소수들 중 더 큰 수환에서는 기약이 아닌 예시들을 보았다. 예를 들어 $\mathbb{Z}[i]$에서 $5 = (2+i)(2-i)$이다. 2와 3이 $\mathbb{Z}[\sqrt{-5}]$에서 기약임에도 불구하고 대응하는 주 아이디얼 $(2), (3)$은 소 아이디얼이 아니다: $(2) = (2, 1+\sqrt{-5})^2, (3) = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$. 이러한 현상은 **분리(splitting)**라 불린다. 용어를 약간 남용하여 $\mathbb{Z}[\sqrt{-5}]$에서 (또는 $\mathbb{Q}[\sqrt{-5}]$에서; 이 경우 환은 $\mathbb{A} \cap \mathbb{Q}[\sqrt{-5}]$인 것으로 간주하라) 3이 2개 소 아이디얼들의 곱으로 분리된다고 말한다. 주어진 소 아이디얼이 주어진 수환에서 어떻게 분리되는지를 결정하는 문제를 고려하겠다. 일반적으로 만약 P가 임의의 수체 K에서의 수환 $R = \mathbb{A} \cap K$의 임의의 소 아이디얼이며 L이 K의 확대수체이면 수환 $S = \mathbb{A} \cap L$의 P에 의해 생성된 아이디얼의 소 아이디얼 분해를 고려할 수 있다. (이러한 아이디얼은 $PS = \{\alpha_1\beta_1 + \cdots + \alpha_r\beta_r : \alpha_i \in P, \beta_i \in S\}$이다. 만약 P가 주 아이디얼 $P = (\alpha)$이면 PS는 단지 $\alpha S = \{\alpha\beta : \beta \in S\}$이다.)

다음에 다시 말하기 전까지 K, L은 항상 $K \subset L$인 수체이며 $R = \mathbb{A} \cap K, S = \mathbb{A} \cap L$일 것이다. 용어 '소 아이디얼'은 '0이 아닌 소 아이디얼'을 의미할 것이다.

Theorem 19. P가 R의 소 아이디얼이고 Q가 S의 소 아이디얼이라 하자. 그 경우 다음 조건들은 서로 동치이다:

(1) $Q|PS$
(2) $Q \supset PS$
(3) $Q \supset P$
(4) $Q \cap R = P$
(5) $Q \cap K = P$

Proof. (1) ⇔ (2) Theorem 15의 Corollary 3; (2) ⇔ (3) Q가 S에서의 아이디얼이므로 자명; (4) ⇒ (3) 자명; (4) ⇔ (5) $Q \subset \mathbb{A}$이므로 자명. 마지막으로 (3) ⇒ (4)가 성립함을 보이기 위해 $Q \cap R = P$ 또는 R임을 관찰하라. 만약 $Q \cap R = R$이면 $1 \in Q$이며 $Q = S$이고 모순이다. □

조건 (1)-(5)가 성립하면 Q가 P **상에 놓여 있다(lying over P)** 또는 P가 Q **하에 놓여 있다(lying under Q)**고 한다.

Theorem 20. S의 모든 소 아이디얼 Q는 R의 유일한 소 아이디얼 P 상에 놓여 있다; R의 모든 소 아이디얼 P는 S의 1개 이상의 소 아이디얼 Q 하에 놓여 있다.

Proof. 전반부는 $Q \cap R$이 R에서의 소 아이디얼임을 보이는 것과 동치이다. 이는 소 아이디얼의 정의와 $1 \notin Q$라는 사실에서 간단히 따라온다. 노름 논의를 통해 $Q \cap R$이 0이 아님을 보이는 것으로 세부사항을 채워라. 후반부에서 P 상에 놓인 소 아이디얼들은 PS의 소인자들이다; 그러므로 우리는 $PS \neq S$임을 보이는 것으로 1개 이상의 소인자가 존재함을 보여야 한다. 이와 동치로 $1 \notin PS$임을 보여야 한다. (우리는 $1 \notin P$임을 알고 있지만, $\alpha_1\beta_1 + \cdots + \alpha_r\beta_r, \alpha_i \in P, \beta_i \in S$가 어째서 1이 될 수 없는가?) $1 \notin PS$임을 보이기 위해 Theorem 15의 Lemma 2를 사용하자: $\gamma \in K - R$이 존재하여 $\gamma P \subset R$을 만족시킨다. 그 경우 $\gamma PS \subset RS = S$이다. 만약 $1 \in PS$이면 $\gamma \in S$이다. 그러나 그 경우 γ가 대수적 정수이므로 $\gamma \in K - R$에 모순이다. □

앞에서 언급한 것과 같이 주어진 P 상에 놓여 있는 소 아이디얼들은 PS의 소 아이디얼 분해에서 등장하는 것들이다. 이들이 등장하는 횟수는 **분기지표(ramification index)**라 불린다. 그러므로 만약 Q^e가 PS의 인수인 Q의 최고차 멱이면 e가 P 상에서의 Q의 분기지표이며 $e(Q|P)$로 표기된다.

Example. $R = \mathbb{Z}, S = \mathbb{Z}[i]$라 하자; 그 경우 S에서의 주 아이디얼 $(1-i)$는 2 상에 놓여 있다. (여기에서 2로 표기하지만 실제로는 $2\mathbb{Z}$를 의미한다.) 사실 $(1-i)$는 소 아이디얼이다. (이는 Theorem 16 이후의 $Z[\sqrt{-5}]/(2, 1+\sqrt{-5})$의 경우와 마찬가지로 $S/(1-i)$의 위수를 고려하는 것으로 보일 수 있다.) $2S = (1-i)^2$이므로 $e((i-1)|2) = 2$이다. 반면에 $p \neq 2$이며 Q가 p 상에 놓여 있는 경우 $e(Q|p) = 1$이다. 더 일반적으로, $R = \mathbb{Z}$이며 어떠한 소수 $p \in \mathbb{Z}$에 대하여 $m = p^r$이고 $\omega = e^{2\pi i/m}, S = \mathbb{Z}[\omega]$이면 S에서의 주 아이디얼 $(1-\omega)$는 p 상에 놓여 있는 소 아이디얼이며 $e((1-\omega)|p) = \varphi(m) = p^{r-1}(p-1)$이다. (Chapter 2, exercise 34(b) 및 Theorem 22의 증명 이후의 언급을 참조하라.) 반면에 $q \neq p$이며 Q가 q 상에 놓여 있는 경우 $e(Q|q) = 1$이다; 이는 Theorem 24에서 따라올 것이다.

Q가 P 상에 놓여 있도록 하는 소 아이디얼 P, Q의 쌍에 연관된 다른 중요한 수가 존재한다. P, Q가 극대 아이디얼이므로 우리는 몫환 R/P와 S/Q가 체임을 알고 있다. 이에 더해 R/P는 자명한 방식으로 S/Q의 부분체로 간주될 수 있다: 포함 관계 $R \subset S$는 환 준동형사상 $R \to S/Q$를 유도하며 그 핵은 $R \cap Q$이다. $R \cap Q = P$임을 알고 있으므로 (Theorem 19) 매장 $R/P \to S/Q$를 얻는다. 이들은 P와 Q에 연관된 **잉여류체(residue field)**라 불린다. 우리는 이들이 모두 유한체임을 알고 있으며 (Theorem 14의 증명을 참조하라) 따라서 S/Q는 R/P 상에서 유한 차수 확대이다; f가 차수라 하자. 그 경우 f는 Q의 P 상에서의 **관성차수(inertial degree)**라 불리며 $f(Q|P)$로 표기된다.

Example. $R = \mathbb{Z}, S = \mathbb{Z}[i]$라 하자; $\mathbb{Z}$에서의 소수 2가 $\mathbb{Z}[i]$에서의 소 아이디얼 $(1-i)$ 하에 놓여 있음을 보였다. $S/2S$는 위수 4를 가지며 $(1-i)$는 $2S$를 진 포함한다; 그러므로 $|S/(1-i)|$는 4의 진 인수가 되어야 하며 유일한 가능성은 2이다. 따라서 이 경우 R/P와 S/Q가 모두 위수 2의 체이며 그러므로 $f = 1$이다. 반면에 $3S$는 (Chapter 1, exercise 3과 S가 PID라는 사실에 의해) S에서의 소 아이디얼이며 $|S/3S| = 9$이고 따라서 $f(3S|3) = 2$이다.

e와 f가 다중 확대에서 곱셈적임을 기억해 두라: 만약 $P \subset Q \subset U$가 3개 수환 $R \subset S \subset T$에서의 소 아이디얼들이면 다음이 성립한다.

$$e(U|P) = e(U|Q)e(Q|P)$$
$$f(U|P) = f(U|Q)f(Q|P)$$

이를 증명하는 것은 독자에게 남긴다. (exercise 10)

일반적으로 Q가 임의의 수환 S에서의 임의의 소 아이디얼이면 Q가 유일한 소수 $p \in \mathbb{Z}$ 상에 놓임을 알고 있다. 그 경우 S/Q는 위수 p^f의 체이다. ($f = f(Q|p)$) 우리는 Q가 pS를 포함함을 알고 있으며 따라서 p^f는 $|S/pS| = p^n$ 이하이다. (여기에서 n은 S에 대응하는 수체 L의 $\mathbb{Q}$ 상에서의 차수이다.) 이는 기반체가 $\mathbb{Q}$인 특수한 경우에 관계 $f \leq n$을 제공한다. 사실 이보다 더 강한 것이 참이다:

Theorem 21. (R, S, K, L이 앞에서와 같고) n이 L의 K 상에서의 차수이며 $Q_1, \ldots, Q_r$이 R의 소 아이디얼 P 상에 놓인 S의 소 아이디얼들이라 하자. 대응하는 분기지표와 관성차수를 $e_1, \ldots, e_r$과 $f_1, \ldots, f_r$이라 하자. 그 경우 $\sum_{i=1}^{r} e_i f_i = n$이다.

우리는 이 정리를 다른 정리와 동시에 증명할 것이다. R-아이디얼 I에 대하여 지표 $|R/I|$를 $\|I\|$로 표기하겠다.

Theorem 22. R, S, K, L이 앞에서와 같으며 $n = [L : K]$라 하자.

(a) R에서의 아이디얼 I, J에 대하여 다음이 성립한다.

$$\|IJ\| = \|I\|\|J\|$$

(b) I가 R에서의 아이디얼이라 하자. S-아이디얼 IS에 대하여 다음이 성립한다.

$$\|IS\| = \|I\|^n$$

(c) $\alpha \in R, \alpha \neq 0$이라 하자. 주 아이디얼 (α)에 대하여 다음이 성립한다.

$$\|(\alpha)\| = |\,\mathrm{N}_{\mathbb{Q}}^{K}(\alpha)|$$

Proof of Theorem 22(a). 먼저 I, J가 서로 소인 경우에 대하여 증명하고 모든 소 아이디얼 P에 대하여 $\|P^m\| = \|P\|^m$임을 보이자. 이는 다음을 함의한다.

$$\|P_1^{m_1} \cdots P_r^{m_r}\| = \|P_1\|^{m_1} \cdots \|P_r\|^{m_r}$$

I, J를 소 아이디얼들로 분해하고 위 공식을 적용하면 Theorem 22(a)를 얻는다.

그러므로 먼저 I, J가 서로 소라 가정하자. 그 경우 $I + J = R$이며 $I \cap J = IJ$이다. (Theorem 17을 참조하라.) 중국인의 나머지 정리(Appendix A)에 의해 다음의 동형사상이 존재한다.

$$R/IJ \to R/I \times R/J$$

따라서 다음이 성립한다.

$$\|IJ\| = \|I\|\|J\|$$

다음으로 소 아이디얼 P에 대한 $\|P^m\|$을 고려하자. 아이디얼들의 연쇄 $R \supset P \supset P^2 \supset \cdots \supset P^m$이 존재하며 따라서 각각의 k에 대하여 다음을 보이면 충분하다.

$$\|P\| = |P^k/P^{k-1}|$$

여기에서 P^k는 곱셈군으로 간주된다. 우리는 사실 다음의 군 동형사상이 존재함을 주장하겠다.

$$R/P \to P^k/P^{k+1}$$

먼저 임의의 $\alpha \in P^k - P^{k+1}$을 고정하면 다음의 자명한 동형사상이 존재한다.

$$R/P \to \alpha R/\alpha P$$

다음으로 포함 관계 $\alpha R \subset P^k$는 다음의 준동형사상을 유도한다.

$$\alpha R \to P^k/P^{k+1}$$

그 핵은 $(\alpha R) \cap P^{k+1}$이며 그 상은 $((\alpha R) + P^{k+1})/P^{k+1}$이다. 우리가 원하는 것을 증명하기 위해서는 $(\alpha R) \cap P^{k+1} = \alpha P$이며 $(\alpha R) + P^{k+1} = P^k$임을 보여야 한다. 이는 P^k가 αR의 인수인 P의 최대 멱임을 명심하고 αR과 P^{k+1}의 최소공배수 및 최대공약수를 고려하는 것으로 간단히 해결될 수 있다. (독자가 확인해 보라.) □

Proof of Theorem 21, Special Case. Theorem 21을 $K = \mathbb{Q}$인 경우에 대하여 증명하자. 그 경우 어떠한 소수 $p \in \mathbb{Z}$에 대하여 $P = p\mathbb{Z}$이다. 다음이 성립한다.

$$pS = \prod_{i=1}^{r} Q_i^{e_i}$$

따라서,

$$\|pS\| = \prod_{i=1}^{r} \|Q_i\|^{e_i} = \prod_{i=1}^{r} (p^{f_i})^{e_i}$$

반면에 우리는 $\|pS\| = p^n$임을 알고 있다. 그러므로 이러한 특수한 경우에 대하여 결과를 수립했다. □

Proof of Theorem 22(b). Theorem 22(a)의 관점에서 I가 소 아이디얼 P인 경우에 대하여 증명하면 충분하다; I를 소 아이디얼들로 분해하는 것으로 일반적인 결과가 따라올 것이다.

S/PS가 체 R/P 상에서의 벡터 공간임을 기억해 두라. (이를 검증하라; 실제로는 S/PS가 R/P를 포함하는 환임을 보여라.) 우리는 이것이 n차원임을 주장하겠다.

먼저 차원이 n 이하임을 보이자. 임의의 $n+1$개 원소들이 선형 종속임을 보이면 충분하다. 그러므로 $\alpha_1, \dots, \alpha_{n+1} \in S$를 고정하고 S/PS의 대응하는 원소들이 R/P 상에서 선형 종속임을 보이자. 이는 보기보다 간단하지 않다. 우리는 물론 $\alpha_1, \dots, \alpha_{n+1}$이 K 상에서 선형 종속임을 알고 있으며 이들이 R 상에서 선형 종속임이 따라온다. (Chapter 2, exercise 25를 참조하라.) 그러므로 어떠한 $\beta_1, \dots, \beta_{n+1} \in R$이 존재하여 $\beta_1\alpha_1 + \cdots + \beta_{n+1}\alpha_{n+1} = 0$을 만족시킨다. 문제는 β_i들이 전부 P에 속하지는 않으며 따라서 $\bmod P$로 모두 0이 되지는 않음을 보이는 것이다. 이를 위해서는 다음과 같은 Theorem 15의 Lemma 2의 일반화가 필요하다:

Lemma. A와 B가 Dedekind 정역 R에서의 0이 아닌 아이디얼이며 $B \subset A$이고 $A \neq R$이라 하자. 그 경우 $\gamma \in K$가 존재하여 $\gamma B \subset R, \gamma B \not\subset A$를 만족시킨다.

Proof of Lemma. Theorem 15에 의해 0이 아닌 아이디얼 C가 존재하여 BC가 주 아이디얼이도록 한다. 이를 (α)라 하자. 그 경우 $BC \not\subset \alpha A$이다; $\beta B \not\subset \alpha A$이도록 하는 임의의 $\beta \in C$를 고정하고 $\gamma = \beta/\alpha$라 하자. 이는 요구사항을 만족시킨다. □

보조정리를 $A = P$와 $B = (\beta_1, \dots, \beta_{n+1})$에 적용하자. 세부사항을 채우는 것은 독자에게 남기겠다. 그러므로 S/PS가 R/P 상에서 n차원 이하라는 사실을 수립했다.

등호를 수립하기 위해 $P \cap \mathbb{Z} = p\mathbb{Z}$라 하고 p 상에 놓여 있는 R의 모든 소 아이디얼 P_i들을 고려하자. 우리는 S/P_iS가 R/P_i 상에서의 벡터 공간이며 차원 $n_i \leq n$임을 알고 있다; 모든 i에 대하여 (특히 $P_i = P$인 경우에도) 등호가 성립함을 보일 것이다. $e_i = e(P_i|p)$이며 $f_i = f(P_i|p)$라 하자. 그 경우 (이미 증명한) Theorem 21의 특수한 경우에 의해 m이 K의 $\mathbb{Q}$ 상에서의 차수라 하면 $\sum e_i f_i = m$이다. $pR = \prod P_i^{e_i}$이며 따라서 $pS = \prod (P_iS)^{e_i}$이다. Theorem 22(a)를 사용하면 다음을 얻는다.

$$\|pS\| = \prod \|P_iS\|^{e_i} = \prod \|P_i\|^{n_i e_i} = \prod (p^{f_i})^{n_i e_i}$$

반면에 $\|pS\| = p^{mn}$이므로 $mn = \sum f_i n_i e_i$이다. 모든 $n_i \leq n$이며 $\sum e_i f_i = m$이므로 모든 i에 대하여 $n_i = n$임이 따라온다. □

Proof of Theorem 21, General Case. $PS = \prod Q_i^{e_i}$이며 따라서 Theorem 22(a)와 f_i의 정의에 의해 다음이 성립한다.

$$\|PS\| = \prod \|Q_i\|^{e_i} = \prod \|P\|^{f_i e_i}$$

반면에 Theorem 22(b)는 $\|PS\| = \|P\|^n$임을 보여준다. 그러므로 $n = \sum e_i f_i$이다. □

Proof of Theorem 22(c). K를 $\mathbb{Q}$의 정규 확대 M으로 확대하고 $T = \mathbb{A} \cap M$이라 하자. 각각의 매장 $\sigma : K \to \mathbb{C}$에 대하여 다음이 성립한다.

$$\|\sigma(\alpha)T\| = \|\alpha T\|$$

이것이 왜 참인지를 보이기 위해서는 σ를 M의 자기동형사상으로 확장하고 $\sigma(T) = T$임을 관찰하라. (독자는 이러한 논의를 검증하라.) $N = \mathrm{N}^K(\alpha)$로 설정하자. 그 경우 Theorem 22(a)에 의해 다음이 성립한다.

$$\|NT\| = \prod_\sigma \|\sigma(\alpha)T\| = \|\alpha T\|^n$$

명백히 $m = [M : K]$라 하면 $\|NT\| = |N|^{mn}$이다. Theorem 22(b)는 $\|\alpha T\| = \|\alpha R\|^m$임을 보여준다. 이들을 조합하면 $\|\alpha R\| = |N|$을 얻는다. □

이러한 결과의 응용으로 $\mathbb{Z}[(\omega)]$ ($\omega = e^{2\pi i/m}, m = p^r$)에서 주 아이디얼 $(1-\omega)$가 소 아이디얼임을 두 가지 방법으로 보일 수 있다: 우리는 $n = p^{r-1}(p-1) = \varphi(m)$에 대하여 $(1-\omega)^n = p\mathbb{Z}[\omega]$임을 알고 있다. n이 $\mathbb{Q}[\omega]$의 $\mathbb{Q}$ 상에서의 차수이므로 $(1-\omega)$를 소 아이디얼들로 추가적으로 분리한다면 Theorem 21에 모순이 된다; 그러므로 $(1-\omega)$는 반드시 소 아이디얼이어야 한다.

