代　数　学　5　及び　6

2024 年度版

はじめに

「代数学 5」と「代数学 6」では Galois 理論を学ぶ. Abel や Galois 達によつて証明された 5 次以上の一般代数方程式には代数的な解の公式が存在しないといふ定理は Galois 理論を生み出す動機であつたが, Galois 理論自体はそれだけを目的にしたものではなく, もつと広い内容を持つてゐる. それを汲み取つていただくために, 「代数学 5」と「代数学 6」を学ぶに際しては,
(1) 体にはどの様なものがあるのか, また,
(2) 体から体への準同型（それは, 本質的には, 必然的に単射となる）にはどの様なものがあるか
の 2 つを常に問題意識として持つておいていただきたい. これら講義の目標はこの問題に対する答を理解し, 多くの体を（別個にではなくて）自己同型写像のなす群を使つて統一的に捉へる感覚を養ふことに尽きる.

数学の書物を読むには, 定義, 定理, 証明の連鎖を緻密に追跡し, そのあとで例を作つてみる, といふのが重要である. さらに, 良い例に接したあとに, 道を遡つて, その例のどこが理論化されたのかを肉付けしていくといふことも必要である. この note にはできるだけ例に接しられる様な問題を入れておいた. また, 第 11 節で述べるいくつかの例が, この講義で述べる理論の流れを掴むのに有用であらうと信じる.

さらに, Android の Smart-phone をお持ちであれば, 是非 `paridroid` を install していただき, いろいろな例の計算を試して欲しい. iPhone をお持ちの場合は `SageMath` である程度代用できる. Computer をお持ちの方には `pari/GP` を install していただきたい.

この講義 note の第 2 章 体論 は, 主に [N] の第 4 章 体論 によつて構成されてをり, 節末問題やところどころの詳細な議論で [Iy] を参考にしてゐる. 参照の便宜のために, 第 1 章で 環論について述べておいた. 概ね, 第 9 節から 17 節が「代数学 5」の範囲で, 第 18 節以降が「代数学 6」の範囲であるが, 初回の講義で適宜, 第 1 章を参考に, 環についての復習がなされるであらう.

この講義 note の作成にあたり, 2017 年度の名城大学理工学部数学科の受講生には, 多くの誤植をご指摘していただいた. そのお陰で, かなり完成度の高いものになつたと思ふ. また 2024 年 3 月に水野義紀氏から, 気付きにくい誤植をいくつかご指摘いただいた. ここに深く感謝申し上げる次第である.

最後に方程式の可解性に関しての定式化について, 一言だけ触れておきたい. 第 28 節で学ぶ, 冪根による拡大については, [Iy] の定義を採用した. この定義は [N] のそれより精密であるが, 持ち上げや合成に関して保たれないため, 関連する種々の性質を導くのに手間が掛かる. しかし, [Iy] の定義を採用してゐる書物は少ないから, その事を解説する講義も恐らく少ないと思はれる. それゆゑ, 名城大学の数学科の講義で, きちんと取り上げておく意味はあるだらうと判断し採用した.

大西 良博

文 献

[N] 永尾 汎（ひろし）: 代数学 （新数学講座 4), 1983 年, 朝倉書店

[Iy] 彌永 昌吉（いやながしょうきち）, 有馬 哲（ありまさとし）, 浅枝 陽（あさえだあきら）: 詳解 代数入門, 1990 年, 東京図書

[A] Emil Artin : Galois theory, 1942, University of Notre Dame press
(日本語訳　エミール・アルティン 著 : ガロア理論入門, 2010, ちくま学芸文庫, 寺田 文行 訳)

[F] 藤﨑 源二郎 : 体と Galois 理論（岩波基礎数学選書), 1991 年, 岩波書店

[M] 松村 英之 : 可換環論（共立講座 現代の数学 4), 1980 年, 共立出版

目 次

記号や言葉の約束

この講義録では以下の慣用的な記号や言葉使ひを用ゐる.

(1) $\mathbb{N}$ で自然数（正の整数）の全体, $\mathbb{Z}$ で整数環, $\mathbb{Q}$ で有理数体, $\mathbb{R}$ で実数体, $\mathbb{C}$ で複素数体を表す.

(2) 多項式 $f(x)$ に対し $f(x)=0$ の根（あるいは解）を単に $f(x)$ の根（あるいは解）と呼ぶことが多い（8.1 を見よ）.

(3) 集合 B とその部分集合 $A \subset B$ および C と写像 $\sigma : B \to C$ について, $\sigma|_A$ で σ の定義域を A に制限した写像（制限写像）を表すものとする.

(4) 集合 A に対し $\#A$ でその要素の個数（濃度）を表す.

第1章　環についての準備

§1.　環と体の概念, 環の準同型

はじめに, 環と体の概念を思ひ出しておく.

定義 1.1. 集合 R が次の 4 つの条件を満たすとき, R は 環 と呼ばれるのであつた.
R0. 加法と呼ばれる演算 $R\times R\to R$, $(a,b)\mapsto a+b$, 及び乗法と呼ばれる演算 $(a,b)\mapsto ab$ が与へられてゐる. これらについて以下が成り立つ. 但し, a, b, c は R の任意の元である.
R1. R は加法に関して可換群である.
（通常, 加法の単位元 (一意的に存在) を 0_R や 0 で表し, $a\in R$ の逆元は $-a$ で表す.）
R2. 乗法の結合法則：$(ab)c=a(bc)$.
R3. 左右の分配法則：$a(b+c)=ab+ac$, $(b+c)a=ba+ca$.

定義 1.2. 環 R が次の性質を有するとき, R は 単位的環 と呼ばれる :
R4. ある元 $1=1_R\in R$ が存在して, R の任意の元 x に対して $1x=x1=x$ が満たされる.

問 1.3. 次の問に答えよ.
(1) 環 R の任意の元 a, $b\in R$ について $0a=a0=0$, $-ab=(-a)b=a(-b)$ となることを示せ.
(2) 単位的環 R に対し, 乗法の単位元は唯 1 つだけしか存在しないことを示せ.

問 1.4. 環 R の加法の単位元と乗法の単位元が一致する場合, 即ち $0=1$ のとき, $R=\{0\}$ であることを示せ. この様な環を 零環 と呼ぶ.

以後, 単位的環においては $0_R\neq 1_R$ と仮定する. ゆゑに, 単位的環は少なくとも 2 つの元を有する.

定義 1.5. 環 R の 0 と異なる 2 元 a, b が $ab=0$ を満たすとき, a を 左零因子, b を 右零因子 と呼ぶ. 左零因子と右零因子をまとめて 零因子 と呼ぶ.

命題 1.6. 単位的環 R と a, $b\in R$ について, 以下の様に定める.
(1) $aa^{-1}=a^{-1}a=1$ となる $a^{-1}\in R$ があれば, それを a の（乗法に関する）逆元といふ.
(2) a が乗法に関する逆元を持つとき, a は R の 単元 または 単数 と呼ばれる. R の単元全体のなす集合を $R^\times$ と記す. $R^\times$ はもちろん乗法に関して群をなす. $R^\times$ を R の 単数群 と呼ぶ.

例 1.7. 全成分が有理数である様な n 次正方行列の全体 $\mathrm{Mat}(n,\mathbb{Q})$ は通常の演算で単位的環環となる. 零行列が加法に関する単位元であり, 単位元が単位行列が乗法に関する単位元である. 単数群は

$$\mathrm{GL}(n,\mathbb{Q})=\{A\in\mathrm{Mat}(n,\mathbb{Q})\,|\,\det(A)\neq 0\}\quad\text{（但し det は行列式をとることを意味する）}$$

である. これは $\mathbb{Q}$ 上の n 次一般線形群 と呼ばれる.

定義 1.8. 単位的環 R がさらに, 次の条件も満たすとき R は 可換環 と呼ばれる :
R5. 乗法の交換法則 : 任意の $a, b \in R$ について $ab = ba$.

定義 1.9. 0 以外のどの元も乗法に関する逆元を持つ単位的環を 斜体 といふ. 零因子を持たない可換環を 整域 と呼ぶ. 零環は整域でないものとする. 斜体が可換環でもあるとき, それを 体 と呼ぶ. 従つて, 体は整域でもある. 我々の定義では, 零環は整域でも体でもないことに注意せよ.

問 1.10. 斜体について答へよ.
(1) 斜体は零因子を持たないことを示せ.
(2) 斜体の 0 以外の各元について, 乗法の逆元は唯 1 つしか存在しないことを示せ.

例 1.11. (1) $\mathbb{Z}$ や Gauss 整数環 $\mathbb{Z}[i]$ は, 通常の演算に関して, 整域であるが体ではない.
(2) $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}$ （但し p は素数）はどれも, 通常の演算に関して, 体である.
(3) 剰余類環 $\mathbb{Z}/6\mathbb{Z}$ は, 通常の演算に関して, 可換環であるが整域ではない.
(4) 次の環 $\mathbb{H}$（Hamilton の四元数体）は斜体であるが可換環ではない.

$$\mathbb{H} = \left\{ \begin{bmatrix} a+bi & c+di \\ -c+di & a-bi \end{bmatrix} \middle| a, b, c, d \in \mathbb{R} \right\} \quad (i \text{ は虚数単位で, 演算は通常のもの}).$$

定義 1.12. 環 R の部分集合 A が **R0** と **R1** を満たすとすると, **R2** と **R3** は自動的に A について成り立つことに留意せよ. つまり A も環である. この場合 A を R の 部分環 であるといふ. さらに R が単位的環（つまり, **R4** を満たす）ならば, 部分環の定義に **R4** も課すものとする. 単位的環 R が **R5** を満たしてゐれば, その部分環 A も **R5** を満たし, A は可換環である.

次に定義する可換環は重要である.

定義 1.13. R を可換環とし, $x_1, \cdots, x_m$ を m 個の 形式的な文字 として, （不定元 と呼ばれる）とする. 係数のすべてが R に属する様な, $x_1, \cdots, x_m$ の多項式の全体は

$$R[x_1, \cdots, x_n]$$

と表記され, 自然な和と積に関して可換環となるが, これは R 上の m 変数多項式環 と呼ばれる. 単項式 $a {x_1}^{k_1} \cdots {x_m}^{k_m} \in R[x_1, \cdots, x_n]$ $(a \in R, \neq 0)$ の 次数 を $k_1 + \cdots + k_m$ と定める. 多項式 $f(x_1, \cdots, x_m)$ に含まれる (0 でない) すべての項を渡つての次数の最大値を, $f(x_1, \cdots, x_m)$ の 次数 と呼び, $n = \deg f(x_1, \cdots, x_m)$ で表す. 特に m が 1 のときに $x_1 = x$ と書くことにすると, $f(x) = c_0 x^n + c_1 x^{n-1} + \cdots + c_n \in R[x]$, $c_0 \neq 0$ のとき, 多項式 $f(x)$ の 次数 は n のことに他ならない. この場合に $f(x)$ は n 次式 であるといひ, $n = \deg f(x)$ で表はす. R が体 K である場合は $K[x]$ を単に 多項式環 とも呼ぶことが多い.
さらに, 一般に, 可換環 B とその部分環, および $a_1, \cdots, a_r \in B$ にてついて, B の部分環

$$A[a_1, \cdots, a_r]$$

を. . . 定義.