이 결과는 Theorem 22(a)를 통해 얻을 수도 있다:

$$\|(1-\omega)\|^n = \|(1-\omega)^n\| = \|p\mathbb{Z}[\omega]\| = p^n$$

따라서 $\|(1-\omega)\| = p$이다. 이에 더해 Theorem 22(a)는 $\|I\|$가 소수이면 I가 소 아이디얼이어야 함을 보여준다.

3차수체에서의 분리에 관한 예시를 제시하겠다. $K=\mathbb{Q}, L=\mathbb{Q}[\sqrt[3]{2}], S=\mathbb{A}\cap L$이라 하자. $\alpha=\sqrt[3]{2}$에 대하여 $S=\mathbb{Z}[\alpha]$임을 알고 있다. (Chapter 2, exercise 41) 명백히 $2S=(\alpha)^3$이며 따라서 (α)는 소 아이디얼이어야 한다. (추가적인 분리는 Theorem 21에 모순이 된다.) 이에 더해 $f((\alpha)|2)=1$이어야 한다. $2S$를 $3S$로 대체하고 α를 $\alpha+1$로 대체하면 유사한 결과가 성립한다. (이를 검증하라.)

동일한 체에서 우리는 $5S=(5,\alpha+2)(5,\alpha^2+3\alpha-1)$임을 보일 수 있으며 우측의 아이디얼들은 서로 소이다. 그러므로 남은 문제는 이들이 추가적으로 분리되는지에 관한 것뿐이다. 환 $S/(5,\alpha^2+3\alpha-1)$은 위수 25의 체임을 보일 수 있다; 그러므로 $(5,\alpha^2+3\alpha-1)$은 소 아이디얼이며 대응하는 관성차수가 2임을 알 수 있다. 다시 Theorem 21을 적용하면 $(5,\alpha+2)$가 관성차수 1을 가지는 소 아이디얼이어야 함을 알 수 있다. (세부사항을 위해서는 exercise 12를 참조하라.)

이제 α가 $\alpha^3=\alpha+1$을 만족시킨다 하고 $L=\mathbb{Q}[\alpha]$라 하자. 그 경우 Chapter 2, exercise 28(d)에서 보인 것과 같이 $S=\mathbb{A}\cap L=\mathbb{Z}[\alpha]$이다. 우리는 다음의 분해가 성립함을 보일 수 있다.

$$23S=(23,\alpha-10)^2(23,\alpha-3)$$

우변의 아이디얼들은 서로 소이다. (exercise 13을 참조하라.) 우변의 인자들이 소 아이디얼이며 대응하는 관성차수가 1임이 따라온다.

마지막 예시에서 23 상에 놓여 있는 소 아이디얼들은 동일한 분기지표를 갖지 않는다; 앞의 예시에서 5 상에서의 소 아이디얼들은 동일한 관성차수를 갖지 않았다. 우리는 이러한 종류의 상황이 정규 확대가 아닌 체 확대에서만 발생할 수 있음을 보일 것이다.

만약 L이 K의 정규 확대이며 P가 $\mathbb{R}=\mathbb{A}\cap K$의 소 아이디얼이면 Galois 군 $G=\mathrm{Gal}(L/K)$가 P 상에 놓인 소 아이디얼들을 치환한다: 만약 Q가 이러한 소 아이디얼 중 하나이며 $\sigma\in G$이면 $\sigma(Q)$는 $\sigma(S)=S$에서의 소 아이디얼이며 $\sigma(P)=P$ 상에 놓인다. 이에 더해 G는 이들을 추이적으로 치환한다:

Theorem 23. 위와 같은 표기법 하에서 (L이 K의 정규 확대인 경우) Q,Q'이 R의 동일한 소 아이디얼 P 상에 놓여 있는 S의 소 아이디얼이라 하자. 그 경우 어떤 $\sigma\in G$에 대하여 $\sigma(Q)=Q'$이다.

Proof. 모든 $\sigma\in G$에 대하여 $\sigma(Q)\neq Q'$이라 하자. 그 경우 중국인의 나머지 정리(Appendix A)에 의해 다음 합동식계의 해가 존재한다.

$$\begin{aligned} x&\equiv 0 \pmod{Q'}\\ x&\equiv 1 \pmod{\sigma(Q)} \qquad (\forall\sigma\in G)\end{aligned}$$

$\alpha\in S$가 이러한 해라 하자. 그 경우 N_K^L의 인수들 중 하나는 $\alpha\in Q'$이므로 다음이 성립한다.

$$\mathrm{N}_K^L(\alpha)\in R\cap Q'=P$$

반면에 각각의 σ에 대하여 $\alpha\notin\sigma(Q)$이므로 $\sigma^{-1}(\alpha)\notin Q$이다. $\mathrm{N}_K^L(\alpha)$를 모든 $\sigma^{-1}(\alpha)$들의 곱으로 표현할 수 있으며 이들 중 어떤 것도 소 아이디얼 Q에 속하지 않으므로 $\mathrm{N}_K^L(\alpha)\notin Q$임이 따라온다. 그러나 우리는 $\mathrm{N}_K^L(\alpha)\in P\subset Q$임을 이미 보였다. □

이로부터 다음을 얻는다:

Corollary. 만약 L이 K 상에서 정규이며 Q,Q'이 P 상에 놓인 소 아이디얼들이면 $e(Q|P)=e(Q'|P)$이며 $f(Q|P)=f(Q'|P)$이다.

Proof. $e(Q|P)=e(Q'|P)$는 유일 인수분해에서 따라온다; $f(Q|P)=f(Q'|P)$는 동형사상 $S/Q\to S/Q'$을 수립하는 것으로 얻어진다. (세부사항을 채워라.) □

따름정리는 정규 확대의 경우 R의 소 아이디얼 P가 S에서 (서로 다른 소 아이디얼 Q_i들에 대하여) $(Q_1Q_2\cdots Q_r)^e$로 분리되며 이들이 모두 P 상에서 동일한 관성차수를 가짐을 보여준다. 이에 더해 Theorem 21에 의해 $ref=[L:K]$이다.

Definition. K,L,R,S가 통상적인 경우와 같다 하자; R의 소 아이디얼 P가 **S에서 분기(ramified in S)**(또는 L에서 분기)임은 P 상에 놓인 S의 어떠한 소 아이디얼 Q에 대하여 $e(Q|P)>1$인 것이다. (다른 말로 하면 PS가 제곱 없는 아이디얼이 아닌 것이다.)

우리는 p가 $\mathbb{Z}[\omega]$ ($\omega=e^{2\pi i/m}, m=p^r$)에서 분기임을 보였으며 $\mathbb{Z}$의 다른 소수가 $\mathbb{Z}[\omega]$에서 분기가 아니라 주장했다. 우리는 2와 3이 $\mathbb{Z}[\sqrt[3]{2}]$에서 분기임을 보였으나 5는 그렇지 않았다. $\alpha^3=\alpha+1$에 대하여 23이 $\mathbb{Z}[\alpha]$에서 분기임을 보였다. 이러한 환의 판별식이 각각 p의 멱; $-3^3\cdot 2^2$; -23임을 기억해 두라. 일반적으로 소수 $p\in\mathbb{Z}$가 수환 R 상에서 분기일 필요충분조건은 $p|\operatorname{disc}(R)$인 것이다. 우리는 지금 한쪽 방향을 보이고 다른 방향은 Chapter 4로 연기할 것이다.

Theorem 24. p가 $\mathbb{Z}$에서의 소수이며 p가 수환 R에서 분기라 하자. 그 경우 $p|\operatorname{disc}(R)$이다.

Proof. P가 p 상에 놓인 R의 소 아이디얼이며 $e(P|p) > 1$이라 하자. 그 경우 $pR = PI$이며 I는 p 상에 놓인 R의 모든 소 아이디얼의 배수이다.

$\sigma_1, \dots, \sigma_n$이 ($R$에 대응되는 수체) K의 $\mathbb{C}$로의 매장들을 나타낸다 하고 통상적인 경우와 같이 모든 σ_i들을 K의 어떠한 ($\mathbb{Q}$ 상에서 정규인) 확대 L의 자기동형사상들로 확장하자.

$\alpha_1, \dots, \alpha_n$이 R에 대한 임의의 정수적 기저라 하자. 우리는 α_i들 중 하나를 적절한 원소로 대체하는 것으로 $p|\operatorname{disc}(R)$임을 보일 것이다. 임의의 $\alpha \in I - pR$을 선택하자 (우리는 I가 pR을 진 포함함을 알고 있다.); 그 경우 α는 p 상에 놓인 R의 모든 소 아이디얼에 속한다. $\alpha = m_1\alpha_1 + \cdots + m_n\alpha_n, m_i \in \mathbb{Z}$로 표기하면 $\alpha \notin pR$이라는 사실은 모든 m_i가 p의 배수이지는 않음을 함의한다. 필요하다면 α_i들을 재배열하는 것으로 $p \nmid m_1$이라 가정할 수 있다. 다음과 같다 하자.

$$d = \operatorname{disc}(R) = \operatorname{disc}(\alpha_1, \dots, \alpha_n)$$

그 경우 다음을 간단히 보일 수 있다.

$$\operatorname{disc}(\alpha, \alpha_2, \dots, \alpha_n) = m_1^2 d$$

(필요하다면 exercise 18을 참조하라.) $p \nmid m_1$이므로 $p|\operatorname{disc}(\alpha, \alpha_2, \dots, \alpha_n)$임을 보이면 충분하다.

α가 p 상에 놓인 R의 모든 소 아이디얼에 포함됨을 상기하라. α가 p 상에 놓인 $S = \mathbb{A} \cap L$의 모든 소 아이디얼에 포함됨이 따라온다. (이러한 각각의 소 아이디얼은 p를 포함하며 R과의 교집합이 R의 어떠한 소 아이디얼이다; 교집합이 p를 포함하므로 p 상에 놓여 있으며 따라서 α를 포함한다.) p 상에 놓인 S의 임의의 소 아이디얼 Q를 고정하고 L의 각각의 자기동형사상 σ에 대하여 $\sigma(\alpha) \in Q$임을 주장하겠다: 이를 보이기 위해서는 $\sigma^{-1}(\alpha)$가 p 상에 놓인 $\sigma^{-1}(S) = S$의 소 아이디얼이며 따라서 α를 포함함을 기억해 두라. 그 경우 특히 모든 i에 대하여 $\sigma_i(\alpha) \in Q$이다. Q가 $\operatorname{disc}(\alpha, \alpha_2, \dots, \alpha_n)$을 포함함이 따라온다. 판별식이 $\mathbb{Z}$에 속해야 하므로 이는 $Q \cap \mathbb{Z} = p\mathbb{Z}$에 속한다. 이는 증명을 완료한다. □

약간 더 강하게 작업하면 $\operatorname{disc}(R)$의 인수인 p의 멱에 대한 더 강한 진술을 얻을 수 있다. exercise 21을 참조하라.

Corollary 1. $\alpha \in R, K = \mathbb{Q}[\alpha]$이며 f가 $\mathbb{Z}$ 상에서의 1계수다항식이고 $f(\alpha) = 0$을 만족시킨다 하자. 만약 p가 소수이며 $p \nmid \mathrm{N}^K f'(\alpha)$를 만족시키면 p는 K에서 비분기이다. (Chapter 2, exercise 21)을 참조하라. □

Corollary 2. $\mathbb{Z}$의 유한 개 소수만이 수환 R에서 분기이다. □

Corollary 3. R, S가 수환이며 $R \subset S$라 하자. 그 경우 R의 유한 개 소 아이디얼만이 S에서 분기이다.

Proof. 만약 P가 R의 소 아이디얼이며 S에서 분기이면 $P \cap \mathbb{Z} = p\mathbb{Z}$는 S에서 분기이다. (e가 다중 확대에서 곱셈적임을 상기하라.) S에서 분기인 p가 유한 개뿐이며 p 상에 놓인 R의 소 아이디얼이 유한 개뿐이므로 S에서 분기인 P가 유한 개뿐이다. □

물론 P가 S에서 분기가 아니지만 p가 S에서 분기일 수도 있다. Exercise 19는 R의 소 아이디얼이 S에서 비분기임을 보이는 더 좋은 도구를 제공한다. 이것 외에도 S의 특정한 소 아이디얼 Q가 R 상에서 분기 (i.e. $P = Q \cap R$에 대하여 $e(Q|P) > 1$)인지를 결정하는 판정법이 존재한다. S의 (R에 대한) **차 아이디얼 (different ideal)**이라 불리는 S의 특수한 아이디얼이 존재하여 R 상에서 분기인 소 아이디얼 Q들을 정확히 인수로 가진다. 우리는 이 장의 마지막 부분의 연습문제들에서 차 아이디얼의 개념을 개발하고 분기 진술의 한쪽 방향을 증명할 것이다. 반대 방향은 Chapter 4에서 증명될 것이다.

이제 우리는 어떠한 소수 $p \in \mathbb{Z}$가 2차수체에서 분리되는 방식을 자세히 고려할 것이다. 제곱 없는 정수 m에 대하여 $R = \mathbb{A} \cap \mathbb{Q}[\sqrt{m}]$이라 하자. $m \equiv 2$ 또는 $3 \pmod 4$일 경우 R이 정수적 기저 $\{1, \sqrt{m}\}$와 판별식 $4m$을 가지며 $m \equiv 1 \pmod 4$일 경우 R이 정수적 기저 $\{1, (1 + \sqrt{m})/2\}$와 판별식 m을 가짐을 상기하라.

p가 $\mathbb{Z}$에서의 소수라 하자. Theorem 21은 3가지 가능성만 존재함을 보여준다:

$$pR = \begin{cases} P^2, & f(P|p) = 1 \\ P, & f(P|p) = 1 \\ P_1P_2, & f(P_1|p) = f(P_2|p) = 1 \end{cases}$$

Theorem 25. 위 표기법 하에서 다음이 성립한다:
만약 $p|m$이면,

$$pR = (p, \sqrt{m})^2 \tag{3.1}$$

만약 m이 홀수이면,

$$2R = \begin{cases} (2, 1+\sqrt{m})^2 & (m \equiv 3 \pmod 4) \quad (3.2) \\ \left(2, \frac{1+\sqrt{m}}{2}\right)\left(2, \frac{1-\sqrt{m}}{2}\right) & (m \equiv 1 \pmod 8) \quad (3.3) \\ \text{소 아이디얼} & (m \equiv 5 \pmod 8) \quad (3.4) \end{cases}$$

만약 p가 홀수이며 $p \nmid m$이면,

$$pR = \begin{cases} (p, n+\sqrt{m})(p, n-\sqrt{m}) & (m \equiv n^2 \pmod p) \quad (3.5) \\ \text{소 아이디얼} & (\forall n\ m \not\equiv n^2 \pmod p) \quad (3.6) \end{cases}$$

(3.3)과 (3.5)에서 인수들이 서로 다르다.

Proof. (3.1)에 대하여 $(p, \sqrt{m})^2 = (p^2, p\sqrt{m}, m)$이다. $p|m$이므로 이는 pR에 포함된다. 반면에 이는 p^2와 m의 최대공약수 p를 포함한다; 따라서 이는 pR을 포함한다.

(3.2), (3.3), (3.5)는 (3.1)과 유사하며 독자에게 남긴다. (3.3)과 (3.5)에서 인수들이 서로 다름은 이 경우 $p \nmid \operatorname{disc}(R)$이라는 사실에서 따라온다.

마지막으로 (3.4)와 (3.6)을 증명하자: 각각의 경우 만약 P가 p 상에 놓인 임의의 소 아이디얼이면 R/P가 $\mathbb{Z}_p$와 동형이 아님을 보이면 충분하다. (그 경우 $f(P|p) = 2$이기 때문이다.) 먼저 p가 홀수이며 $p \nmid m$이고 m이 $\bmod p$로 제곱수가 아니라 가정하고 다항식 $x^2 - m$을 고려하자. 이는 R에서 근을 가지며 따라서 R/P에서 근을 가진다. 그러나 가정에 의해 이것이 $\mathbb{Z}_p$에서 근을 갖지 않는다. 이는 R/P와 $\mathbb{Z}_p$가 동형일 수 없음을 보여주며 (우리가 관찰한 것과 같이) (3.6)을 함의한다.

다음 다항식을 사용하여 (3.4)도 마찬가지로 보일 수 있다.

$$x^2 - x + \frac{1-m}{4}$$

세부사항은 독자에게 남긴다. $1-m$이 4의 배수라 가정했으므로 이러한 다항식을 R/P와 $\mathbb{Z}_2$에서 고려할 수 있음을 기억해 두라. □

이러한 분리에 수반된 소 아이디얼들은 주 아이디얼처럼 보이지 않는다. 그러나 우리는 특정한 경우에 이들이 주 아이디얼이 되어야 함을 알고 있다: 예를 들어 $m = -1$ 또는 $m = -3$일 경우. (Chapter 1, exercise 7, 14) 독자는 이러한 두 경우에 여러 소 아이디얼들의 주 생성자를 기술할 수 있는가?