ここで, 環から環への写像について以下の定義をする.

定義 1.14. 環 R から環 T への写像 $\varphi : R \to T$ が 2 つの条件
H1. 任意の $a, b \in R$ に対し, $\varphi(a+b) = \varphi(a) + \varphi(b)$,
H2. 任意の $a, b \in R$ に対し, $\varphi(ab) = \varphi(a)\varphi(b)$
を満たすとき φ は 環準同型 といはれる. **H2** より $\varphi(1)^2 - \varphi(1) = 0$ ゆゑ, T が整域であれば, $\varphi(1) = 1$ または $\varphi(1) = 0$ である. (R と T の加法と乗法の単位元を同じ記号 0, 1 で書いてゐる.)

問 1.15. 環 R の 1 を環 T の 0 に写す環準同型は, 環 R のあらゆる元を環 T の 0 に写すことを示せ. この様な写像を 零写像 と呼ぶ.

定義 1.16. 環 A から環 B への準同型が全単射であるときそれを（環の）同型 と称する. 同型の逆写像は同型である. 環 A から環 B への同型が存在するとき, 記号で $A \simeq B$ と表す.

定義 1.17. 環 R の空でない部分集合 $I \subset R$ は 2 つの条件
I1. $a \in I$, $b \in I$ ならば $a + b \in I$,
I2. $a \in I$, $x \in R$ ならば $xa \in I$
を共に満たすとき, R の 左 ideal と呼ばれる. また $I \subset R$ が, 上記 **I1** と
I3. $a \in I$, $x \in R$ ならば $ax \in I$
を共に満たすとき, R の 右 ideal と呼ばれる.
I が左 ideal かつ右 ideal であるとき I は R の 両側 ideal 或いは, 単に ideal と呼ばれる.

問 1.18. 単位的環 R の左 ideal (或いは右 ideal) I について, $I \ni 1 \iff I = R$ であることを示せ.

命題–定義 1.19. 以下, 環 A から環 B への準同型 φ について述べる.
(1) 部分集合 $S \subset A$ について $\varphi(S) = \{ f(x) \,|\, x \in S \}$ を φ による S の 像 と呼ぶ. $S = A$ のときは $\mathrm{Im}(\varphi) = \varphi(A)$ なる記号も使はれ, これは単に φ の 像 と呼ばれる.
(2) 上記 (1) において S が A の左 ideal, 右 ideal, または両側 ideal I である場合, $\varphi(I)$ は, それぞれ, B の左 ideal, 右 ideal, または両側 ideal である.
(3) 部分集合 $T \subset B$ について $\varphi^{-1}(T) = \{ x \in A \,|\, \varphi(x) \in T \}$ を φ による T の 逆像 と呼ぶ. $T = \{0\}$ のときは $\mathrm{Ker}\,\varphi = \varphi(\{0\})$ と書かれて, これは φ の 核 と呼ばれる.
(4) 上記 (3) において T が B の左 ideal, 右 ideal, または両側 ideal J である場合, $\varphi^{-1}(J)$ は, それぞれ, A の左 ideal, 右 ideal, または両側 ideal である.
特に $\mathrm{Ker}\,\varphi$ は A の両側 ideal である.

問 1.20. 上の 1.19 の主張の部分 (2), (4) を証明せよ.

定理 1.21. （準同型定理）環 A から環 B への準同型 φ から, 誘導される写像
$$\overline{\varphi} : x + \mathrm{Ker}\,\varphi \mapsto \varphi(x)$$
によつて, 下記の同型が得られる :
$$A/\mathrm{Ker}\,\varphi \simeq \mathrm{Im}(\varphi).$$

証明 1.19(4) より $\mathrm{Ker}\,\varphi$ は A の両側 ideal であり, 剰余類環 $A/\mathrm{Ker}\,\varphi$ が定義される. この写像が全射であることは明らかであり,
$$x + \mathrm{Ker}\,\varphi = y + \mathrm{Ker}\,\varphi \iff x - y \in \mathrm{Ker}\,\varphi \iff \varphi(x - y) = 0 \iff \varphi(x) = \varphi(y)$$

だから, 写像は問題なく定義され, 単射であることもわかる. 加法に関して

$$\begin{aligned}\overline{\varphi}\big((x+\operatorname{Ker}\varphi)+(y+\operatorname{Ker}\varphi)\big) &= \overline{\varphi}(x+y+\operatorname{Ker}\varphi) = \varphi(x+y) = \varphi(x)+\varphi(y)\\ &= \overline{\varphi}(x+\operatorname{Ker}\varphi)+\overline{\varphi}(y+\operatorname{Ker}\varphi)\end{aligned}$$

によつて **H1** が成り立つ. ここまでは（加法に関しての）群の準同型定理を得る過程と全く同じである. さて, 乗法に関しては

$$\begin{aligned}\overline{\varphi}\big((x+\operatorname{Ker}\varphi)(y+\operatorname{Ker}\varphi)\big) &= \overline{\varphi}\big((xy+\operatorname{Ker}\varphi)\big) = \varphi(xy) = \varphi(x)\varphi(y)\\ &= \overline{\varphi}(x+\operatorname{Ker}\varphi)\,\overline{\varphi}(y+\operatorname{Ker}\varphi)\end{aligned}$$

であるから **H2** も成り立つ. よつて $\overline{\varphi}$ は環の準同型でもある. □

定義 1.22. R を整域とする. 記号 $\frac{a}{b}$（$a\in R, 0\neq b\in R$）の全体 S に関係 $\frac{a}{b}\sim\frac{a'}{b'}$ を $ab'-a'b=0$ で定めるとこれは同値関係になり, これによる分類で得られる集合 $S/\sim$ は和 $\frac{a}{b}+\frac{a'}{b'}=\frac{ab'+a'b}{bb'}$, 積 $\frac{a}{b}\frac{a'}{b'}=\frac{aa'}{bb'}$ に関して体をなし, $\frac{a}{1}$ と $a\in R$ を同一視することで R は $S/\sim$ の部分環になる. $S/\sim$ を R の <u>商体</u> または <u>分数体</u> と呼び, $S=\operatorname{frac}(R)$ と記す. S は整域 R を含む最小の体に他ならない.