Theorem 25를 주어진 소수 p에 적용하기 위해서는 어떠한 경우에 m이 제곱수 $\bmod p$가 아닌지를 결정할 수 있어야 한다. 이는 물론 Gauss의 2차상호법칙에 의해 수행될 수 있다. 우리는 Chapter 4에서 2차수체에서 소수가 분리되는 방법과 원분체에서 소수가 분리되는 방법을 비교하는 것으로 이를 수립할 것이다. 이제 후자의 문제로 넘어가자.

$\omega = e^{2\pi i/m}$이라 하고 소수 $p \in \mathbb{Z}$를 고정하자. $\mathbb{Q}[\omega]$가 $\mathbb{Q}$의 정규 확대이므로 Theorem 23의 따름정리에 의해 다음이 성립한다.

$$pR = (Q_1 Q_2 \cdots Q_r)^e$$

여기에서 Q_i들은 $\mathbb{Z}[\omega]$의 서로 다른 소 아이디얼들이며 p 상에서 모두 동일한 관성차수 f를 가진다. 이에 더해 $ref = \varphi(m)$이다.

Theorem 26. $m = p^k n, p \nmid n$ 형태로 표현하자. 그 경우 (위 표기법 하에서) $e \equiv \varphi(p^k)$이며 f는 p의 $\bmod n$에서의 (곱셈적) 위수이다. (i.e. $p^f \equiv 1 \pmod n$이며 f가 이러한 성질을 가지는 최소 양의 정수이다.)

Proof. $\alpha = \omega^n, \beta = \omega^{p^k}$로 설정하자. 그 경우 α, β는 각각 1의 p^k승근 및 n승근이다. p가 체 $\mathbb{Q}[\alpha]$와 $\mathbb{Q}[\beta]$에서 어떻게 분리되는지를 고려하자; $\mathbb{Q}[\omega]$에 대한 결과가 간단히 따라올 것이다.

$p \nmid m$일 경우 $k = 0, n = m$이며 따라서 $\alpha = 1, \beta = \omega$이다.

$p|m$이라 가정하고 p가 p^k번째 원분체 $\mathbb{Q}[\alpha]$에서 어떻게 분리되는지를 고려하자. 우리는 다음이 성립함을 알고 있다.

$$p = u(1-\alpha)^{\varphi(p^k)}$$

여기에서 u는 $\mathbb{Z}[\alpha]$에서의 가역원이다. (Chapter 2, exercise 34(b)) 앞에서 언급한 것과 같이 이는 $p\mathbb{Z}[\alpha]$가 주 아이디얼 $(1-\alpha)$의 $\varphi(p^k)$승멱임을 함의한다. $\varphi(p^k) = [\mathbb{Q}[\alpha] : \mathbb{Q}]$이므로 Theorem 21은 이것이 $p\mathbb{Z}[\alpha]$의 소 아이디얼 분해여야 함을 보여준다.

이제 n번째 원분체 $\mathbb{Q}[\beta]$에서 무엇이 일어나는지를 고려하자. $p \nmid n$이며 $\mathrm{disc}(\mathbb{Z}[\beta])$가 $n^{\varphi(n)}$의 인수이므로 (Chapter 2에서 Theorem 8 이후에 보였음) p가 비분기이다. 그러므로 다음이 성립한다.

$$p\mathbb{Z}[\beta] = P_1 P_2 \cdots P_r$$

여기에서 P_i들은 $\mathbb{Z}[\beta]$의 서로 다른 소 아이디얼들이며 p 상에서 각각 동일한 관성차수 f를 가지고 $rf = \varphi(n)$을 만족시킨다. (이러한 r과 f는 p의 $\mathbb{Q}[\omega]$에서의 분리에 대한 r과 f임이 밝혀질 것이지만, 우리는 아직 이를 모른다.) f가 $\bmod n$에서 p의 위수임을 주장하겠다.

이를 보이기 위해 먼저 $\mathbb{Q}[\beta]$의 $\mathbb{Q}$ 상에서의 Galois 군이 $\bmod n$ 정수 곱셈군 $\mathbb{Z}_n^*$와 동형임을 상기하라; $\mathbb{Q}[\beta]$의 자기동형사상 σ가 합동류 $\bar{a} \in \mathbb{Z}_n^*$ ($a \in \mathbb{Z}$)에 대응할 필요충분조건은 $\sigma(\beta) = \beta^a$인 것이다. 특히 σ가 $\bar{p}$에 대응하는 자기동형사상을 나타낸다 하자. $\langle\sigma\rangle$가 σ에 의해 생성된 부분군을 나타낸다 하자; 그러므로 $\langle\sigma\rangle$는 σ의 멱들로 구성된다. 군 $\langle\sigma\rangle$의 위수는 원소 σ의 위수와 동일하며 이는 $\bmod n$에서 p의 위수와 같다. 따라서 우리는 $\langle\sigma\rangle$가 위수 f를 가짐을 보여야 한다.

임의의 $P = P_i$를 고정하면 $f = f(P|p)$의 정의에 의해 체 $\mathbb{Z}[\beta]/P$가 $\mathbb{Z}_p$ 상에서 차수 f를 가짐을 상기하라. 결과적으로 $\mathbb{Z}[\beta]/P$의 $\mathbb{Z}_p$ 상에서의 Galois 군은 위수 f의 순환군이며 모든 원소를 자신의 p승멱으로 대응시키는 자기동형사상 τ에 의해 생성된다. (Appendix C를 참조하라.)

우리가 원하는 것을 증명하기 위해서는 모든 $a \in \mathbb{Z}$에 대하여 $\sigma^a = 1$ iff $\tau^a = 1$임을 보이면 충분하다. 이는 순환군 $\langle\sigma\rangle$와 $\langle\tau\rangle$가 동일한 위수를 가짐을 보여줄 것이다.

명백히 $\sigma^a = 1$ iff $\beta^{p^a} = \beta$ iff $p^a \equiv 1 \pmod n$이다. 반면에 $\tau^a = 1$ iff $\beta^{p^a} \equiv \beta \pmod P$임을 간단히 보일 수 있다. 그러므로 $\beta^{p^a} \equiv \beta \pmod P$인 경우 $p^a \equiv 1 \pmod 1$임을 보여야 한다. $p^a \equiv b \pmod n, 1 \le b \le n$으로 표기하자. $\beta^{p^a} = \beta^b$이며 따라서 $\beta^b \equiv \beta \pmod P$이다. β가 $\mathbb{Z}[\beta]$에서의 가역원이므로 이는 $\beta^{b-1} \equiv 1 \pmod P$임을 함의한다. 이제 다음 공식을 상기하라.

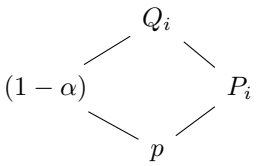
$$(1-\beta)(1-\beta^2)\cdots(1-\beta^{n-1}) = n$$

(Chapter 1, exercise 16을 참조하라.) 이는 만약 $b > 1$이면 $n \in P$임을 보여준다; 그러나 $p \in P$이며 $(n, p) = 1$이므로 이는 불가능하다. 따라서 $b = 1$이다.

이는 p 상에 놓인 $\mathbb{Z}[\beta]$에서의 각각의 소 아이디얼 P에 대하여 $f(P|p)$가 $\bmod n$에서 p의 위수라는 사실의 증명을 완료한다.

마지막으로 $\mathbb{Z}[\alpha]$과 $\mathbb{Z}[\beta]$에 대한 결과를 합치자. 각각 $P_1, \ldots, P_r$ 상에 놓인 $\mathbb{Z}[\omega]$의 소 아이디얼 $Q_1, \ldots, Q_r$을 고정하자. (Theorem 20은 Q_i들이 존재함을 보여준다.) 모든 Q_i들은 $p \in \mathbb{Z}$ 상에 놓여 있으며 따라서 ($(1-\alpha)$가 p 상에 놓여 있는 $\mathbb{Z}[\alpha]$의 유일한 소 아이디얼임을 보였으므로) 모든 Q_i들이 $\mathbb{Z}[\alpha]$에서의 $(1-\alpha)$ 상에 놓여 있어야 한다. 우측의 도표를 고려하면 다음을 얻는다.

$$e(Q_i|p) \ge e((1-\alpha)|p) = \varphi(p^k)$$
$$f(Q_i|p) \ge f(P_i|p) = f$$



이에 더해 Theorem 21에 의해 $rf = \varphi(n)$이므로 $\varphi(p^k)rf = \varphi(m)$이다. 그 경우 Theorem 21을 p의 $\mathbb{Z}[\omega]$에서의 분리에 적용하면 Q_i들만이 p 상에 놓인 $\mathbb{Z}[\omega]$의 소 아이디얼이며 위 부등식에서 등호가 성립해야 함을 보여준다. 이는 증명을 완료한다. □

Theorem 26을 $p \nmid m$인 특수한 경우에 대하여 재진술하자:

Corollary. 만약 $p \nmid m$이면 p는 $\varphi(m)/f$개의 서로 다른 $\mathbb{Z}[\omega]$의 소 아이디얼로 분리된다. (여기에서 f는 $\bmod m$에서 p의 위수이다.)

우리는 아직 주어진 소수가 주어진 수환에서 어떻게 분리되는지를 결정하는 일반적인 과정을 제시하지 않았다. 이러한 과정은 존재하며 거의 항상 적용 가능하다. 이는 특히 Theorem 22와 23 사이에서 3차수체에서의 소 아이디얼 분해를 어떻게 찾았는지를 설명해 준다.

R, S, K, L이 통상적인 경우와 같으며 $n = [L : K]$라 하자. K 상에서의 차수 n의 원소 $\alpha \in S$를 고정하자. 그 경우 $L = K[\alpha]$이다. 일반적으로 $R[\alpha]$는 S의 (덧셈) 부분군이며 진부분군일 수도 있다. 그러나 몫군 $S/R[\alpha]$는 유한군이어야 한다. (이를 보이는 한 가지 방법은 $m = [K : \mathbb{Q}]$라 할 경우 S와 $R[\alpha]$가 모두 계수 mn의 자유가환군임을 관찰하는 것이다; 다른 방법은 $S/R[\alpha]$가 유한생성 비틀림 군임을 보이는 것이다.)

우리는 R의 유한 개를 제외한 모든 소 아이디얼 P에 대하여 P의 S에서의 분리가 특정 다항식 $\bmod P$의 분해에 의해 결정될 수 있음을 보일 것이다. 구체적으로 이는 P가 $S/R[\alpha]$의 위수의 인수가 아닌 소수 $p \in \mathbb{Z}$ 상에 놓여 있는 경우에 성립할 것이다; 그러므로 만약 $S = R[\alpha]$이면 이는 모든 P에 대하여 성립한다.

R의 소 아이디얼 P를 고정하고 다음과 같은 표기법을 도입하자: 다항식 $h \in R[x]$에 대하여 $\bar{h}$가 h의 계수들을 $\bmod P$로 축약하여 얻어진 $(R/P)[x]$에서의 대응하는 다항식을 나타낸다 하자.

이제 g가 α의 K 상에서의 기약 1계수다항식이라 하자. g의 계수들은 (대수적 정수 α의 공액들에 의해 표현될 수 있으므로) 대수적 정수이며 따라서 이들은 $\mathbb{A} \cap K = R$에 속한다. 그러므로 $g \in R[x]$이며 $\bar{g} \in (R/P)[x]$를 고려할 수 있다. $\bar{g}$는 $(R/P)[x]$에서 1계수 기약 인수들로 유일하게 분해된다. 우리는 이러한 분해를 다음 형태로 표기할 수 있다.

$$\bar{g} = \bar{g}_1^{e_1} \bar{g}_2^{e_2} \cdots \bar{g}_r^{e_r}$$

여기에서 g_i들은 R 상에서의 1계수다항식들이다. $\bar{g}_i$들이 서로 다르다 가정되었다.

Theorem 27. 모든 것이 위와 같다 하고, P 하에 놓여 있는 $\mathbb{Z}$의 소수 p가 $|S/R[\alpha]|$의 인수가 아니라 가정하자. 그 경우 PS의 소 아이디얼 분해는 다음에 의해 주어진다.

$$Q_1^{e_1} Q_2^{e_2} \cdots Q_r^{e_r}$$

여기에서 Q_i는 P와 $g_i(\alpha)$에 의해 생성된 S에서의 아이디얼 $(P, g_i(\alpha))$이다; 다른 말로 하면,

$$Q_i = PS + (g_i(\alpha))$$

또한 $f(Q_i|P)$는 g_i의 차수와 같다.

Proof. f_i가 g_i의 차수를 나타낸다 하자. 이는 $\bar{g}_i$의 차수와 같다. 다음을 증명하자.

(1) 각각의 i에 대하여 $Q_i = S$ 또는 S/Q_i가 위수 $|R/P|^{f_i}$의 체이다.
(2) $i \neq j$이면 $Q_i + Q_j = S$이다.
(3) $PS | Q_1^{e_1} Q_2^{e_2} \cdot Q_r^{e_r}$

잠시 이들이 성립한다 가정하고 여기에서 결과가 어떻게 따라오는지를 보이겠다: 필요하다면 Q_i들을 재정렬하는 것으로 $Q_1, \ldots, Q_s \neq S$이며 $Q_{s+1} = \cdots = Q_r = S$라 가정할 수 있다. ($r = s$임이 밝혀질 것이다.) 우리는 항상 $Q_1, \ldots, Q_s$가 S의 소 아이디얼임을 알 수 있으며 이들은 P를 포함하므로 명백히 P 상에 놓여 있다. 이는 또한 $i \leq s$에 대하여 $f(Q_i|P) = f_i$임을 보여준다. (2)는 $Q_1, \ldots, Q_s$가 서로 다름을 보여주며 ($Q_{s+1} = \cdots = Q_r = S$이므로) (3)은 $PS | Q_1^{e_1} Q_2^{e_2} \cdot Q_s^{e_s}$가 된다. PS의 소 아이디얼 분해가 $Q_1^{d_1} Q_2^{d_2} \cdots Q_s^{d_s}$이며 $i = 1, \ldots, s$에 대하여 $d_i \leq e_i$임이 따라온다. Theorem 21을 적용하면 $n = d_1 f_1 + \cdots + d_s f_s$를 얻는다. 반면에 n이 g의 차수이며 이는 $e_1 f_1 + \cdots + e_r f_r$이다. 그러므로 $r = s$이며 모든 i에 대하여 $d_i = e_i$임이 따라온다.

(1), (2), (3)을 보이는 것이 남아있다.

Proof of (1). 요구된 위수의 체를 찾아보면 다음이 이러한 체임을 알 수 있다. (Appendix A를 참조하라.)

$$F_i = (R/P)[x]/(\bar{g}_i)$$

F_i와 S/Q_i 간의 연결을 수립하기 위하여 $R[x]$에서 이들 각각으로의 준동형사상이 존재함을 관찰하자:

$R[x] \to F_i$는 계수들을 $\bmod P$로 축약시킨 후 $\bmod (\bar{g}_i)$로 축약시키는 자명한 방법으로 정의된다. 이는 명백히 전사이며 그 $R[x]$에서의 핵이 P와 g_i에 의해 생성됨을 어렵지 않게 보일 수 있다: $(P, g_i) = P[x] + (g_i)$. (exercise 25를 참조하라.) 그러므로 다음의 동형사상이 존쟿나다.

$$R[x]/(P, g_i) \to F_i$$

이제 x에 α를 대입하는 것으로 $R[x]$를 S로 대응시키자; 이는 환 준동형사상 $R[x] \to S/Q_i$를 유도한다. (P, g_i)가 그 핵에 포함됨을 간단히 보일 수 있다. 위 동형사상은 (P, g_i)가 극대 아이디얼임을 보여주며 따라서 핵은 (P, g_i) 또는 $R[x]$ 전체이다. 이에 더해 $R[x]$는 S/Q_i로 전사 대응된다: 이를 보이기 위해서는 $S = R[\alpha] + Q_i$임을 보여야 한다. 우리는 $p \in P \subset Q_i$임을 알고 있으며 따라서 $pS \subset Q_i$이다. $S = R[\alpha] + pS$임을 주장하겠다; 이는 $p \nmid |S/R[\alpha]|$라는 가정에서 따라온다. ($R[\alpha] + pS$의 S에서의 지표는 $|S/R[\alpha]|$와 $|S/pS|$의 공약수이지만 $|S/pS|$는 p의 멱이므로 이들이 서로 소이다.) 그러므로 $R[x] \to S/Q_i$가 전사이다. 핵의 두 가능성을 고려하면 $Q_i = S$이거나 또는 S/Q_i가 F_i와 동형인 $R[x]/(P, g_i)$와 동형이라 결론지을 수 있다.

Proof of (2). $\bar{g}_i$들이 주 아이디얼 정역 $(R/P)[x]$에서의 서로 다른 기약다항식들임을 상기하라; 따라서 $i \neq j$가 주어진 경우 R 상에서의 다항식 h, k가 존재하여 다음을 만족시킨다.

$$\bar{g}_i \bar{h} + \bar{g}_j \bar{k} = 1$$

이는 다음을 함의한다.

$$g_i h + g_j k \equiv 1 \qquad (\mathrm{mod}\, P[x])$$

x를 α로 대체하면 다음의 합동 관계를 얻는다.

$$g_i(\alpha)h(\alpha) + g_j(\alpha)k(\alpha) \equiv 1 \qquad (\mathrm{mod}\, PS)$$

(이것이 전부 타당함을 스스로에게 납득시켜라.) $1 \in (P, g_i(\alpha), g_j(\alpha)) = Q_i + Q_j$임이 따라오며 이는 (2)를 증명한다.