演 習 問 題

1.23. 以下の問に答へよ. 但し, $\mathbb{Q}(\sqrt{2})\cap\mathbb{Q}(\sqrt{3})=\mathbb{Q}$ であることを既知としてよい.

(1) 次の 2 つは通常の演算で体となることを示せ：

$$\mathbb{Q}(\sqrt{2})=\{\,a+b\sqrt{2}\,|\,a,\ b\in\mathbb{Q}\},\qquad \mathbb{Q}(\sqrt{3})=\{\,a+b\sqrt{3}\,|\,a,\ b\in\mathbb{Q}\}.$$

(2) $\mathbb{Q}(\sqrt{3})$ からそれ自身への零写像以外の環準同型を 2 つ挙げよ.

(3) $\mathbb{Q}(\sqrt{2})$ から $\mathbb{Q}(\sqrt{3})$ への環準同型は零写像に限ることを示せ.

1.24. i を虚数単位とし, $\mathbb{D}=\left\{\left[\begin{array}{cc} a+bi & c+di\\ -c+di & a-bi\end{array}\right]\middle|\, a,b,c,d\in\mathbb{Q}\right\}$ とする.

(1) $\mathbb{D}$ は通常の演算で斜体をなすことを示せ：

(2) <u>Gauss 数体</u> $\mathbb{Q}(i)$ から $\mathbb{D}$ への零写像ではない環準同型を 3 つ求めよ.

1.25. 有理数を成分とする 4 次正方行列

$$I=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix},\quad B=\begin{bmatrix}0&0&-1&0\\0&0&0&1\\1&0&0&0\\0&-1&0&0\end{bmatrix},\quad C=\begin{bmatrix}0&2&0&0\\-1&0&0&0\\0&0&0&2\\0&0&-1&0\end{bmatrix}$$

について,

$$\mathbb{T}=\{\,aI+bB+cC+dBC\,|\,a,b,c,d\in\mathbb{Q}\,\}$$

とおく. これについて次の問に答へよ.

(1) $B^2=-I$, $C^2=-2I$, $BC=-CB$, $(BC)^2=-2I$ であることを示せ.

(2) $\mathbb{T}$ は I, B, C, BC を基とする $\mathbb{Q}$ 上の 4 次元 vector 空間であることを示せ.

(3) $\det(aI+bB+cC+dBC)=(a^2+b^2+2c^2+2d^2)^2$ であることを示せ.

(4) $\mathbb{T}$ は行列の通常の演算で斜体になることを示せ.

(5) 体 $\mathbb{Q}(\sqrt{-2})=\{\,a+b\sqrt{-2}\,\big|\,a,b\in\mathbb{Q}\}$ から $\mathbb{T}$ への零写像でない環準同型を 3 つ求めよ.

§2. 環上の加群

ここでは環上の加群について述べる. これは ideal の概念の一般化でもある.

定義 2.1. 集合 M に演算 $M\times M\to M$, $(m,m')\mapsto m+m'$ が定義されてゐるとせよ. このとき M が加群[1] であるとは, これが Abel 群（可換群）であることである. この術語の意味は「M は群であるが演算を加法の記号 "+" で表す」といふだけのものであるが, 歴史的な理由があり, 敢てこの術語を用意する. また, 以下で環上の加群を定義した後は環 $\mathbb{Z}$ 上の加群と理解することができる.

定義 2.2. 環 A, B と 加群 M が与へられたとせよ. このとき, 以下の様に定義する.
(1) 写像 $\varphi\colon A\times M\to M$, $(a,m)\mapsto am$ が定められてゐて, 次の性質 ${}_A\mathbf{M1}$ から ${}_A\mathbf{M4}$ の全てが満たされてゐるならば, M は左 A 加群, A 左加群, あるいは環 A 上の左加群 などと称され, 写像 φ は A の M への左作用 と称される :
${}_A\mathbf{M1}$. 任意の $a\in A$ と任意の m, $m'\in M$ について $a(m+m')=am+am'$,
${}_A\mathbf{M2}$. 任意の a, $a'\in A$ と任意の $m\in M$ について $(a+a')m=am+a'm$,
${}_A\mathbf{M3}$. 任意の a, $a'\in A$ と任意の $m\in M$ について $(aa')m=a(a'm)$,
${}_A\mathbf{M4}$. 任意の $m\in M$ について $1m=m$.
(2) 写像 $\psi\colon M\times B\to M$, $(m,b)\mapsto mb$ が定められてゐて, 次の性質 $\mathbf{M}_B\mathbf{1}$ から $\mathbf{M}_B\mathbf{4}$ の全てが満たされてゐるならば, M は右 B 加群, B 右加群, あるいは環 B 上の右加群 などと称され, 写像 ψ は B の M への右作用 と称される :
$\mathbf{M}_B\mathbf{1}$. 任意の $b\in B$ と任意の m, $m'\in M$ について $(m+m')b=mb+m'b$,
$\mathbf{M}_B\mathbf{2}$. 任意の b, $b'\in R$ と任意の $m\in M$ について $m(b+b')=mb+mb'$,
$\mathbf{M}_B\mathbf{3}$. 任意の b, $b'\in R$ と任意の $m\in M$ について $m(bb')=(mb)b'$,
$\mathbf{M}_B\mathbf{4}$. 任意の $m\in M$ について $m1=m$.
(3) M が左 A 加群であると同時に右 B 加群であつて, それらの右作用と左作用が互換であるとき, 即ち, 条件
${}_A\mathbf{M}_B$ 任意の $a\in A$ と任意の $b\in B$ と任意の $m\in M$ について $(am)b=a(mb)$
が成り立つとき, M は両側 (A,B) 加群, あるいは (A,B) 両側加群 などと称される.

注意 2.3. M が左 A 左加群のとき, 以下のことが成り立つ.
(1) ${}_A\mathbf{M1}$ において $m=m'=0_M$ とすることで, $a\,0_M=0_M$ （$\forall a\in A$）であることがわかる.
(2) ${}_A\mathbf{M2}$ において $a=a'=0_A$ とおけば, $0_A\,m=0_M$ （$\forall m\in M$）であることがわかる.
(3) ${}_A\mathbf{M1}$ と ${}_A\mathbf{M2}$ を無視すれば, M は乗法群 $A^\times$ の (左からの) 作用域（34.1 を参照）であるとも考へられる.
(4) $I\subset A$ が左 ideal であることは, I が左 A 加群であることに他ならない.
もちろん, 以上のことは右 B 加群についても, 同様である.

[1] Abel 群を表す英語は Abelian group, 可換群を表す英語は commutative group, 加群を表す英語は module である.

§ 3. 可換環の ideal と剰余類環

素 ideal と極大 ideal の概念について述べる.

定義 3.1. 可換環においては, 左 ideal, 右 ideal, 両側 ideal の概念 (定義は 1.17 にて) は, もちろん同一のもの (ideal) となる. R を可換環とする. いま R の ideal P が, $P \subsetneqq R$ および
P. 任意の $a, b \in R$ に対し, $ab \in P \iff a \in P$ または $b \in P$ である;
を満たすとき P は素 ideal といはれる. また, R の R と異なる ideal M について, M を真に含む ideal が R に限るとき, M は極大 ideal であるといはれる.

問 3.2. 可換環 R の ideal I について答へよ.
(1) $I \ni 1 \iff I = R$ であることを示せ.
(2) 任意の $a \in R$ に対し, 集合 $aR + I$ も ideal であることを示せ.

問 3.3. 可換環 R の ideal I について, I が極大 ideal であることと $a \notin I \Rightarrow aR + I = R$ が成り立つこととは同値であることを示せ.

問 3.4. 可換環 R, T に対し, 環準同型 $\varphi : R \to T$ の核 $\mathrm{Ker}\,\varphi = \{a \in R \mid \varphi(a) = 0\}$ は R の ideal であることを示せ.

問 3.5. 体の ideals は $\{0\}$ とその体自身の 2 つだけであることを示せ.
(($\{0\}$ は 0 の生成する ideal であるから, 通常 (0) と書かれる.))

ここで, 剰余類環を定義する.

命題 3.6. 可換環 R とその ideal I から定まる, 加法に関する剰余類[2] R/I について

$$(a + I) + (b + I) = a + b + I,$$
$$(a + I)(b + I) \subset ab + I \quad (\text{一般に, 集合としては等しくならない})$$

が成り立つ. それゆゑ R/I に加法と乗法をそれぞれ

$$(a + I) + (b + I) = a + b + I, \quad (a + I)(b + I) = ab + I$$

を定めることができる. これにより R/I は可換環になる. 但し, 加法の単位元は I であり, 乗法の単位元は $1 + I$ である.

証明 第 2 式は $(a + I)(b + I) = ab + aI + bI + I^2 \subset ab + I$ となつて正しい. これ以外については, ほぼ明らかであらうから省略する. □

例 3.7. $m \in \mathbb{N}$ とする. 剰余類環 $\mathbb{Z}/m\mathbb{Z}$ については「代数学 1」で学んだ. これの単数群 $(\mathbb{Z}/m\mathbb{Z})^\times$ は $\{a + \mathbb{Z} \mid 1 \leqq a \leqq m - 1,\ \gcd(a, m) = 1\}$ から成り, 法 m の既約剰余類 と呼ばれる. これの要素の個数は $\#(\mathbb{Z}/m\mathbb{Z})^\times = \varphi(m)$[3] である.

問 3.8. 可換環 R とその ideal I について, 写像 $\rho : R \to R/I,\ a \mapsto a + I$ が環準同型であることを示せ. また $\mathrm{Ker}(\rho)$ は何か.

次の命題は, 次章で頻繁に使はれる.

---

[2] $x, y \in R$ について $x - y \in I$ といふ関係が同値関係であることは簡単にわかる. この関係による類別を ideal I による剰余類と称して R/I と書く.
[3] $n \mapsto \varphi(n)$ は Euler の totient 函数.

命題 3.9. 可換環 R の ideal I による剰余類環 R/I について次が成り立つ.
(1) R/I が整域であるためには I が素 ideal であることが必要十分である.
(2) R/I が体であるためには I が極大 ideal であることが必要十分である.

証明 $a \in R$ の属する R/I の類 $a+I$ を $\overline{a}$ と書く. (1) は 3.10 の問とし, (2) のみ示す.
（十分性） $a \in R$ について

$$\begin{aligned}
\overline{a} \neq \overline{0} &\iff a+I \neq I \iff a \notin I \\
&\Longrightarrow aR+I = R \quad (\because 3.3) \\
&\iff aR+I \ni 1 \quad (\because 3.2\ (1)) \\
&\iff af+g=1 \text{ となる } f \in R,\ g \in I \text{ が存在} \\
&\iff \overline{a}\,\overline{f} = \overline{1} \text{ となる } \overline{f} \in R/I \text{ がある} \iff \overline{a} \text{ は乗法に関して逆元を持つ}
\end{aligned}$$

となるからである. （必要性） I が極大 ideal でなければ, 3.3 により, $a \notin I$ かつ $aR+I \neq R$ なる ideal a が存在するが, 前者より $\overline{a} \neq \overline{0}$ で, 後者と 3.2 より $aR+I \not\ni 1$ であるから, $\overline{a}\,\overline{f} = \overline{1}$ なる f は存在しない. つまり $\overline{a}$ は乗法の逆元を持たない. □

問 3.10. 3.9 (1) を証明せよ.