Proof of (3). 표기법을 간략화하기 위해 $\gamma_i = g_i(\alpha)$라 하자. 그 경우 $Q_i = (P, \gamma_i)$이다. 곱 $Q_1^{e_1} \cdots Q_r^{e_r}$이 다음 아이디얼에 포함됨을 (따라서 이를 인수로 가짐을) 간단히 보일 수 있다.

$$(P, \gamma_1^{e_1}\gamma_2^{e_2} \cdots \gamma_r^{e_r})$$

이 아이디얼은 PS이다. 이를 보이기 위해 우리는 곱 $\gamma_1^{e_1} \cdots \gamma_r^{e_r}$이 PS에 속함을 보여야 한다. 우리는 다음을 알고 있다.

$$\bar{g}_1^{e_1}\bar{g}_2^{e_2} \cdots \bar{g}_r^{e_r} = \bar{g}$$

따라서 다음이 성립한다.

$$g_1^{e_1} g_2^{e_2} \cdots g_r^{e_r} \equiv g \qquad (\mathrm{mod}\, P[x])$$

(2)에서와 마찬가지로 이는 다음을 함의한다.

$$\gamma_1^{e_1}\gamma_2^{e_2} \cdots \gamma_r^{e_r} \equiv g(\alpha) = 0 \qquad (\mathrm{mod}\, PS)$$

이는 증명을 완료한다. □

특히 $L = \mathbb{Q}[\alpha]$이며 $p^2 \nmid \mathrm{disc}(\alpha)$인 경우 p에 대한 조건이 만족됨을 일러두겠다. 이는 $|S/R[\alpha]|^2$가 $|S/\mathbb{Z}[\alpha]|^2$(이 경우 유한하다)의 인수이며 후자의 수가 $\mathrm{disc}(\alpha)$의 인수이기 때문이다. (Chapter 2, exercise 27(c)를 참조하라.)

Theorem 27의 응용을 제시하겠다. $\alpha = \sqrt{m}$으로 선택하면 $p = 2, m \equiv 1 \pmod 4$인 경우를 제외한 Theorem 25의 결과들을 다시 얻을 수 있다; 이러한 예외적인 경우 $\alpha = (1 + \sqrt{m})/2$로 선택하면 결과를 얻을 수 있다. 다른 예시로, $\mathbb{Z}[\alpha]$에서 다항식 $x^3 - x - 1 \bmod p$를 분해하는 것으로 임의의 소수가 어떻게 분리되는지를 결정할 수 있다. 추가적인 예시들은 exercise 26, 27에 제시되어 있다. Theorem 27의 몇 가지 흥미로운 응용을 위해서는 exercise 29, 30을 참조하라.

Exercises (연습문제)

1.

4 | Galois Theory Applied to Prime Decomposition (소 아이디얼 분해에 대한 Galois 이론의 적용)

지금까지 우리의 이론에서 수체의 Galois 이론적 측면은 부각되지 않았다. 본질적으로 우리가 수행한 것은 m번째 원분체의 Galois 군을 결정하고 (이는 정수 $\bmod m$ 곱셈군이었다) 정규 확대의 경우에 Galois 군이 주어진 소 아이디얼 상에 놓인 소 아이디얼들을 치환함을 보인 것뿐이다. (Theorem 23) Galois 이론은 원분체에서의 분리에 관한 Theorem 26의 증명에서도 등장한다. 이 장에서 우리는 수환의 소 아이디얼이 확대체에서 어떻게 분리되는지를 결정하는 일반적인 문제에 Galois 이론을 적용할 것이다.

K와 L이 수체이며 L이 K의 정규 확대라 하자. 그러므로 K를 점별 고정하는 L의 모든 자기동형사상들로 구성된 Galois 군 G는 위수 $n = [L : K]$를 가진다. 통상적인 경우와 같이 R, S가 대응하는 수환을 나타낸다 하자. R의 소 아이디얼 P를 고정하고 P 상에 놓인 S의 모든 소 아이디얼 Q들이 동일한 분기지표 e와 관성차수 f를 가짐을 상기하라. (Theorem 23의 따름정리) 그러므로 만약 이러한 소 아이디얼이 r개 존재한다면 $ref = n$이다. (Theorem 21) P 상에 놓인 각각의 소 아이디얼 Q에 대하여 G의 2가지 부분군을 정의할 것이다:

분해군(decomposition group):

$$D = D(Q|P) = \{\sigma \in G : \sigma Q = Q\}]$$

관성군(inertia group):

$$E = E(Q|P) = \{\sigma \in G : \sigma(\alpha) \equiv \alpha \pmod{Q}\ \forall \alpha \in S\}$$

이들이 실제로 G의 부분군이며 $E \subset D$임은 명백하다. (조건 $\sigma Q = Q$는 $\sigma(\alpha) \equiv 0 \bmod Q$ iff $\alpha \equiv 0 \pmod{Q}$로 표현될 수 있다; 명백히 E에 대한 조건이 이것을 함의한다.)

D의 구성원들은 체 S/Q에 자연스러운 방식으로 자기동형사상을 유도한다: 모든 $\sigma \in G$는 S의 자기동형사상으로 제한되며, 만약 $\sigma \in D$이면 유도된 준동형사상 $S \to S/Q$의 핵이 Q이다; 그러므로 각각의 $\sigma \in D$는 다음의 가환 도표를 만족시키는 S/Q의 자기동형사상 $\bar{\sigma}$를 유도한다:

$$\begin{array}{ccc} S & \xrightarrow{\sigma} & S \\ \downarrow & & \downarrow \\ S/Q & \xrightarrow{\bar{\sigma}} & S/Q \end{array}$$

이에 더해 σ가 K를 고정하며 따라서 R을 점별 고정하므로 $\bar{\sigma}$가 부분체 R/P를 점별 고정함이 명백하다. 그러므로 $\bar{\sigma}$는 S/Q의 R/P 상에서의 Galois 군 $\bar{G}$의 구성원이다. 이러한 논의는 함수 $D \to \bar{G}$가 존재한다고 말하는 것으로 종합될 수 있다. 이것이 군 준동형사상임을 간단히 보일 수 있다: D에서의 자기동형사상의 합성은 $\bar{G}$에서의 합성에 대응한다. 준동형사상 $D \to \bar{G}$의 핵이 E임을 간단히 보일 수 있다; 이는 E가 D의 정규 부분군이며 몫군 D/E가 $\bar{G}$에 매장됨을 보여준다. 우리는 $D \to \bar{G}$가 사실 전사임을 보일 것이며 따라서 $D/E \to \bar{G}$가 동형사상이다. 우리는 $\bar{G}$의 구조를 알고 있다: 이는 위수 f의 순환군이며 (Appendix C를 참조하라) 따라서 D/E도 그러하다.

이제 D와 E의 고정체를 살펴보자; 이들을 각각 L_D, L_E로 표기하자. L_D는 **분해체(decomposition field)**이며 L_E는 **관성체(inertia field)**이다. 일반적으로 우리는 다음의 표기법을 채택한다: G의 임의의 부분군 H에 대하여 L_H는 H의 고정체를 나타낸다; 그러므로 $L_{\{1\}} = L, L_G = K$이다. 더 일반적으로, 임의의 부분집합 $X \subset L$에 대하여 X_H가 $X \cap L_H$를 나타낸다 하자. 그러므로 S_H는 L_H에서의 수환이며 Q_H는 Q 하에 놓인 S_H의 유일한 소 아이디얼이다. 명백히 Q_H는 P 상에 놓여 있으며 정의로부터 S_H/Q_H가 S/Q와 R/P 사이의 중간체임을 간단히 보일 수 있다. (이것들을 전부 검증하라.)

이제 우리는 주요 결과를 기술할 수 있다:

Theorem 28. $K, L, R, S, P, Q, G, D, E, r, e, f$가 위에서와 같다 하자. 그 경우 다음이 성립한다:

차수		분기지표	관성차수
e	$\begin{matrix} L & Q \\ \vert & \vert \\ L_E & Q_E \end{matrix}$	e	1
f	$\begin{matrix} \vert & \vert \\ L_D & Q_D \end{matrix}$	1	f
r	$\begin{matrix} \vert & \vert \\ K & P \end{matrix}$	1	1

Proof. $[L_D : K] = r$임을 보이는 것으로 시작하자. Galois 이론에 의해 우리는 $[L_D : K]$가 D의 G에서의 지표와 같음을 알고 있다. 각각의 좌 잉여류 σD ($\sigma \in G$)는 Q를 σQ로 대응시킨다. (i.e. 잉여류의 각각의 구성원이 Q를 σQ로 대응시킨다.) 명백히 $\sigma D = \tau D$ iff $\sigma Q = \tau Q$이다. 이는 좌 잉여류 σD들과 소 아이디얼 σQ들 간에 1-1 대응을 수립한다; Theorem 23에서 보인 것과 같이 이러한 소 아이디얼들은 P 상에 놓인 S의 소 아이디얼 전부이며 따라서 이들은 r개 존재한다. 이는 주장을 증명한다.

다음으로 $e(Q_D|P)$와 $f(Q_D|P)$가 모두 1임을 보이자. 먼저 Q가 Q_D 상에 놓인 S의 유일한 소 아이디얼임을 주목하라: 이러한 소 아이디얼은 반드시 L_D 상에서의 L의 Galois 군에 의해 추이적으로 치환되어야 하며 (L은 자동적으로 L_D의 정규 확대이다) 이 Galois 군이 D이고 D가 Q를 Q로만 대응시키므로 Q가 Q_D 상에 놓인 유일한 소 아이디얼이다. Theorem 21로부터 다음이 따라온다.

$$[L : L_D] = e(Q|Q_D)f(Q|Q_D)$$

$[L_D : K] = r$임을 보였으며 $ref = n$이므로 좌변의 수는 ef이다. 이에 더해 우변의 인자들은 각각 e와 f를 초과할 수 없다; 결과적으로 두 경우 모두 등호가 성립해야 하며 따라서 다음이 성립해야 한다.

$$e(Q_D|P) = f(Q_D|P) = 1$$

다음으로 $f(Q|Q_E) = 1$임을 보이자. 이는 S/Q가 S_E/Q_E의 자명 확대임과 동치이다. S/Q의 S_E/Q_E 상에서의 Galois 군이 자명군임을 보이면 충분하다. (Appendix C를 참조하라.) 이를 위해 우리는 각각의 $\theta \in S/Q$에 대하여 어떠한 $m \geq 1$이 존재하여 $(x-\theta)^m$이 S_E/Q_E에 속한 계수를 가짐을 보일 것이다; 그 경우 Galois 군의 모든 구성원이 θ를 $(x-\theta)^m$의 근으로 대응시키며 이는 θ밖에 없다. 따라서 이는 요구된 것을 증명한다.

$\theta \in S/Q$에 대응하는 $\alpha \in S$를 고정하자; 명백히 다음 다항식은 S_E-계수이다.

$$g(x) = \prod_{\sigma \in E} (x - \sigma\alpha)$$

계수들을 $\bmod Q$로 축약하는 것으로 $\bar{g} \in (S/Q)[x]$를 얻으며 이는 사실 S_E/Q_E-계수이다. 그러나 모든 $\sigma(\alpha)$는 $\theta \bmod Q$로 축약되므로 (왜 그런가?) $\bar{g}(x) = (x-\theta)^m$이다. (여기에서 $m = |E|$이다.) 이는 $f(Q|Q_E) = 1$임의 증명을 완료한다.

$f(Q_D|P) = 1$이라는 사실과 조합하면 이는 $f(Q_E|Q_D) = f(Q|P) = f$임을 보여준다. 그 경우 Theorem 21에 의해 $[L_E : L_D] \geq f$여야 한다. 그러나 우리는 (정리 앞의 언급에서) E가 D의 정규 부분군이며 몫군이 위수 f의 군 $\bar{G}$에 매장됨을 보였다. 그러므로 $[L_E : L_D] = |D/E| \leq f$이고 따라서 정확히 f이다. 다시 Theorem 21에 의해 $e(Q_E|Q_D) = 1$이다. 마지막으로 이미 수립된 차수와 분기지표들을 고려하면 $[L : L_E] = e$이며 $e(Q|Q_e) = e$임을 간단히 알아낼 수 있다. □

Corollary 1. 자연스러운 대응 $\sigma \mapsto \bar{\sigma}$ 하에서 D가 $\bar{G}$로 전사 대응된다; 그 핵은 E이고 따라서 D/E가 위수 f의 순환군이다.

Proof. 우리는 이미 D/E가 $\bar{G}$에 매장됨을 보였다. 이에 더해 $|D/E| = [L_E : L_D]$이므로 두 군이 모두 위수 f를 가진다. □

다음의 특수한 경우는 '분해체'와 '관성체'라는 용어를 채택한 이유를 보여준다.

Corollary 2. D가 G의 정규 부분군이라 하자. 그 경우 P는 L_D에서의 r개 서로 다른 소 아이디얼들로 분리된다. 만약 E도 G에서 정규이면 이들은 모두 L_E에서도 소 아이디얼로 남아있는다. (즉 이는 L_E에서 불변(inert)한다.) 마지막으로 이들 각각은 L에서 e중멱이 된다.

Proof. 만약 D가 G에서 정규이면 Galois 이론에 의해 L_D가 K의 정규 확대이다. 우리는 Q_D가 P 상에서 분기지표와 관성차수 1임을 알고 있으며 따라서 P 상에 놓인 L_D의 임의의 소 아이디얼 P'도 그러하다. (Theorem 23의 따름정리) 그 경우 이러한 소 아이디얼이 정확히 r개 존재해야 한다. (Theorem 21) L과 L_D에서 P 상에 놓인 소 아이디얼이 정확히 r개 존재하므로 L_E에서도 정확히 r개 존재한다. 이는 각각의 P'이 L_E에서의 유일한 P'' 하에 놓임을 함의한다; 그러나 P''이 P' 상에서 분기일 수도 있다. 만약 E가 G에서 정규이면 (따라서 L_E가 K 상에서 정규이면) $e(P''|P) = e(Q_E|P) = 1$이며 따라서 $e(P''|P) = 1$이다. 이는 P'이 L_E에서 불변임을 증명한다: $P'' = P'S_E$이다. 마지막으로 P''이 L에서 e중멱이 됨을 보이는 것은 독자에게 남기겠다. □

우리는 이미 이 현상의 예시를 관찰했다: $\mathbb{Z}$에서의 소수 2는 $\mathbb{Q}[\sqrt{-23}]$에서의 서로 다른 2개 소 아이디얼로 분리되며 이들은 $\mathbb{Q}[\omega], \omega = e^{2\pi i/23}$에서도 소 아이디얼로 남는다. (Chapter 3, exercise 17) 이는 Corollary 2에 의해 예측될 수 있다. Theorem 26은 2가 $\mathbb{Q}[\omega]$에서 2개 소 아이디얼로 분리됨을 보여주며 따라서 분해체가 $\mathbb{Q}$ 상에서 차수 2이다; 이에 더해 Galois 군이 위수 22의 순환군이므로 $\mathbb{Q}[\omega]$의 2차 부분체가 유일하게 존재한다. 그러므로 분해체는 $\mathbb{Q}[\sqrt{-23}]$이어야 한다. 마지막으로 2가 $\mathbb{Q}[\omega]$에서 비분기이므로 관성체는 $\mathbb{Q}[\omega]$ 전체이다.

약간 더 일반적으로, L이 K 상에서 정규이며 Galois 군이 순환군이고 P(K에서의 소 아이디얼)가 L에서의 r개 소 아이디얼로 분리된다면 분해체는 K 상에서 차수 r인 유일한 중간체이며 P는 분해체를 포함하는 임의의 중간체에서 r개 소 아이디얼들로 분리된다.

다른 예시로 체 $L = \mathbb{Q}[i, \sqrt{2}, \sqrt{5}]$를 고려하자; 이는 $\mathbb{Q}$의 차수 8의 정규 확대이며 Galois 군은 위수 2의 순환군 3개의 직접합이다. 소수 2는 $\mathbb{Q}[i]$의 2개 소 아이디얼들로 분리되며 $\mathbb{Q}[\sqrt{2}]$에서 불변이고 $\mathbb{Q}[\sqrt{5}]$에서 제곱이 된다. 그러므로 L은 5 상에 놓인 소 아이디얼을 2개 이상 가져야 하고 이들 각각은 분기지표와 관성차수가 2 이상이어야 한다; 이러한 수들이 모두 정확히 2임이 따라온다. 관성체는 $\mathbb{Q}$ 상에서 차수 4인 체여야 하며 이곳에서 5가 비분기여야 한다. 유일한 가능성은 $\mathbb{Q}[i, \sqrt{2}]$이다. 그러므로 $(2+i)$와 $(2-i)$는 $\mathbb{Q}[i, \sqrt{2}]$에서도 여전히 소 아이디얼이며 L의 소 아이디얼의 제곱이다.

비가환 예시를 소개하겠다: $\omega = e^{2\pi i/3}$에 대하여 $L = \mathbb{Q}[\sqrt[3]{19}, \omega]$라 하자. 그 경우 L은 $\mathbb{Q}$의 6차 정규 확대이며 Galois 군 S_3를 가진다. (3개 대상의 치환군) 소수 3의 분리를 고려하자: 이는 $\mathbb{Q}[\omega]$에서 제곱이며 $\mathbb{Q}[\sqrt[3]{19}]$에서 P^2Q 형태이다. (Chapter 3, exercise 26) 결과적으로 L은 3 상에 놓인 소 아이디얼을 2개 이상 가져야 하며 따라서 분기지표가 2의 배수여야 한다. 유일한 가능성은 L이 3 상에서 3개 소 아이디얼을 가지며 각각 $e = 2, f = 1$인 것이다. 이러한 각각의 소 아이디얼에 대하여 분해체는 $\mathbb{Q}$ 상에서 3차이다. 3차 체가 3개 존재한다: $\mathbb{Q}[\sqrt[3]{19}], \mathbb{Q}[\omega\sqrt[3]{19}], \mathbb{Q}[\omega^2\sqrt[3]{19}]$. 3 상에서의 소 아이디얼 중 어떤 것을 고려하는지에 따라 이들이 모두 분해체가 될 수 있다. (이들이 모두 등장한다는 사실은 이들 각각이 L의 자기동형사상에 의해 이들 중 다른 것으로 대응될 수 있다는 사실에서 간단히 따라온다.) $f = 1$이므로 관성체도 동일하다. 3이 어떠한 가능한 분해체에서도 3개의 서로 다른 소 아이디얼들로 분리되지 않음을 기억해 두라; 이는 사실 (하나의 분해체에서 P^2Q로 분해되며 분해체들이 모두 $\mathbb{Q}$의 동형 확대이므로) 각각의 분해체에서 분기이다. 이는 D에서의 정규성 조건이 Corollary 2에서 필수적임을 보여준다.