演 習 問 題

3.11. 可換環 R の ideal I および部分環 A について次の問に答へよ.
(1) $A+I$ が R の部分環であることを示せ.

3.12. n を自然数とせよ. 法 n による剰余類環 $\mathbb{Z}/n\mathbb{Z}$ が体であるためには, n が素数であることが必要十分である. これを示せ.

3.13. 有理数係数の多項式の全体 $\mathbb{Q}[x]$ は通常の演算で可換環をなす. この可換環から体 $\mathbb{Q}(\sqrt{2}\,)$ への環準同型で, その核が ideal (x^2-2) であるものを全て求めよ.

§ 4. 約元と倍元, 素元と既約元

次の様に定義する.

定義 4.1. R の 可換環とする.
(1) $a, b \in R, b \neq 0$ について, $a = bc$ となる $c \in R$ が存在するとき, a は b で割り切れる, a は b の倍元, b は a を割る, b は a の約元, などと称する. このことを記号で $b \mid a$ と記す.
(2) $a, b \in R, b \neq 0$ について, 特に $c \in R^\times$ によつて $a = cb$ であるとき a と b は同伴であるといはれ, 記号 $a \sim b$ で表す. この関係は同値関係である (下記の 4.2).
(3) 0 でもなく, 単元でもない $p \in R$ について次の様に定める.
下記の条件 **Irr** が成り立つとき p は既約元, あるいは既約であるといはれ, 満たされないときは可約元 または 可約であるといはれる.
Irr. 任意の $a \in R$ について, $a \mid p$ ならば $a \sim p$ または $a \in R^\times$.
(4) 0 でもなく, 単元でもない $p \in R$ について次の様に定める.
下記の条件 **Pr** が成り立つとき p は素元であるといはれる.
Pr. 任意の $a, b \in R$ について, $p \mid ab$ ならば $p \mid a$ であるか $p \mid b$ である.

問 4.2. R を可換環とする. R における同伴は同値関係であることを示せ.

問 4.3. R を整域とする. R の 2 つの ideal (a), (b) について, 次が成り立つことを示せ:

$$(a) \subset (b) \iff b \mid a.$$

例題 4.4. (1) 可換環 R の元 $a, b \neq 0$ について, a と b が同伴ならば $a \mid b$ かつ $b \mid a$ である.
(2) もし R が整域ならば (1) の逆も正しい. R が整域でないと逆は正しくない (7.8(1)〜(3) を見よ).

解答 (前半). 仮定より $b = ac$ ($c \in R^\times$) と書けるが, $c^{-1} \in R^\times$ であり, $a = bc^{-1}$ なので $b \mid a$ である.
(後半). $b = ac$, $a = bc'$ と書けてゐれば, $b = bcc'$ であり, $b(1 - cc') = 0$ である. R が整域であれば $1 - cc' = 0$ ゆゑ $cc' = 1$ であるから, c と c' は単元である. よつて a と b は同伴である. □

命題 4.5. 整域においては素元は既約元である.

証明 R を整域, $p \in R$ ($\notin R^\times, \neq 0$) を R の素元として, $a \mid p$ とする. このとき $ab \in (p)$ となるから, $a \in (p)$ または $b \in (p)$ である. ゆゑに $p \mid a$ または $p \mid b$. もし $p \mid a$ であれば 仮定 $a \mid p$ と合はせて, 4.4 から $a \sim p$. もし $p \mid b$ であれば $b = pc$ と書ける. このとき $p = ab = apc = acp$. R は整域で $p \neq 0$ なので $1 = ac$ となり a は単元である. 以上より p が既約元である. □

注意 4.6. (1) 整域においても, 必ずしも既約元は素元とは限らない. 7.7 を見よ.
(2) 整域でない可換環で素元なのに既約元でない元の例.
7.8(4) を見よ.

命題 4.7. 可換環 R と元 $p \in R$ ($p \neq 0$) について, (p) が素 ideal $\iff$ p は素元.

証明 まづ $a \mid p \iff a \in (p)$ である. 実際, $a \in (p) \iff (\exists b \in R, p = ab) \iff a \mid p$ であるから. これにより, (p) が素 ideal であることの定義は直ちに p が素元であることの定義に書き直される. □

§5. Noether 加群, Noether 環（と Artin 加群, Artin 環）

以下では R を環として, 左 R 加群についてのみ述べるが, 右 R 加群についても同様である.

命題 5.1. 環 R と R 加群 M について, 次の (1) 〜 (3) は互ひに同値である.
(1) （昇鎖律）M の部分 R 加群からなる増加する任意の無限列 $N_1 \subset N_2 \subset \cdots$ について, ある $m \in \mathbb{N}$ が存在して $N_m = N_{m+1} = N_{m+2} = \cdots$ が成り立つ.
(2) M の部分 R 加群からなる空でないどんな集合も（包含関係に関して）極大元を含む.
(3) M のどの部分 R 加群も R 上有限生成である.

証明 （ここは [Iy], p.226 に従つて述べる）(1) $\Rightarrow$ (2). 対偶を示す. 極大元を含まないその様な集合 $\mathscr{M}$ があれば, 極大元の定義から $N_1 \subsetneqq N_2 \subsetneqq \cdots$ を満たす様な部分集合 $\{N_j\} \subset \mathscr{M}$ が存在する.
(2) $\Rightarrow$ (3). N を M 任意の任意の部分 R 加群とせよ. いま

$$\mathscr{M} = \{\, L \subset M \,|\, L \text{ は } L \subset N \text{ なる } M \text{ の有限生成部分 } R \text{ 加群} \,\}$$

とおく. $\{0\} \in \mathscr{M}$ ゆゑ $\mathscr{M} \neq \varnothing$ である. 仮定より, $\mathscr{M}$ の極大元が存在するので, それを M_0 とする. $M_0 = N$ であれば証明は終はるから, $M_0 \subsetneqq N$ としやう. 元 $x \in N, \notin M_0$ をとり, $M_0 + Rx$ を考へると R 上有限生成で $M_0 \subsetneqq M_0 + Rx \subset N$ となる. これは M_0 が極大元であることに反する.
(3) $\Rightarrow$ (1). 任意に与へられた部分 R 加群の増加列 $N_1 \subset N_2 \subset \cdots$ について $N = \bigcup_{i=1}^{\infty} N_i$ とおく. 仮定より N は R 上有限生成である. よつて $N = Rb_1 + R_2 + \cdots + Rb_r$ の形に書かれる. 各 $1 \leqq j \leqq r$ に対し $b_j \in N_{n_j}$ なる N_{n_j} が存在するが, $n_1, \cdots, n_r$ の最大値を m とすれば, すべての b_j が N_m に属し, $N \subset N_{n_1} + \cdots + N_{n_r} \subset N_m \subset N$, つまり $N_m = N$ となる. $n \geqq m+1$ ならば, $N_m \subset N_n$ なのであるから, やはりすべての b_j が N_n に属するので, 同じ議論で $N_n = N$ であり, $N_m = N_{m+1} = \cdots$ となつてゐる. □

定義 5.2. 環 R に対して, 次の様の定義をおく.
(1) 5.1 で述べた同値な条件を満たす R 加群を Noether R 加群 と呼ぶ.
(2) R 自身を R 加群とみて Noether R 加群であるとき, R を Noether 環 と呼ばれる.

注意 5.3. 環 R を R 加群とみたとき, その部分 R 加群は R の ideals に他ならない（2.3(4)）から, R が Noether 環であるといふことは以下の同値な条件のいづれかを満たすことに他ならない.
(1) （昇鎖律）M の ideals からなる増加する任意の無限列 $I_1 \subset I_2 \subset \cdots$ について, ある $m \in \mathbb{N}$ が存在して $I_m = I_{m+1} = I_{m+2} = \cdots$ が成り立つ.
(2) M の ideal(s) からなる空でないどんな集合も（包含関係に関して）極大元を含む.
(3) M のいかなる ideal も R 上有限生成である.

以下の主張は, 上のことから言ふまでもないが, 引用の便宜のため 5.1 の系として述べておく.

系 5.4. 環 R が左 Noether 環であるためには, R の任意の左 ideal が R 上に有限生成であることが必要十分である. 特に PID（後述） は Noether 環である.

§ 6. 単項 ideal 環

定義 6.1. 可換環 R について, 次の様に定義する.
(1) I を R の ideal とする. I が 1 つの元 a の倍元の全体 aR に一致するとき, I を a で生成された 単項 ideal と称し, $I=(a)$ と略記する.
(2) R のすべての ideal が単項 ideal であるとき, R は 単項 ideal 環 と称される.
(3) R が単項 ideal 環でかつ整域であれば, R は 単項 ideal 整域 または PID[4] と呼ばれる.

命題 6.2. PID においては, 既約元はすべて素元である. 従つて PID においては既約元と素元の概念が一致する.

証明 前半を示すために, R を任意の PID とし, q を R の既約元とせよ. いま $a, b\in R$ について $q|ab$ であるとすれば, ideal (a,q) が単項であるので, ある $c\in R$ によつて $(a,q)=(c)$ と書ける. とくに $c|q$ である. q は既約元なので **Irr** によつて $q\sim c$ または $c\in R^\times$. 前者であれば $(a,q)=(c)=(q)$ ゆゑ $q|a$ である. 後者であれば $ax+qy=1$ ゆゑ $abx+qby=b$. 仮定 $q|ab$ とあはせて, $q|b$ である. 以上から q は素元である. 後半は, PID がそもそも整域であることと, 4.5 から従ふ. □

命題 6.3. PID の任意の ideal I について, I が素 ideal $\iff$ I が極大 ideal.

証明 R を PID であるとし, (p) を R の素 ideal とせよ. 任意に $(p)\subset I\subset R$ なる ideal I を考察する. R は PID ゆゑ, $I=(a)$ と書ける. よつて $p=ac$ と書ける. p は素元なので 4.5 より既約元でもある. ゆゑに $a\in R^\times$ または $a\sim p$ である. いひ替へれば $I=(a)=R$ または $I=(a)=(p)$ である. つまり (p) は極大 ideal である. □

[3] 英語の principal ideal domain（単項 ideal 整域）の頭文字をとつたもの.

命題 6.4. R を PID とし, I を R の ideal とするとき, 剰余類環 R/I は一意分解環である. しかし, これは PID とは限らない.