이제 우리는 변형된 상황을 고려할 것이다. K가 L의 더 큰 부분체 K'으로 대체된다면 무엇이 일어나겠는가? 우리는 K'이 어떠한 부분군 $H \subset G$의 고정체임을 알고 있다; 위 표기법을 따르면 $K' = L_H$이다. 이에 더해 환 $R' = \mathbb{A} \cap K'$은 S_H이며 $P' = Q \cap R'$은 Q 하에 놓인 R'의 유일한 소 아이디얼이다. P'은 또한 P 상에 놓이지만 이것이 P 상에 놓인 유일한 소 아이디얼일 필요는 없다. 우리는 L이 K'의 정규 확대임을 알고 있으며 따라서 분해군 $D(Q|P')$과 관성군 $E(Q|P')$을 고려할 수 있다. 정의에 의해 다음이 즉시 따라온다.

$$D(Q|P') = D \cap H$$
$$E(Q|P') = E \cap H$$

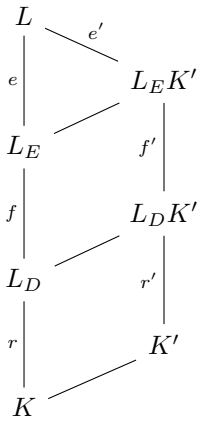
여기에서 D와 E는 (P 상에 놓인 Q에 대한) 앞에서와 같은 군이다. 그 경우 Galois 이론에 의해 체 L_DK'과 L_EK'이 각각 Q의 P' 상에서의 분해체와 관성체이다. 우리는 이러한 관찰을 통해 분해체와 관성체에 대한 어떠한 극대 및 극소 조건들을 수립할 것이다.

Theorem 29. 위 표기법 하에서 다음이 성립한다.

(1) L_D는 $e(P'|P) = f(P'|P) = 1$을 만족시키는 중간체 K' 중 최대인 것이다.
(2) L_D는 Q가 P' 상에 놓인 S의 유일한 소 아이디얼이도록 하는 K' 중 최소인 것이다.
(3) L_E는 $e(P'|P) = 1$이도록 하는 K' 중 최대인 것이다.
(4) L_E는 Q가 P' 상에서 완전분기(i.e. $e(Q|P') = [L : K']$)이도록 하는 K' 중 최소인 것이다.

Proof. 먼저 우리가 이미 L_D와 L_E가 이러한 성질들을 가짐을 보였음을 인지하라: 예를 들어 우리는 Theorem 28의 증명에서 Q가 Q_D 상에 놓인 S의 유일한 소 아이디얼임을 보였다; 이는 $e(Q|Q_D)f(Q|Q_D) = ef = [L : L_D]$라는 사실에서도 복원될 수 있다.

이제 $K' = L_H$가 Q가 P' 상에 놓인 유일한 소 아이디얼이도록 하는 임의의 중간체라 하자. 우리는 모든 $\sigma \in H$가 Q를 P' 상에 놓인 다른 소 아이디얼로 대응시킴을 알고 있으며 따라서 $H \subset D$여야 한다. 이는 $L_D \subset K'$을 함의하며 (2)를 수립한다. 이러한 결과는 다음 도표를 고려하는 것으로 얻어질 수도 있다. (여기에 나타난 차수들은 Theorem 28을 P 상에서의 Q와 P' 상에서의 Q에 대하여 모두 적용하여 얻어졌다.) 여기에서 e', f', r'은 P'의 정규 확대 L에서의 분리에 연관된 수들이다. 그러므로 r'은 P' 상에 놓인 소 아이디얼들의 개수이다.



이러한 도표는 만약 $r' = 1$이면 $K' = L_D K'$이며 따라서 $L_D \subset K'$임을 함의한다.

다음으로 $e(P'|P) = f(P'|P) = 1$이라 가정하자. 그 경우 e, f가 순차적 확대에서 곱셈적이라는 사실에 의해 $e = e'$이며 $f = f'$이다. 위 도표를 고려하면 L_D와 $L_D K'$이 L에서 동일한 지표를 가짐을 알 수 있다. 이들 중 하나가 다른 하나에 포함되므로 이들은 서로 같아야 하며 따라서 $K' \subset L_D$이다. 그러므로 (1)을 얻는다.

(3)도 마찬가지이다: 만약 $e(P'|P) = 1$이면 $e = e'$이고 따라서 $L_E = L_E K'$이고 따라서 $K' \subset L_E$이다.

마지막으로 만약 Q가 P' 상에서 완전분기이면 $[L : K'] = e'$이다. 위 도표를 고려하면 $K' = L_E K'$이며 따라서 $L_E \subset K'$이다. □

이 정리는 몇 가지 흥미로운 결과들을 가진다. 우리는 이를 이용하여 2차상호법칙을 증명할 것이다. 다음 개념을 도입하는 것이 유용할 것이다: 수체 K에서의 소 아이디얼 P가 확대체 F에서 **완전분리(splits completely)**됨은 P가 $[F : K]$개 서로 다른 소 아이디얼들로 분리되는 것이다. 이 경우 Theorem 21에 의해 이러한 모든 소 아이디얼들은 같은 e를 가지며 $f = 1$이어야 한다. 역으로 P 상에 놓인 F의 모든 소 아이디얼들이 같은 e를 가지며 $f = 1$이면 P는 (다시 Theorem 21에 의해) F에서 완전분리된다. 만약 소 아이디얼이 K의 확대체 F에서 완전분리되면 이는 임의의 부분확대에서도 완전분리됨이 따라온다. 이를 Theorem 29의 관찰 (1)과 조합하면 다음을 얻는다.

Corollary. (P 상에 놓인 어떠한 Q에 대하여) 만약 D가 G의 정규 부분군이면 P가 K'에서 완전분리될 필요충분조건은 $K' \subset L_D$인 것이다.

Proof. 만약 P가 K'에서 완전분리되면 ($P' = Q \cap R'$이라 할 경우) 명백히 $e(P'|P) = f(P'|P) = 1$이다. 그 경우 (1)에 의해 $K' \subset L_D$이다. 역으로 Theorem 28의 Corollary 2는 P가 L_D에서 완전분리되며 따라서 $K \subset K' \subset L_D$인 임의의 K'에서도 완전분리됨을 보여준다. □

이는 G가 가환군이며 따라서 G의 모든 부분군이 정규인 상황에 적용될 수 있다.

p가 $\mathbb{Z}$에서의 홀수 소수라 하자. $n \in \mathbb{Z}, p \nmid n$에 대하여 **Legendre 기호(Legendre symbol)**를 다음과 같이 정의한다.

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & (n\text{이 } \bmod p\text{로 제곱수}) \\ -1 & (\text{그 외의 경우}) \end{cases}$$

2차상호법칙은 다음이 성립함을 주장한다: 2에 대해서는 다음이 성립하며,

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & (p \equiv \pm 1 \pmod 8) \\ -1 & (p \equiv \pm 3 \pmod 8) \end{cases}$$

홀수 소수 $q \neq p$에 대해서는 다음이 성립한다.

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & (p \text{ 또는 } q \equiv 1 \pmod 4) \\ -\left(\frac{p}{q}\right) & (p \equiv q \equiv 3 \pmod 4) \end{cases}$$

우리는 $p-1$의 임의의 인수 d에 대하여 소수가 $\bmod p$로 d중멱이 되는지에 대한 판정법을 수립할 것이다. 이것은 모두 $\omega = e^{2\pi i/p}$에 대한 원분체 $\mathbb{Q}[\omega]$에서 이루어진다. 우리는 $\mathbb{Q}[\omega]$의 $\mathbb{Q}$ 상에서의 Galois 군 G가 위수 $p-1$의 순환군임을 알고 있으며 따라서 $p-1$의 각각의 인수 d에 대하여 $\mathbb{Q}$ 상에서 d차인 유일한 부분체 $F_d \subset \mathbb{Q}[\omega]$가 존재한다. ($F_d$는 위수 $(p-1)/d$를 가지는 G의 유일한 부분군의 고정체이다.) 이에 더해 $F_{d_1} \subset F_{d_2}$ iff $d_1 | d_2$인 것이다.

Theorem 30. p가 홀수 소수이며 q가 p가 아닌 임의의 소수라 하자. $p-1$의 인수 d를 고정하자. 그 경우 q가 $\bmod q$로 d중멱일 필요충분조건은 q가 F_d에서 완전분리되는 것이다.

Proof. q가 $\mathbb{Q}[\omega]$에서 r개의 서로 다른 소 아이디얼들로 분리됨을 알고 있다. 여기에서 $f = (p-1)/r$은 q의 $\bmod p$ 곱셈군 $\{1, \ldots, p-1\}$에서의 위수이다. 이것이 위수 $p-1$의 순환군이므로 d중멱들은 위수가 $(p-1)/d$의 인수들인 모든 원소들로 구성된 위수 $(p-1)/d$의 유일한 부분군을 형성한다. (독자는 이것을 확실히 이해하라. 이 이상의 군론은 필요하지 않다.) 그러므로 다음이 모두 서로 동치이다:

- q가 $\bmod p$로 d중멱이다.
- $f | (p-1)/d$
- $d | r$
- $F_d \subset F_r$

마지막으로 q 상에 놓인 $\mathbb{Z}[\omega]$의 임의의 소 아이디얼 Q에 대하여 F_r이 q 상에서의 Q에 대한 분해체임을 관찰하라. (이는 분해체가 $\mathbb{Q}$ 상에서 차수 r을 가져야 하며 이러한 체는 F_r뿐이기 때문이다.) 그러므로 Theorem 29의 따름정리에 의해 조건 $F_d \subset F_r$은 q가 F_d에서 완전분해됨과 동치이다. □

Corollary (THE QUADRATIC RECIPROCITY LAW (2차상호법칙))**.** (진술은 위에 적혀 있다.)

Proof. $\left(\frac{q}{p}\right) = 1$ iff q가 F_2에서 완전분해되는 것이다. F_2가 무엇인가? $\mathbb{Q}[\omega]$가 $\mathbb{Q}[\sqrt{\pm p}]$를 포함하며 여기에서 부호가 $+$일 필요충분조건은 $p \equiv 1 \pmod 4$인 것이었음을 상기하자. (Chapter 2, exercise 8) 그러므로 이것이 F_2여야 한다. 그 경우 결과는 Theorem 25에서 따라온다; 세부사항을 확인하는 것은 독자에게 남기겠다. exercise 3을 참조하라. □

Theorem 29를 사용하여 (정규성에 대한 가정이 없는) 다음 결과를 수립할 수도 있다.

Theorem 31. K가 수체이며 L, M이 K의 확대라 하자. K의 소 아이디얼 P를 고정하자. 만약 P가 L, M 모두에서 비분기이면 P는 합성체 LM에서 비분기이다. 만약 P가 L, M 모두에서 완전분리이면 P는 LM에서 완전분리이다.

Proof. 먼저 P가 L, M에서 비분기라 가정하고 P'가 P 상에 놓인 LM의 임의의 소 아이디얼이라 하자. 우리는 $e(P'|P) = 1$임을 보여야 한다. F가 LM을 포함하는 K의 임의의 정규 확대이며 Q가 P' 상에 놓인 F의 임의의 소 아이디얼이라 하자. (Theorem 20에 의해 이러한 Q가 존재한다.) Q도 P 상에 놓여 있다; $E = E(Q|P)$가 대응하는 관성군이며 F_E가 관성체라 하자. 소 아이디얼 $Q \cap L$과 $A \cap M$가 P 상에서 반드시 비분기여야 하므로 Theorem 29는 F_E가 L, M을 포함함을 보여준다. 따라서 F_E는 LM도 포함하며 이는 $Q \cap LM = P'$이 P 상에서 비분기임을 함의한다.

완전분리성에 대한 증명도 E를 D로 대체해야 한다는 점을 제외하면 완전히 동일하다. 이를 확인하는 것은 독자에게 남기겠다. LM에서의 완전분리가 P 상에 놓인 LM의 모든 소 아이디얼 P'에 대하여 $e(P'|P) = f(P'|P) = 1$이라는 조건과 동치임을 상기하라. □

Corollary 1. K와 L이 수체이며 $K \subset L$이고 P가 K에서의 소 아이디얼이라 하자. 만약 P가 L에서 비분기이거나 완전분리이면 L의 K 상에서의 정규 폐포 M에서도 같은 것이 성립한다. (M은 L을 포함하는 K의 최소 정규 확대이다; 이는 K를 점별 고정하는 모든 매장 $\sigma : L \to \mathbb{C}$에 대한 모든 체 $\sigma(L)$들의 합성이다.)

Proof. 만약 P가 L에서 비분기이면 모든 $\sigma(L)$에서도 동일한 것이 성립한다. 그 경우 Theorem 31을 반복적용하면 P는 M에서 비분기임을 알 수 있다. 동일한 논의는 P가 L에서 완전분리이면 M에서도 완전분리임을 보여준다. □

L이 K의 정규 확대인 상황으로 돌아가자. G, R, S, P, Q가 앞에서와 같다 하자. 우리는 Q가 동일한 P 상에 놓인 S의 다른 소 아이디얼 Q'으로 대체될 경우 $D(Q|P)$와 $E(Q|P)$에 무슨 일이 일어나는지를 알아내고자 한다. 우리는 어떠한 $\sigma \in G$에 대하여 $Q' = \sigma Q$임을 알고 있다(Theorem 23); 그러므로 다음을 간단히 보일 수 있다.

$$D(\sigma Q|P) = \sigma D(Q|P)\sigma^{-1}$$
$$E(\sigma Q|P) = \sigma E(Q|P)\sigma^{-1}$$

(이를 검증하는 것은 독자에게 남기겠다.) 그러므로 D와 E는 G의 공액 부분군으로 대체된다. 특히 만약 G가 가환군인 경우 군 $D(Q|P)$와 $E(Q|P)$는 P에만 의존하며 Q에 의존하지 않는다.

The Frobenius Automorphism (Frobenius 자기동형사상)

이제 P가 L에서 비분기라 가정하자. 즉 $E(Q|P)$가 자명군이다. 그 경우 $D(Q|P)$가 S/Q의 R/P 상에서의 Galois 군과 동형이다. 이러한 Galois 군은 모든 $x \in S/Q$를 $x^{\|P\|}$로 대응시키는 특수한 생성자를 가진다. (Appendix C를 참조하라.) 대응하는 자기동형사상 $\phi \in D$는 모든 $\alpha \in S$에 대하여 다음을 만족시킨다.

$$\phi(\alpha) \equiv \alpha^{\|P\|} \pmod{Q}$$

P가 L에서 비분기라 가정하면 ϕ는 이러한 성질을 가지는 D의 유일한 원소이며, (이러한 성질이 명백히 $\phi \in D$임을 함의하므로) 사실 G의 유일한 원소이다. 우리는 Q와 P에 대한 종속성을 나타내기 위해 이러한 자기동형사상을 $\phi(Q|P)$로 표기하겠다. 이는 Q의 P 상에서의 **Frobenius 자기동형사상(Frobenius automorphism)**이라 불린다. 각각의 $\sigma \in G$에 대하여 $\phi(\sigma Q|P) = \sigma\phi(Q|P)\sigma^{-1}$임을 간단히 보일 수 있다. (연습문제.) P 상에 놓인 모든 소 아이디얼이 이러한 형태이므로 우리는 원소 $\phi(Q|P)$의 공액류가 P에 의해 유일하게 결정된다 결론지을 수 있다. 특히 만약 G가 가환군이면 $\Phi(Q|P)$가 비분기 소 아이디얼 P에 의해 유일하게 결정된다. 이러한 ϕ는 모든 Q에 대하여 동일한 합동식을 만족시키며 따라서 P 상에 놓인 모든 소 아이디얼 Q들의 곱인 PS에 대하여 다음이 만족시킨다.

$$\phi(\alpha) \equiv \alpha^{\|P\|} \pmod{PS}$$

이를 모두 요약하면 다음과 같다:

Theorem 32. L이 K의 정규 확대이며 P가 L에서 비분기인 K의 소 아이디얼이라 하자. P 상에 놓인 L의 각각의 소 아이디얼 P에 대하여 유일한 $\phi \in G$가 존재하여 다음을 만족시킨다.

$$\phi(\alpha) \equiv \alpha^{\|P\|} \pmod{Q} \qquad (\forall \alpha \in S)$$

G가 가환군인 경우 ϕ는 P에만 의존하며 다음을 만족시킨다.

$$\phi(\alpha) \equiv \alpha^{\|P\|} \pmod{PS} \qquad (\forall \alpha \in S)$$

□

Frobenius 자기동형사상의 중요성의 편린은 그 위수가 $f(Q|P)$이며 따라서 $\phi(Q|P)$가 P가 L에서 어떻게 분리되는지를 나타낸다는 사실로부터 알 수 있다. ($\bar{G}$가 위수 $f(Q|P)$의 순환군이며 동형사상 $D \to \bar{G}$ 하에서 $\phi(Q|P)$가 $\bar{G}$의 생성자에 대응되므로 우리는 이를 알 수 있다.) 그러므로 예를 들어 비분기 소 아이디얼 P가 정규 확대 L에서 완전분리될 필요충분조건은 $\phi = 1$인 것이다.

원분체는 좋은 예시를 제공한다. $L = \mathbb{Q}[\omega], \omega = e^{2\pi i/m}$이며 $K = \mathbb{Q}$라 하자. 우리는 $\sigma \in G, \sigma(\omega) = \omega^k$와 $\bar{k} \in \mathbb{Z}_m^*$의 대응 하에서 G가 정수 $\bmod m$ 곱셈군 $\mathbb{Z}_m^*$와 동형임을 알고 있다. Frobenius 자기동형사상은 모든 비분기 소수 p(즉 m의 인수가 아닌 모든 소수 및 $m \equiv 2 \pmod 4$인 경우 $p = 2$)에 대하여 정의된다. Galois 군이 가환군이므로 ϕ는 p에만 의존한다. $\forall \alpha \in \mathbb{Z}[\omega]$ $\phi(\alpha) \equiv \alpha^p \pmod{p\mathbb{Z}[\omega]}$가 성립해야 한다. G의 어떠한 구성원이 이것을 만족시키는지를 간단히 추측할 수 있다; 이는 물론 ω를 ω^p로 대응시키는 자기동형사상 σ여야 한다. 일반적으로 다음이 성립한다.

$$\sigma\left(\sum a_i\omega^i\right) = \sum a_i\omega^{pi} \qquad (a_i \in \mathbb{Z})$$

그러므로 우리는 정수 a_i들에 대하여 다음을 보여야 한다.

$$\sum a_i\omega^{pi} \equiv \left(\sum a_i\omega^i\right)^p \pmod{p\mathbb{Z}[\omega]}$$

이를 검증하는 것은 독자들에게 남기겠다. (필요하다면 Chapter 2, exercise 5를 참조하라.) 이것이 (원래 Theorem 26에서 증명된) $p \nmid m$인 경우 f가 p의 mod m에서의 위수임을 보이는 다른 방법을 제공함을 기억해 두라. 앞의 증명에서도 본질적으로 동일하게 $\bar{G}$와 σ에 의해 생성된 군 간의 동형사상을 수립했다; 그러나 우리는 아직 분해군과 관성군의 필수적인 성질들을 개발하지 않았으며 따라서 약간 다른 논의가 필요하다.

Frobenius 자기동형사상은 Chapter 8에서 재등장할 것이며 이곳에서 우리는 Frobenius 자기동형사상이 유체론에서 중심적인 역할을 수행하며 놀라운 성질을 가짐을 보게 될 것이다: 만약 L이 K의 정규 확대이며 Galois 군 G가 가환군이면 G의 모든 구성원이 K의 무한히 많은 소 아이디얼들에 대한 Frobenius 자기동형사상이다. 위에서 기술된 원분체의 경우에는 이러한 사실이 어떠한 유명한 정리가 되는가?

Frobenius 자기동형사상이 정규 확대의 경우에만 정의되었음에도 불구하고 이는 임의의 확대에서의 비분기 소 아이디얼의 분리를 결정하기 위해 사용될 수 있다. $K \subset L \subset M$이 수체들이며 M이 K 상에서 정규라 하자. R, S, T가 각각 K, L, M에서의 수환을 나타낸다 하자. M에서 비분기인 K의 소 아이디얼 P를 고정하자. (그러므로 만약 P가 L에서 비분기이면 M을 L의 K 상에서의 정규 폐포로 선택할 수 있다.) P 상에 놓인 M의 임의의 소 아이디얼 U를 고정하고 $\phi = \phi(U|P), D = D(U|P)$라 하자. 마지막으로 H가 L을 점별 고정하는 G의 부분군, i.e. M의 L 상에서의 Galois 군이라 하자. 우리는 ϕ에 의한 H의 우 잉여류들의 치환을 고려하는 것으로 P가 L에서의 분리를 결정할 수 있음을 보이겠다.

잉여류 $H\sigma, \sigma \in G$들은 ϕ에 의한 우 곱셈에 의해 치환된다: $H\sigma$는 $H\sigma\phi$로 대응된다. 우 잉여류들의 집합은 서로 소 집합(궤도)들로 분할되며 이들은 각각 어떠한 $\sigma \in G$에 대하여 다음과 같은 형태를 가진다.

$$\{H\sigma, H\sigma\phi, H\sigma\phi^2, \ldots, H\sigma\phi^{m-1}\}$$

여기에서 $H\sigma\phi^m = H\sigma$이다. 이와 동치로, 이는 치환을 구성하는 순환들 중 하나이다.

Theorem 33. 위 표기법 하에서 H의 G에서의 우 잉여류들의 집합이 다음 집합들로 분할된다 하자.

$$\{H\sigma_1, H\sigma_1\phi, H\sigma_1\phi^2, \ldots, H\sigma_1\phi^{m_1-1}\}$$
$$\vdots$$
$$\{H\sigma_r, H\sigma_r\phi, H\sigma_r\phi^2, \ldots, H\sigma_r\phi^{m_r-1}\}$$

그 경우 P의 L에서의 분리는 다음에 의해 주어진다.

$$PS = Q_1 Q_2 \cdots Q_r$$

여기에서 $Q_i = (\sigma_i U) \cap S$이다. 이에 더해 $f(Q_i|P) = m_i$이다.

Proof. 명백히 모든 Q_i들은 P 상에 놓인 S의 소 아이디얼들이다. 이들이 서로 다름을 보이자: $Q_i = Q_j, i \neq j$라 가정하자. 그 경우 $\sigma_i U$와 $\sigma_j U$는 S의 동일한 소 아이디얼 상에 놓인 T의 소 아이디얼들이다. 그 경우 Theorem 23에 의해 어떠한 $\tau \in H$에 대하여 $\tau\sigma_i U = \sigma_j U$이다. 그 경우 $\sigma_j^{-1}\tau\sigma_i \in D$이다. D가 ϕ에 의해 생성된 순환군이므로 어떠한 k에 대하여 $\sigma_j^{-1}\tau\sigma_i = \phi^k$이다. 그러나 그 경우 $H\sigma_i$와 $H\sigma_j\phi^k$가 동일한 잉여류이지만 이들이 분할의 서로 다른 부분에 속하므로 이는 불가능하다. 따라서 Q_i들이 서로 다르다.

각각의 i에 대하여 $f(Q_i|P) \geq m_i$임을 주장하겠다; Theorem 21 및 $m_1 + \cdots + m_r = [L : K]$라는 사실에 의해 (이것이 왜 성립하는가?) 각각의 i에 대하여 등호가 성립하며 Q_i들이 P 상에 놓인 S의 소 아이디얼 전부임이 따라올 것이다.

임의의 $Q = Q_i$를 고정하고 $m = m_i, \sigma = \sigma_i$라 하자. 그러므로 $Q = (\sigma U) \cap S$이며 우리는 $f(Q|P) \geq m$임을 보여야 한다. 다음을 어렵지 않게 보일 수 있다. (exercise 11을 참조하라.)

$$\phi(\sigma U|Q) = \phi(\sigma U|P)^{f(Q|P)}$$

따라서 다음이 성립한다.

$$\phi(\sigma U|Q) = (\sigma\phi\sigma^{-1})^{f(Q|P)} = \sigma\phi^{f(Q|P)}\sigma^{-1}$$

반드시 $\phi(\sigma U|Q) \in H$여야 하므로 $\sigma\phi^{f(Q|P)}\sigma^{-1} \in H$이다; 이와 동치로 $H\sigma\phi^{f(Q|P)} = H\sigma$이다. 이는 주장과 마찬가지로 $f(Q|P) \geq m$임을 보여준다. □

Theorem 33의 구체적인 응용이 exercise 13에 주어져 있다.

Theorem 24의 역을 증명하는 것으로 이 장을 마치겠다. 증명은 Theorem 28(구체적으로는 $|E| = e$라는 사실)과 Theorem 31의 따름정리를 사용한다.

Theorem 34. K가 수체이며 $R = \mathbb{A} \cap K$이고 소수 $p \in \mathbb{Z}$가 disc(R)의 인수라 하자. 그 경우 p는 K에서 분기이다.

Proof. R에 대한 정수적 기저 $\alpha_1, \ldots, \alpha_n$을 고정하면 $\operatorname{disc}(R) = |\operatorname{T}^K(\alpha_i\alpha_j)|$이다. 모든 정수들을 $\bmod p$로 축약하면 우리는 이를 체 $\mathbb{Z}_p$ 상에서의 행렬식으로 간주할 수 있다. 그 경우 $p|\operatorname{disc}(R)$이므로 이는 0이다. 이는 행들이 $\mathbb{Z}_p$ 상에서 선형 종속임을 함의한다. 이와 동치로 모두 p의 배수이지는 않은 정수 $m_1, \ldots, m_n \in \mathbb{Z}$가 존재하여 각각의 j에 대하여 다음이 p의 배수이도록 한다.

$$\sum_{i=1}^{n} m_i \operatorname{T}^K(\alpha_i\alpha_j)$$

$\alpha = \sum m_i\alpha_i$라 하면 각각의 j에 대하여 $p|\operatorname{T}^K(\alpha\alpha_j)$를 얻는다. $\operatorname{T}^K(\alpha R) \subset p\mathbb{Z}$가 따라온다. m_i들이 모두 p의 배수이지는 않으므로 $\alpha \notin pR$임을 기억해 두라. (이것이 왜 성립하는가?)

이제 p가 K에서 비분기라 가정하자. 우리는 모순을 얻을 것이다. 가정에 의해 pR은 서로 다른 소 아이디얼들의 곱이다; 이러한 소 아이디얼들 중 하나가 α를 포함하지 않음이 따라온다. (그렇지 않으면 α는 이러한 소 아이디얼들의 교집합(i.e. 최소공배수이며 곱)에 속할 것이다.) 그러므로 p 상에 놓인 R의 어떠한 소 아이디얼 P에 대하여 $\alpha \notin P$이다.

이제 L이 $\mathbb{Q}$ 상에서의 K의 정규 폐포라 하자. 그 경우 Theorem 31의 따름정리에 의해 p는 L에서 비분기이다. P 상에 놓인 $S = \mathbb{A} \cap L$의 임의의 소 아이디얼 Q를 고정하면 ($\alpha \in R$이며 $Q \cap R = P$이므로) $\alpha \notin Q$가 성립한다.

다음으로 우리는 $S = \mathbb{A} \cap L$에 대하여 $\operatorname{T}^L(\alpha S) \subset p\mathbb{Z}$임을 주장하겠다. 자취의 추이성 및 $\alpha \in K$라는 사실을 이용하면 다음을 얻는다.

$$\operatorname{T}^L(\alpha S) = \operatorname{T}^K \operatorname{T}^L_K(\alpha S) = \operatorname{T}^K(\alpha \operatorname{T}^L_K(S)) \subset \operatorname{T}^K(\alpha R) \subset p\mathbb{Z}$$

이제 Q에 속하지 않지만 p 상에 놓인 S의 다른 모든 소 아이디얼에 속하는 임의의 원소 $\beta \in S$를 고정하자; 중국인의 나머지 정리에 의해 이러한 원소가 존재함을 간단히 보일 수 있다. 각각의 $\gamma \in S$에 대하여 다음이 성립함을 주장하겠다.

(1) $\operatorname{T}^L(\alpha\beta\gamma) \in Q$
(2) 각각의 $\sigma \in G - D$에 대하여 $\sigma(\alpha\beta\gamma) \in Q$

여기에서 G는 L의 $\mathbb{Q}$ 상에서의 Galois 군이며 D는 분해군 $D(Q|p)$이다. 우리가 이미 $\operatorname{T}^L(\alpha S) \subset p\mathbb{Z}$임을 보였으며 $p\mathbb{Z} \subset Q$이므로 첫째 진술은 자명하다. 둘째 진술을 보이기 위해 ($\sigma^{-1}Q$가 Q와 달라야 하므로) $\beta \in \sigma^{-1}Q$임을 기억해 두라; 그러므로 $\sigma(\beta) \in Q$이며 이는 (2)를 함의한다.

(1)과 (2)로부터 다음을 얻는다.

$$\sum_{\sigma \in D} \sigma(\alpha\beta\gamma) \in Q \qquad (\forall \gamma \in S)$$

이는 다음과 같이 모순으로 이어진다: 우리는 D의 원소들이 S/Q의 자기동형사상들을 유도함을 알고 있다; 그러므로 우리는 (자기동형사상 $\sigma \in D$들을 포함하여) 모든 것을 $\bmod Q$로 축약할 수 있다. 이는 다음을 준다.

$$\sum_{\sigma \in D} \bar{\sigma}(\bar{\alpha}\bar{\beta}\bar{\gamma}) = 0 \qquad (\forall \gamma \in S)$$

명백히 $\bar{\alpha}\bar{\beta}$는 S/Q의 0이 아닌 원소이며 (γ가 S 전체 범위를 가지므로) $\bar{\gamma}$는 S/Q 전체 범위를 가진다. 다음이 성립함이 따라온다.

$$\sum_{\sigma \in D} \bar{\sigma}(x) = 0 \qquad (\forall x \in S/Q)$$

그러나 $\bar{\sigma}$들은 S/Q의 서로 다른 자기동형사상들이다; 이는 관성군 $E(Q|p)$가 자명군이기 때문이다. (p가 L에서 비분기임을 상기하라.) 서로 다른 자기동형사상들의 합은 절대 0이 될 수 없다. (exercise 15를 참조하라.) 그러므로 우리는 모순을 얻는다. □

판별식이 p를 정확히 홀수 회 인수로 가지는 경우에 대한 훨씬 간단한 증명이 존재한다.

Exercises (연습문제)

5 | The Ideal Class Group and the Unit Group (아이디얼류군과 가역원군)

수환 R의 아이디얼류군이 0이 아닌 아이디얼들의 다음 관계 하에서의 동치류들로 구성됨을 상기하라.

$$I \sim J \text{ iff 어떠한 0이 아닌 } \alpha, \beta \in R\text{에 대하여 } \alpha I = \beta J$$

군 연산은 자명한 방식으로 정의된 곱셈이며 이것이 실제로 군이라는 사실은 Chapter 3에서 증명되었다. (Theorem 15의 Corollary 1) 이 장에서 우리는 수환의 아이디얼류군이 유한군임을 증명하고 특정 경우에 아이디얼류군을 결정할 수 있도록 해주는 몇 가지 정량적 결과들을 수립할 것이다.

우리는 또한 수환의 가역원군의 구조를 결정할 것이다.

아이디얼류군의 유한성은 놀라울 만큼 간단히 보일 수 있다. 먼저 다음을 증명하겠다.

Theorem 35. K가 수체이고 $R = \mathbb{A} \cap K$라 하자. (K에 의존하는) 양의 실수 λ가 존재하여 R의 0이 아닌 모든 아이디얼 I가 다음을 만족시키는 0이 아닌 원소 α를 포함하도록 한다.

$$|\,\mathrm{N}_{\mathbb{Q}}^{K}(\alpha)| \leq \lambda \|I\|$$

(λ가 I에 독립적임을 강조하겠다. 만약 그렇지 않다면 이 정리는 그다지 강력하지 못했을 것이다.)

Proof. R의 정수적 기저 $\alpha_1, \ldots, \alpha_n$을 찾고 $\sigma_1, \ldots, \sigma_n$이 K의 $\mathbb{C}$로의 매장들을 나타낸다 하자. λ가 다음과 같이 선택될 수 있음을 주장하겠다.

$$\prod_{i=1}^{n} \sum_{j=1}^{n} |\sigma_i \alpha_j|$$

임의의 아이디얼 I에 대하여 m이 다음을 만족시키는 유일한 양의 정수라 하자.

$$m^n \leq \|I\| < (m+1)^n$$

다음과 같은 R의 $(m+1)^n$개 원소들을 고려하자.

$$\sum_{j=1}^{n} m_j \alpha_j \quad , \quad m_j \in \mathbb{Z} \quad , \quad 0 \leq m_j \leq m$$

이들은 $\|I\|$개보다 많으므로 이들 중 2개는 $\mathrm{mod} I$로 합동이어야 한다; 이들의 차를 취하면 다음 형태를 가지는 I의 0이 아닌 구성원을 얻는다.

$$\alpha = \sum_{j=1}^{n} m_j \alpha_j \quad , \quad m_j \in \mathbb{Z} \quad , \quad |m_j| \leq m$$

마지막으로 다음이 성립한다.

$$|\,\mathrm{N}_{\mathbb{Q}}^{K}(\alpha)| = \prod_{i=1}^{n} |\sigma_i \alpha| \leq \prod_{i=1}^{n} \sum_{j=1}^{n} m_j |\sigma_i \alpha_j| \leq m^n \lambda \leq \|I\| \lambda$$

□

Corollary 1. R의 모든 아이디얼류는 (정리에서와 같은 λ에 대하여) $\|J\| \leq \lambda$인 아이디얼 J를 포함한다.

Proof. 아이디얼류 C가 주어진 경우 역원 류 C^{-1}을 고려하고 임의의 아이디얼 $I \in C^{-1}$을 고려하자. 정리에서와 마찬가지로 $\alpha \in I$를 얻어라. I는 주 아이디얼 (α)를 포함하며 따라서 어떠한 아이디얼 J에 대하여 $(\alpha) = IJ$이다. $J \in C$가 반드시 성립해야 한다. 마지막으로 Theorem 22를 사용하면 다음을 얻는다.

$$|\,\mathrm{N}_{\mathbb{Q}}^{K}(\alpha)| = \|(\alpha)\| = \|I\| \cdot \|J\|$$

결과가 따라온다. □

Corollary 2. R의 아이디얼류는 유한 개만 존재한다.

Proof. 유한 개 J만이 $\|J\| \leq \lambda$를 만족시킬 수 있다: 이 부등식은 J의 가능한 소인자들을 유한집합으로 제한하며 이들이 등장할 수 있는 멱에 대한 상계를 준다. (만약 $J = \prod P_i^{n_i}$이면 $\|J\| = \prod \|P_i\|^{n_i}$이다.) □

예를 들어 $R = \mathbb{Z}[\sqrt{2}]$를 고려하자. 정수적 기저 $\{1, \sqrt{2}\}$를 선택하면 Theorem 35의 증명에서 $\lambda = (1+\sqrt{2})^2$를 얻는다. 이는 5와 6 사이에 있는 수이다. 그러므로 모든 아이디얼류는 $\|J\| \leq 5$인 아이디얼 J를 포함해야 한다. J의 가능한 소인자는 $2, 3, 5$ 상에 놓인 것들뿐이며 (왜 그러한가?) 따라서 우리는 $2R, 3R, 5R$을 분해할 것이다: $2R = (\sqrt{2})^2$이며 $3R, 5R$은 소 아이디얼이다. (Theorem 25) 이는 $\|J\| \leq 5$를 만족시키는 아이디얼 J들은 $R, (\sqrt{2}), 2R$뿐임을 보여준다. R의 모든 아이디얼이 주 아이디얼임이 따라온다.

$3, 5, -1, -2, -3$과 같은 다른 작은 m 값에 대한 $R = \mathbb{A} \cap \mathbb{Q}[\sqrt{m}]$에 대하여 동일한 것을 시도하는 것을 독자에게 남기겠다. $m = -5$인 경우 모든 아이디얼류가 $\|J\| \leq 10$인 어떠한 J를 포함함을 알 수 있으며 따라서 $2, 3, 5, 7$ 상에 놓인 소 아이디얼들을 고려하자: Theorem 25에 의해 다음이 성립한다.

$$\begin{aligned}
2R &= (2, 1+\sqrt{-5})^2 \\
3R &= (3, 1+\sqrt{-5})(3, 1-\sqrt{-5}) \\
5R &= (\sqrt{-5})^2 \\
7R &= (7, 3+\sqrt{-5})(7, 3-\sqrt{-5})
\end{aligned}$$

$(2, 1+\sqrt{-5})$가 주 아이디얼이 아님을 간단히 보일 수 있다: 만약 이것이 주 아이디얼 (α)라면 다음이 성립해야 하며,

$$|\,\mathrm{N}_{\mathbb{Q}}^{K}(\alpha)| = \|(\alpha)\| = 2$$

따라서 $\mathrm{N}_{\mathbb{Q}}^{K}(\alpha) = \pm 2$여야 한다. $a, b \in \mathbb{Z}$에 대하여 $\alpha = a + b\sqrt{-5}$로 표기하면 $a^2 + 5b^2 = \pm 2$를 얻으며 이는 명백히 불가능하다. 마찬가지로 우리는 $3R$과 $7R$의 소인자들이 주 아이디얼이 아님을 보일 수 있다. $(2, 1+\sqrt{-5})$를 포함하는 아이디얼류는 아이디얼류군에서 위수 2의 원소이다. 이것과 $3, 7$ 상에 놓여 있는 소 아이디얼을 포함하는 아이디얼류들 간의 관계를 조사하기 위해 노름이 $2, 3, 7$만을 인수로 가지는 원소들을 살펴보자: $\mathrm{N}(a + b\sqrt{-5}) = a^2 + 5b^2$를 고려하면 $\mathrm{N}(1+\sqrt{-5}) = 6$임을 알 수 있으며 따라서 주 아이디얼 $(1+\sqrt{-5})$의 소인자들은 2와 3 상에 놓여 있어야 한다. (이러한 각각의 소인자 P에 대하여 $\|P\|$는 $\|(1+\sqrt{-5})\| = 6$의 인수이다; 따라서 $\|P\| = 2$ 또는 3이다.) I를 포함하는 아이디얼류를 $\bar{I}$로 표기하면 $\overline{(2, 1+\sqrt{-5})}$가 3 상에 놓인 소 아이디얼 중 하나인 P에 대한 $\bar{P}$의 역원임을 알 수 있다. $\overline{(2, 1+\sqrt{-5})}$가 위수 2를 가지므로 $\bar{P} = \overline{(2, 1+\sqrt{-5})}$이다. 3 상에 놓인 다른 소 아이디얼 Q에 대해서도 ($\bar{Q} = \bar{P}^{-1}$이므로) 동일한 것이 성립함을 간단히 보일 수 있다. 유사한 논의가 7 상에 놓인 소 아이디얼들에 대해서도 적용된다. 주 아이디얼이 아닌 모든 아이디얼이 동일한 아이디얼류에 속하며 따라서 아이디얼류가 2개 존재한다 결론지을 수 있다.

이는 λ의 값을 개선하는 (i.e. 감소시키는) 것으로 더 간단히 얻을 수도 있다: $(2, 1+\sqrt{-5})$만을 고려하면 충분함이 밝혀질 것이다. 고차의 경우에는 현재의 λ 값이 빠르게 증가하므로 감소된 λ 값이 훨씬 더 유용할 것이다.

λ의 개선은 R을 $\mathbb{R}^n$에 n차원 격자로서 매장하고 몇 가지 일반적인 기하학적 결과들을 적용하는 것으로 얻어질 것이다.

$\sigma_1, \ldots, \sigma_r$이 K의 $\mathbb{R}$로의 매장을 나타내며 $\tau_1, \bar{\tau}_1, \ldots, \tau_s, \bar{\tau}_s$가 K의 $\mathbb{C}$로의 남은 매장들을 나타낸다 하자. (상선은 복소 공액을 나타낸다; 실수 값이 아닌 매장들이 복소 공액 쌍을 가짐은 자명하다.) 그러므로 $r + 2s = n = [K : \mathbb{Q}]$이다. 각각의 α를 다음의 순서 n조로 대응시키는 함수 $K \to \mathbb{R}^n$을 얻을 수 있다.

$$(\sigma_1(\alpha), \ldots, \sigma_r(\alpha), \mathcal{R}\tau_1(\alpha), \mathcal{I}\tau_1(\alpha), \ldots, \mathcal{R}\tau_s(\alpha), \mathcal{I}\tau_s(\alpha))$$

여기에서 $\mathcal{R}$과 $\mathcal{I}$는 각각 복소수의 실수부와 허수부를 나타낸다. 이 함수가 자명한 핵을 가지는 덧셈적 준동형사상임을 간단히 보일 수 있다. 따라서 (덧셈 구조만을 고려하면) 이는 K의 $\mathbb{R}^n$으로의 매장이다. $R = \mathbb{A} \cap K$가 n차원 격자 ($\mathbb{R}^n$의 $\mathbb{R}$-기저의 $\mathbb{Z}$-선형생성) $\wedge_R$로 전사 대응됨을 주장하겠다. 이를 보이기 위해 R에 대한

정수적 기저 $\alpha_1, \dots, \alpha_n$을 고정하자; 이들은 $\mathbb{Z}$ 상에서 R을 생성하며 따라서 이들의 $\mathbb{R}^n$에서의 상들은 $\mathbb{Z}$ 상에서 $\wedge_R$을 생성한다. 우리는 이러한 상들이 $\mathbb{R}$ 상에서 선형 독립임을 보여야 한다.

i행이 α_i의 상이도록 하는 $n \times n$ 행렬을 구축하자. 우리는 그 행렬식이 0이 아니며 따라서 행들이 $\mathbb{R}$ 상에서 선형 독립임을 보일 것이다. 이러한 행렬식은 (i행의 전형적인 원소들을 나타내는 것으로 표기하겠다) 다음과 같다.

$$|\dots, \sigma(\alpha_i), \dots, \mathcal{R}\tau(\alpha_i), \mathcal{I}\tau_(\alpha_i), \dots|$$

기본 행 연산들을 통해 이를 다음으로 변환시킬 수 있다.

$$\frac{1}{(2i)^s}|\dots, \sigma(\alpha_i), \dots, \bar{\tau}(\alpha_i), \tau(\alpha_i), \dots|$$

이러한 마지막 행렬식을 제곱한 것이 $\operatorname{disc}(R)$이며 이는 0이 아니다. (Theorem 7)

우리는 다음을 증명했다.

Theorem 36. 함수 $K \to \mathbb{R}^n$은 R을 n차원 격자 $\wedge_R$로 전사 대응시킨다. 이러한 격자의 기본평행체는 다음의 부피를 가진다.

$$\frac{1}{2^s}\sqrt{|\operatorname{disc}(R)|}$$

$\mathbb{R}^n$에서의 n차원 격자 $\wedge$의 **기본평행체(fundamental parallelotope)**는 다음 형태의 집합을 의미한다.

$$\left\{\sum_{i=1}^{n} a_i v_i : a_i \in \mathbb{R}, 0 \le a_i < 1\right\}$$

여기에서 $\{v_1, \dots, v_n\}$은 $\wedge$의 임의의 $\mathbb{Z}$-기저이다. 이러한 평행체의 n차원 부피는 행 $v_1, \dots, v_n$을 가지는 행렬의 행렬식의 절댓값임이 잘 알려져 있다. λ에 대한 임의의 기저가 동일한 부피를 제공함을 간단히 보일 수 있으며 (exercise 2를 참조하라) 따라서 이러한 부피는 $\wedge$의 불변량이다. 우리는 이를 $\operatorname{vol}(\mathbb{R}^n/\wedge)$로 표기할 것이다. 그러므로 우리는 다음을 결정했다.

$$\operatorname{vol}(\mathbb{R}^n/\wedge_R) = \frac{1}{2^s}\sqrt{|\operatorname{disc}(R)|}$$

정수계수를 유리수계수로 대체하면 다음을 얻는다.

Corollary. K의 상은 $\mathbb{R}^n$에서 조밀하다.

일반적인 n차원 격자 $\wedge$의 경우로 돌아가 M이 $\wedge$의 n차원 부분격자라 하자. 그 경우 $\wedge/M$은 유한군이며 다음을 간단히 보일 수 있다. (exercise 3을 참조하라.)

$$\operatorname{vol}(\mathbb{R}^n/M) = \operatorname{vol}(\mathbb{R}^n/\wedge)|\wedge/M|$$

이를 R의 0이 아닌 아이디얼 I의 상 $\wedge_I$에 적용하면 다음을 얻는다.

$$\operatorname{vol}(\mathbb{R}^n/\wedge_I) = \operatorname{vol}(\mathbb{R}^n/\wedge_R)|\wedge_R/\wedge_I| = \frac{1}{2^s}\sqrt{|\operatorname{disc}(R)|}\|I\|$$

이는 Theorem 35에서 λ의 값을 개선하려는 우리의 시도와 관계가 있다.

다음으로 r과 s에 의존하는 $\mathbb{R}^n$에서의 특수한 '노름'을 다음과 같이 정의하자: 각각의 점 $x = (x_1, \dots, x_n) \in \mathbb{R}^n$에 대하여 다음과 같이 설정하자.

$$\mathrm{N}(x) = x_1 \cdots x_r (x_{r+1}^2 + x_{r+2}^2) \cdots (x_{n-1}^2 + x_n^2)$$

이는 물론 체 노름과 일치하도록 고안되었다: 만약 $\alpha \in R$이 $x \in \wedge_R$로 대응된다면 $\mathrm{N}(x) = \mathrm{N}_{\mathbb{Q}}^K(\alpha)$이다. 우리는 다음의 일반적인 결과를 증명할 것이다:

Theorem 37. 위와 같이 정의된 N에 대하여 $\mathbb{R}^n$에서의 모든 n차원 격자 $\wedge$는 다음을 만족시키는 0이 아닌 점 x를 포함한다.

$$|\mathrm{N}(x)| \le \frac{n!}{n^n}\left(\frac{8}{\pi}\right)^s \operatorname{vol}(\mathbb{R}^n/\wedge)$$

이를 $\wedge = \wedge_I$에 대하여 적용하면 다음을 얻는다.

Corollary 1. R의 0이 아닌 모든 아이디얼 I는 다음을 만족시키는 원소 α를 포함한다.

$$|\operatorname{N}_{\mathbb{Q}}^{K}(\alpha)| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc}(R)|}\cdot\|I\|$$

□

Corollary 2. R의 모든 아이디얼류는 다음을 만족시키는 아이디얼 J를 포함한다.

$$\|J\| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\operatorname{disc}(R)|}$$

□

Minkowski 상수라 불리는 인자 $\frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s$는 n이 증가할수록 빠르게 감소하므로 이는 매우 대단한 결과이다. 어떠한 경우에도 이는 Theorem 35에서의 λ 값보다 개선을 보여준다. 예를 들어 $R=\mathbb{Z}[\sqrt{-5}]$인 경우 다음이 성립한다.

$$\|J\| \leq \frac{4\sqrt{5}}{\pi} < 3$$

그러므로 모든 아이디얼류는 $\|J\| \leq 2$를 만족시키는 어떠한 J를 포함한다. 이는 아이디얼류군을 결정하기 위해 $(2, 1+\sqrt{-5})$만을 고려하면 충분하다는 앞에서의 우리의 주장을 정당화한다.

다른 좋은 예시는 5번째 원분체 $\mathbb{Q}[\omega], \omega = e^{2\pi i/5}$이다. 모든 아이디얼류는 $\|J\| \leq \frac{15\sqrt{5}}{2\pi^2}$를 만족시키는 어떠한 J를 포함한다. 이 값은 2 미만이며 따라서 모든 아이디얼류는 R을 포함한다. 다른 말로 하면 모든 아이디얼이 주 아이디얼이다.

추가적인 예시들은 연습문제에 제시되어 있다.

Corollary 2를 바라보는 다른 방법은 이것이 $|\operatorname{disc}(R)|$에 대한 하계를 제공한다는 것이다. 특히 이는 다음이 성립함을 보여준다.

$$\sqrt{|\operatorname{disc}(R)|} \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^s$$

$n \geq 2$인 경우 우변의 수는 1보다 크다. (exercise 5를 참조하라.) 따라서 다음이 성립한다.

Corollary 3. $R \neq \mathbb{Z}$일 경우 $|\operatorname{disc}(R)| > 1$이다. □

이 따름정리의 중요성은 이것에 의해 Kronecker-Weber 정리의 증명을 완료할 수 있다는 것이다: $\operatorname{disc}(R)$은 소인수를 가져야 하며 Theorem 34에 의해 이는 반드시 R에서 분기여야 한다. 그러므로 (Chapter 4에서 주장했던 것과 같이) 각각의 $K \neq \mathbb{Q}$에 대하여 K에서 분기인 $\mathbb{Z}$의 소수가 존재한다.

Theorem 37을 증명하기 위해서는 Minkowski에 의한 다음의 정리가 필요하다.

Lemma 1. $\wedge$가 $\mathbb{R}^n$에서의 n차원 격자이며 E가 다음을 만족시키는 $\mathbb{R}^n$의 볼록 가측 중심대칭 부분집합이라 하자.

$$\operatorname{vol}(E) > 2^n \operatorname{vol}(\mathbb{R}^n/\wedge)$$

그 경우 E는 $\wedge$의 어떠한 0이 아닌 점을 포함한다. 만약 E가 컴팩트하다면 강한 부등식은 $\geq$로 약화될 수 있다.

(**볼록(convex)**은 만약 $x, y \in E$이면 이들을 잇는 선분이 E에 속함을 의미한다. **가측(measurable)**은 $\mathbb{R}^n$에서의 Lebesgue 측도에 대한 것이며, Lebesgue 측도 $\operatorname{vol}(E)$가 n차원 부피에 대한 임의의 합리적인 직관적 개념과 일치한다는 점과 Lebesgue 측도가 쌍마다 서로 소 가측 집합 $E_1, E_2, \ldots$에 대하여 다음을 만족시킨다는 의미로 가산 가법적이라는 사실을 제외하면 추가적으로 설명하지는 않을 것이다.

$$\operatorname{vol}\left(\bigcup_{i=1}^{\infty} E_i\right) = \sum_{i=1}^{\infty} \operatorname{vol}(E_i)$$

마지막으로 **중심대칭(centrally symmetric)**은 0에 대하여 대칭임을 의미한다: 만약 $x \in E$이면 $-x \in E$이다.)

Proof. F가 $\wedge$에 대한 기본평행체라 하자. 그 경우 $\mathbb{R}^n$은 평행이동 $x_F, x \in \wedge$들의 분리합집합이다. 다음이 성립함이 따라온다.

$$\frac{1}{2}E = \coprod_{x\in\wedge}\left(\left(\frac{1}{2}E\right)\cap(x+F)\right)$$

여기에서 $t \in \mathbb{R}$에 대하여 $tE = \{te : e \in E\}$이며 $\coprod$는 분리합집합을 의미한다. 따라서 강한 부등식을 가정하면 다음이 성립한다.

$$\begin{aligned}\operatorname{vol}(F) < \frac{1}{2^n}\operatorname{vol}(E) &= \operatorname{vol}\left(\frac{1}{2}E\right) \\ &= \sum_{x\in\wedge} \operatorname{vol}\left(\left(\frac{1}{2}E\right) \cap (x+F)\right) \\ &= \sum_{x\in\wedge} \operatorname{vol}\left(\left(\left(\frac{1}{2}E\right) - x\right) \cap F\right)\end{aligned}$$

후자의 등호는 집합의 Lebesgue 측도가 평행이동 불변량이기 때문에 성립한다. 위 식은 집합 $((\frac{1}{2}E)-x)\cap F$들이 쌍마다 서로 소일 수 없음을 보여준다. $(\frac{1}{2}E)-x$와 $(\frac{1}{2}E)-y$가 교차하도록 하는 임의의 두 점 $x, y \in \wedge$를 고정하자; 그 경우 $x-y$는 $\wedge$의 0이 아닌 점이며 E의 볼록성과 대칭성에 의해 E가 $x-y$를 포함함을 간단히 보일 수 있다.

이제 E가 컴팩트라 가정하자. ($\mathbb{R}^n$에서 이는 유계 닫힌집합을 의미한다.) 강한 부등식을 $\geq$로 약화시키자. $m = 1, 2, \ldots$에 대하여 정리의 전반부는 집합 $(1+\frac{1}{m})E$가 $\wedge$의 0이 아닌 점 x_m을 포함함을 함의한다. x_m들은 모두 $2E$에 속하므로 $m \to \infty$에서 유계이다; 서로 다른 점 x_m들이 유한 개만 존재할 수 있음이 따라온다. 그 경우 이들 중 하나가 무한히 많은 m에 대하여 $(1+\frac{1}{m})E$에 속하며 따라서 폐포 $\bar{E} = E$에 속한다. □

Corollary (Corollary of the Lemma (보조정리의 따름정리))**.** 다음을 만족시키는 $\operatorname{vol}(A) > 0$인 컴팩트 볼록 중심대칭 집합 A가 주어졌다 하자.

$$a \in A \Rightarrow |\operatorname{N}(a)| \leq 1$$

그 경우 모든 n차원 격자 $\wedge$는 다음을 만족시키는 0이 아닌 점 x를 포함한다.

$$|\operatorname{N}(x)| \leq \frac{2^n}{\operatorname{vol}(A)}\operatorname{vol}(\mathbb{R}^n/\wedge)$$

Proof. 다음을 만족시키는 t에 대한 $E = tA$에 대하여 보조정리를 적용하라.

$$t^n = \frac{2^n}{\operatorname{vol}(A)}\operatorname{vol}(\mathbb{R}^n/\wedge)$$

세부사항을 확인하라. □

Proof of Theorem 37. 우리는 먼저 A를 다음 부등식들에 의해 정의된 집합으로 취하면 더 약한 결과를 매우 쉽게 얻을 수 있음을 일러두겠다.

$$|x_1| \leq 1, \ldots, |x_r| \leq 1, x_{r+1}^2 + x_{r+2}^2 \leq 1, \ldots, x_{n-1}^2 + x_n^2 \leq 1$$

$\operatorname{vol}(A) = 2^r\pi^s$이며 모든 $\wedge$가 다음을 만족시키는 0이 아닌 점 x를 포함한다는 사실을 얻는다.

$$|\operatorname{N}(x)| \leq \left(\frac{4}{\pi}\right)^s \operatorname{vol}(\mathbb{R}^n/\wedge)$$

그러나 우리는 더 좋은 방법을 사용할 수 있다. A를 다음에 의해 정의하자.

$$|x_1| + \cdots + |x_r| + 2\left(\sqrt{x_{r+1}^2 + x_{r+2}^2} + \cdots + \sqrt{x_{n-1}^2 + x_n^2}\right) \leq n$$

A가 볼록임을 어렵지 않게 보일 수 있으며 (exercise 4를 참조하라) 조건 $a \in A \Rightarrow |\operatorname{N}(a)| \leq 1$은 다음의 n개 양의 실수들의 기하평균과 산술평균을 비교하면 얻어진다.

$$|x_1|, \ldots, |x_r|, \sqrt{x_{r+1}^2 + x_{r+2}^2}, \sqrt{x_{r+1}^2 + x_{r+2}^2}, \ldots, \sqrt{x_{n-1}^2 + x_n^2}, \sqrt{x_{n-1}^2 + x_n^2}$$

기하평균 $\sqrt[n]{|\operatorname{N}(a)|}$는 산술평균 이하이며 산술평균은 1 이하이다. 이에 더해 우리는 다음을 증명할 것이다.

$$\operatorname{vol}(A) = \frac{n^n}{n!}2^r\left(\frac{\pi}{2}\right)^s$$

이는 Theorem 37을 증명할 것이다.

일반적으로 $V_{r,s}(t)$가 다음에 의해 정의된 $\mathbb{R}^{r+2s}$의 부분집합의 부피를 나타낸다 하자.

$$|x_1| + \cdots + |x_r| + 2\left(\sqrt{x_{r+1}^2 + x_{r+2}^2} + \cdots + \sqrt{x_{r+2s-1}^2 + x_{r+2s}^2}\right) \leq t$$

그 경우 다음이 성립한다.

$$V_{r,s}(t) = t^{r+2s} V_{r,s}(1)$$

다음이 성립함을 주장하겠다.

$$V_{r,s}(1) = \frac{1}{(r+2s)!} 2^r \left(\frac{\pi}{2}\right)^s$$

만약 $r > 0$이면 다음이 성립한다.

$$\begin{aligned} V_{r,s}(1) &= 2\int_0^1 V_{r-1,s}(1-x)\, dx \\ &= 2\int_0^1 (1-x)^{r-1+2s}\, dx\, V_{r-1,s}(1) \\ &= \frac{2}{r+2s} V_{r-1,s}(1) \end{aligned}$$

이를 반복적용하면 다음을 얻는다.

$$V_{r,s}(1) = \frac{2^r}{(r+2s)(r+2s-1)\cdots(2s+1)} V_{0,s}(1)$$

$s = 0$인 경우 무슨 일이 일어나는지 고려하는 것은 독자에게 남긴다. $V_{0,0}(1)$이 어떻게 정의되는가? $s > 0$에 대하여 $V_{0,s}(1)$을 결정하는 것이 남아있다. 다음이 성립한다.

$$V_{0,s}(1) = \iint V_{0,s-1}(1 - 2\sqrt{x^2+y^2})\, dx\, dy$$

여기에서 적분은 원형 영역 $x^2 + y^2 \leq 1/4$ 상에서 취했다. 극좌표로 변환하면 다음을 얻는다.

$$\begin{aligned} V_{0,s}(1) &= \int_0^{2\pi}\int_0^{1/2} V_{0,s-1}(1-2\rho)\rho\, d\rho\, d\theta \\ &= V_{0,s-1}(1) 2\pi \int_0^{1/2} (1-2\rho)^{2(s-1)} \rho\, d\rho \\ &= V_{0,s-1}(1)\frac{\pi}{2}\int_0^1 u^{2(s-1)}(1-u)\, du \\ &= V_{0,s-1}(1)\frac{\pi}{2}\left(\frac{1}{2s-1} - \frac{1}{2s}\right) = V_{0,s-1}(1)\frac{\pi}{2}\frac{1}{(2s)(2s-1)} \end{aligned}$$

그러므로 다음이 성립한다.

$$V_{0,s}(1) = \left(\frac{\pi}{2}\right)^s \frac{1}{(2s)!}$$

이것들을 모두 조합하면 $V_{r,s}(1)$에 대한 요구된 값을 얻는다. $\mathrm{vol}(A)$에 대한 공식이 즉시 따라온다.

이는 Theorem 37의 증명을 완료한다. □

The Unit Theorem (가역원 정리)

수환 R에서의 가역원들의 곱셈군 U를 고려하자. 우리는 U가 (R에서의 1의 근들로 구성된) 유한 순환군과 자유가환군의 직접곱임을 보일 것이다. 앞 절의 표기법 하에서 이러한 자유가환군은 계수 $r+s-1$을 가진다. 그러므로 허 2차수체의 경우 U는 단순히 1의 근들로만 구성된다. (우리는 Chapter 2에서 노름을 고려하는

것으로 이를 보였다.) 실 2차수체의 경우 1의 제곱근은 1과 -1이며 자유 성분은 계수 1을 가진다. 그러므로 (R에서의 **기본가역원(fundamental unit)**이라 불리는) 어떠한 가역원 u에 대하여 다음이 성립한다.

$$U = \{\pm u^k : k \in \mathbb{Z}\}$$

기본가역원은 조건 $u > 1$ 하에서 유일하게 결정된다. $\mathbb{Z}[\sqrt{2}]$에서의 기본가역원은 $1+\sqrt{2}$이며 $\mathbb{Z}[\sqrt{3}]$에서의 기본가역원은 $2+\sqrt{3}$이다.

실 2차수체의 기본가역원은 때로는 놀라울 만큼 클 수도 있다. 예를 들어 $\mathbb{Z}[\sqrt{31}]$에서는 $1520+273\sqrt{31}$이다. 이보다 더 나쁜 경우로, $\mathbb{Z}[\sqrt{94}]$에서는 $2143295+221064\sqrt{94}$이다. 반면에 $\mathbb{Z}[\sqrt{95}]$에서는 $39+4\sqrt{95}$에 불과하다. 이러한 가역원들을 결정하는 알고리즘이 존재한다. 이들 중 한 가지는 연분수를 이용한다. Borevich and Shafarevich, *Number Theory*, Chapter 2, Section 7.3을 참조하라. 더 간단하지만 덜 효과적인 방법이 이 장의 끝부분의 exercise 33에 제시되어 있다.

U의 자유 성분이 순환군이도록 하는 다른 종류의 수환도 존재한다. $\mathbb{R}$로의 매장을 하나만 가지는 3차 수체들은 (예를 들어 순 3차수체) $r = s = 1$이므로 이러한 성질을 가진다; 이에 더해 체가 $\mathbb{R}$로의 매장을 가지므로 1의 근은 ± 1뿐이다. 그러므로 실 2차수체의 경우와 마찬가지로 어떠한 가역원 u에 대하여 다음이 성립한다.

$$U = \{\pm u^k : k \in \mathbb{Z}\}$$

예시를 위해서는 exercise 35-42를 참조하라.

$\mathbb{R}$로의 매장을 갖지 않는 $\mathbb{Q}$ 상에서의 4차수체는 $r = 0, s = 2$를 가지며 따라서 어떠한 가역원 u에 대하여 다음을 만족시킨다.

$$U = \{\theta u^k : k \in \mathbb{Z}, \theta\text{는 1의 근}\}$$

또한 차수가 4이므로 가능한 θ는 많지 않다. 한 가지 예시는 5번째 원분체이다. 여기에서 u는 ($\omega = e^{2\pi i/5}$라 하면) $1+\omega$로 선택될 수 있다. exercise 47을 참조하라.

Theorem 38. U가 수환 $R = \mathbb{A} \cap K$에서의 가역원군이라 하자. r과 $2s$가 각각 K의 $\mathbb{C}$로의 실 매장 및 허 매장의 개수를 나타낸다 하자. 그 경우 U는 K에서의 1의 근들로 구성된 유한 순환군 W와 계수 $r+s-1$의 자유가환군 V의 직접곱 $W \times V$이다.

다른 말로 하면 V는 $r+s-1$개 가역원 $u_1, \ldots, u_{r+s-1}$들의 어떠한 집합에 대한 다음 형태의 곱들로 구성된다.

$$u_1^{k_1} u_2^{k_2} \cdots u_{r+s-1}^{k_{r+s-1}} \qquad (k_i \in \mathbb{Z})$$

이러한 집합은 R에서의 **기본가역원계(fundamental system of units)**라 불린다. 주어진 V의 원소에 대하여 지수 $k_1, \ldots, k_{r+s-1}$은 유일하게 결정된다.

Proof. 다음과 같은 함수들의 열이 존재한다.

$$U \subset R - \{0\} \longrightarrow \wedge_R - \{0\} \xrightarrow{\log} \mathbb{R}^{r+s}$$

여기에서 다음은 (K의 $\mathbb{R}^n$으로의 매장의 제한으로) 자명하게 정의되며,

$$R - \{0\} \longrightarrow \wedge_R - \{0\}$$

log는 다음과 같이 정의된다: $(x_1, \ldots, x_n) \in \wedge_R - \{0\}$에 대하여 $\log(x_1, \ldots, x_n)$은 다음의 순서 $(r+s)$조이다.

$$(\log|x_1|, \ldots, \log|x_r|, \log(x_{r+1}^2 + x_{r+2}^2), \ldots, \log(x_{n-1}^2 + x_n^2))$$

이것이 잘 정의됨을 기억해 두라: 실수 $|x_1|, \ldots, x_{n-1}^2 + x_n^2$는 모두 $\wedge_R - \{0\}$의 임의의 점에서 강하게 양수이다. (왜 그런가?)

편의성을 위해 합성 $R - \{0\} \to \mathbb{R}^{r+s}$와 $U \to \mathbb{R}^{r+s}$도 log라 지칭하겠다. $\mathbb{R}^{r+s}$는 **로가리듬 공간(logarithmic space)**이라 불린다.

다음이 성립함을 간단히 보일 수 있다:

(1) $\log \alpha\beta = \log \alpha + \log \beta \ \forall \alpha, \beta \in \mathbb{R} - \{0\}$
(2) (가역원의 노름이 1 또는 -1이므로) $\log(U)$는 $y_1 + \cdots + y_{r+s} = 0$에 의해 정의된 초평면 $H \subset \mathbb{R}^{s+1}$에 포함된다.
(3) $\mathbb{R}^{r+s}$의 임의의 유계 부분집합의 U에서의 역상이 유한집합이다. (유계집합의 $\wedge_R - \{0\}$에서의 역상이 이미 유한집합이다. 스스로에게 이를 설득하라.)

(1)과 (2)는 $\log : U \to H$가 곱셈군에서 덧셈군으로의 준동형사상임을 보여준다. (3)은 U에서의 핵이 유한집합임을 보여주며 이는 다시 핵이 K에서의 1의 근들로 구성됨을 함의한다: 핵의 모든 원소가 유한 위수를 가져야 한다. 역으로 모든 1의 근이 핵에 속함을 간단히 보일 수 있다. 이에 더해 핵이 순환군임을 간단히 보일 수 있다. (일반적으로 단위 원의 모든 유한 부분군이 순환군이다.)

(3)은 또한 상 $\log(U) \subset \mathbb{R}^{r+s}$의 모든 유계 부분집합이 유한집합이라는 성질을 보여준다. 우리는 exercise 31에서 이러한 성질을 가지는 $\mathbb{R}^{r+s}$의 부분군이 반드시 격자여야 함을 보일 것이다. (일반적으로 $\mathbb{R}^m$에서의 **격자(lattice)**는 $\mathbb{R}$ 상에서 선형 독립인 벡터들의 집합의 $\mathbb{Z}$-선형생성을 의미한다. 격자는 자유가환군이지만 그 역은 일반적으로 성립하지 않는다. 다른 말로 하면 $\mathbb{R}^m$에서의 $\mathbb{R}$-선형 독립 집합은 $\mathbb{Z}$-선형 독립이지만 그 역은 성립하지 않는다.) $\log(U)$는 H에 포함되며 따라서 이는 어떠한 차원 $d \leq r+s-1$을 가지는 격자이다. 이제부터 이를 $\wedge_U$로 표기하자.

다음으로 U가 직접곱임을 보이자. 우리는 $\wedge_U$가 계수 d의 자유가환군임을 알고 있다; $\wedge_U$의 $\mathbb{Z}$-기저로 대응되는 가역원 $u_1, \ldots, u_d \in U$를 고정하고 V가 u_i들에 의해 생성된 U의 (곱셈적) 부분군이라 하자. u_i들이 V를 자유 생성하며 따라서 V가 계수 d의 자유가환군임을 간단히 보일 수 있다; 이에 더해 W가 핵이라 하면 $U = W \times V$이다. 세부사항을 확인하는 것은 독자에게 남기겠다.

남은 것은 $d = r+s-1$임을 보이는 것이다. 이를 위해서는 log 벡터들이 $\mathbb{R}$ 상에서 선형 독립이도록 하는 $r+s-1$개 가역원들을 찾으면 충분하다. 그러나 가역원들을 만들기 전에 특정 대수적 정수의 존재성을 보장하는 보조정리가 필요하다.

Lemma 1. $1 \leq k \leq r+s$인 임의의 k를 고정하자. 0이 아닌 각각의 $\alpha \in R$에 대하여 0이 아닌 $\beta \in R$이 존재하여 다음을 만족시키며,

$$|\operatorname{N}_{\mathbb{Q}}^{K}(\beta)| \leq \left(\frac{2}{\pi}\right)^{s} \sqrt{|\operatorname{disc}(R)|}$$

만약 다음과 같이 표기하면

$$\log(\alpha) = (a_1, \ldots, a_{r+s})$$
$$\log(\beta) = (b_1, \ldots, b_{r+s})$$

각각의 $i \neq k$에 대하여 $b_i < a_i$를 만족시킨다. ($|\operatorname{N}_{\mathbb{Q}}^{K}(\beta)|$ 상계의 실제 값은 중요하지 않다. 우리가 알아야 하는 것은 α에 독립적인 상계가 존재한다는 사실이다.)

Proof. 이는 Theorem 37의 증명에서 사용된 Minkowski 기하 보조정리의 간단한 응용이다. E를 다음 부등식에 의해 정의된 $\mathbb{R}^n$의 부분집합으로 취하자.

$$|x_1| \leq c_1, \ldots, |x_r| \leq c_r$$
$$x_{r+1}^2 + x_{r+2}^2 \leq c_{r+1}, \ldots, x_{n-1}^2 + x_n^2 \leq c_{r+s}$$

여기에서 c_i들은 다음을 만족시키도록 선택되었다.

$$0 < c_i < e^{a_i} \qquad (\forall i \neq k)$$
$$c_1 c_2 \cdots c_{r+s} = \left(\frac{2}{\pi}\right)^{s} \sqrt{|\operatorname{disc}(R)|}$$

그 경우 $\operatorname{vol} E = 2^r \pi^s c_1 \cdots c_{r+s} = 2^r \operatorname{vol}(\mathbb{R}^n / \wedge_R)$이다. (이를 확인하라.) Minkowski 보조정리는 E가 $\wedge_R$의 어떠한 0이 아닌 점을 포함함을 보여주며 β가 R의 대응되는 원소로 취해질 수 있음을 간단히 검증할 수 있다. □

Lemma 1을 이용하면 특수한 가역원이 존재함을 보일 수 있다:

Lemma 2. $1 \leq k \leq r+s$인 임의의 k를 고정하자. 그 경우 $u \in U$가 존재하여 만약 다음과 같다 하면,

$$\log(u) = (y_1, \ldots, y_{r+s})$$

모든 $i \neq k$에 대하여 $y_i < 0$을 만족시킨다.

Proof. 0이 아닌 임의의 $\alpha_1 \in R$에 대하여 Lemma 1을 반복적용하여 각각의 $i \neq k$와 각각의 $j \geq 1$에 대하여 $\log(\alpha_{j+1})$의 i번째 좌표가 $\log(\alpha_j)$의 i번째 좌표보다 작도록 하며 $|\operatorname{N}_{\mathbb{Q}}^{K}(\alpha_j)|$가 유계이도록 하는 R의 원소들의 열 $\alpha_1, \alpha_2, \ldots$를 얻자. 그 경우 $\|(\alpha_j)\|$들이 유계이다; 이는 (Theorem 35의 Corollary 2에서와 같이) 서로 다른 아이디얼 (α_j)들이 유한 개만 존재함을 함의한다. $(\alpha_j) = (\alpha_h)$이며 $j < h$인 임의의 j, h를 고정하면 어떠한 $u \in U$에 대하여 $\alpha_h = \alpha_j u$이다. 이는 증명을 완료한다. □

Lemma 2는 가역원 $u_1, \ldots, u_{r+s}$가 존재하여 $\log(u_k)$의 k번째를 제외한 모든 좌표가 음수이도록 한다. $\log(u_k) \in H$이므로 k번째 좌표는 반드시 양수여야 한다. $\log(u_k)$를 k행으로 가지는 $(r+s) \times (r+s)$ 행렬을 형성하자; 이러한 행렬이 계수 $r+s-1$을 가자며 따라서 $r+s-1$개 선형 독립 행들이 존재함을 주장하겠다. 이는 가역원 정리의 증명을 완료할 것이다.

일반적으로 다음이 참이다:

Lemma 3. $A = (a_{ij})$가 $\mathbb{R}$ 상에서의 $m \times m$ 행렬이며 다음을 만족시키고,

$$\text{모든 } i\text{에 대하여 } a_{ii} > 0$$
$$\text{모든 } i \neq j\text{에 대하여 } a_{ij} < 0$$

각각의 행의 합이 0이라 하자. 그 경우 A의 계수는 $m-1$이다.

Proof. 앞의 $m-1$개 열들이 선형 독립임을 보이자: v_j들이 열벡터이며 t_j들이 모두 0이지는 않은 실수이고 $t_1 v_1 + \cdots + t_{m-1} v_{m-1} = 0$이라 하자. 일반성을 잃지 않고 어떠한 $t_k = 1$이며 다른 모든 $t_j \leq 1$이라 가정할 수 있다. (왜 그런가?) k행을 살펴보면 다음의 모순을 얻는다.

$$0 = \sum_{j=1}^{m-1} t_j a_{kj} \geq \sum_{j=1}^{m-1} a_{kj} > \sum_{j=1}^{m} a_{kj} = 0$$

□

이제 증명이 완료된다. □

Exercises (연습문제)

6 | The Distribution of Ideals in a Number Ring (수환에서의 아이디얼의 분포)