証明 仮定より $I=(f)$, $f\in R$ と書ける. $J\subset R/I$ を R/I の任意の ideal とせよ. $\tilde{J}=\{a\in R\,|\,a+I\in J\}$（$J$ の 引き戻し）とおくと, 仮定より $\tilde{J}=(g)$, $g\in R$ と書ける. つまり J は元 $g+I\in R/I$ によつて生成された単項 ideal である :

$$J=gR/I=(g+I).$$

ちなみに $I\in J$ ゆゑ, もちろん $I\subset\tilde{J}$ であるから, 4.3 により $g\,|\,f$ である. このことから f の約元は有限個しかないから, $I=(f)\neq(0)$ であれば R/I は Artin 環であることもすぐわかる. また, もちろん I が素 ideal でなければ R/I は整域ではないから PID とはならない. □

注意 6.5. 上の結果と 5.4 によれば, 特に PID の剰余類環 Noether 環である. ちなみに, 一般に PID は Artin 環ではないが, 0 でない ideal による剰余類環は Artin 環でもある（[N], p.120, 例題 29.9 などを参照）.

定義 6.6. 整域 R があり, R から 整列集合[5] W（但し, 順序の記号は通常の $\leqq$, $<$ 等で表す）への写像 $o:R\to W$ が与へられてゐて, それが次の 2 つの性質を持つとする :
E1. $0\neq a\in R \implies o(0)<o(a)$,
E2. $0\neq a\in R$, $b\in R$ ならば

$$b=aq+r,\quad o(r)<o(a)$$

を満たす q, $r\in R$ が存在する.
このとき R は Euclid 整域であるといはれる. この状況で o を R に付随する 順序写像 と呼ぶことにする. Euclid 整域

例 6.7. Euclid 整域の例を挙げておく.
(1) 有理整数環 $\mathbb{Z}$ は Euclid 整域である. 但し, 整列集合 W としては通常の順序での $\{0\}\cup\mathbb{N}$ をとり, 写像 o としては $o(a)=|a|$ ととればよい.
(2) 体 K 上の多項式環 $K[x]$ は Euclid 整域である. 但し, 整列集合 W としては通常の順序での $\{-\infty,0\}\cup\mathbb{N}$ をとり, 写像 o としては $o(f(x))=\deg f(x)$ ととればよい. 但し $\deg 0=-\infty$. 即ち, 任意の $f(x)$, $g(x)\in K[x]$ に対し $q(x)$, $r(x)\in K[x]$ が一意的に存在して, 次が成り立つ :

(6.8) $$f(x)=g(x)\,q(x)+r(x),\quad \deg r(x)<\deg g(x).$$

ここで $\deg f(x)=-\infty \iff f(x)=0$（多項式としての 0）であることに注意せよ.

命題 6.9. Euclid 整域は PID である.

証明 R を Euclid 整域とする. 付随する順序写像を $o:R\to W$ とする. W の順序は通常の記法を用ゐる. I を R の任意の ideal とせよ. I の中の 0 でない元のうち, o の値が最小となるものを 1 つとり, それを p とせよ. ここで, $o(W)$ も整列集合であることに注意せよ. いま, 任意に $a\in I$ をとるとき, 仮定から

$$a=pq+r,\quad o(r)<o(p)$$

となる $r\in R$ が存在する. もし $r\neq 0$ であれば, $r=a-pq\in I$ なので, p の選び方に反する. よつて

[4] 付録の 33.6 とその例 33.7 を見よ.

$r = 0$ でなければならない. つまり $a \in (p)$ である. これは $(p) \supset I$ であることを示すが, もちろん $(p) \subset I$ なので $I = (p)$ である. 従つて I は単項 ideal である. これで主張が示された. □

例 6.10. $\mathbb{Z}$ や $K[x]$（但し K は体で x は不定元）は 6.7 により Euclid 整域であるから, 6.9 によつて, これらは PID でもある.

§7. 一意分解環

定義 7.1. 可換環 R が次を満たすとき R は一意分解環 または UFD[6] と呼ばれる.

U1.（分解の可能性）任意の $a \in R$（$a \neq 0, a \notin R^\times$）に対し, 既約元 $b_1, \cdots, b_m \in R$（有限個）が存在して, $a = b_1 \cdots b_m$ と表される.

U2.（分解の一意性）上記の表示は順序と同伴元の違ひを除いて一意的である. 即ち, もし $b_1, \cdots, b_m$, $c_1, \cdots, c_n \in R$ が既約元で, $b_1 \cdots b_m = c_1 \cdots c_n$ であつたならば, $m = n$ であつて, $b_1, \cdots, b_m$ と $c_1, \cdots, c_n$ は順序を入れ替へれば, 各 i について b_i と c_i は互ひに同伴になる.

問 7.2. 体は UFD であることを示せ.

例 7.3. 整域 $\mathbb{Z}[\sqrt{-5}\,]$ は UFD でない. 実際, $4 = (\sqrt{-5}+1)(\sqrt{-5}-1) = 2^2$ といふ様に 2 種類の分解が存在し, $(\sqrt{-5} \pm 1)$, 2 はどれも既約元である (7.7 も参考にされたい).

命題 7.4. 可換環 R が UFD であるためには, R の任意の元が既約元の積に分解され（つまり **U1** の成立), すべての既約元が素元であることが必要十分である.

証明 （必要性). UFD の定義より **U1** は成り立つ. いま $p \in R$ が既約元であるとし, $a, b \in R$ について $p|ab$ とする. このとき $c \in R$ が存在して, $pc = ab$ と書ける. **U1** を使つて, この右辺を既約元の積に分解し, 既約分解の一意性 **U2** を用ゐれば, $p|a$ または $p|b$ であることがわかる. よつて p は素元である.

（十分性). 既約分解の一意性 **U2** を示せばよい. いま $x \in R$ が 2 通りの既約元分解

$$q_1 q_2 \cdots q_r = p_1 p_2 \cdots p_s$$

を持つたとする. このとき $q_1 \,|\, p_1 p_2 p_3 \cdots p_s$ であるので, $q_1 \,|\, p_1$ または $q_1 \,|\, p_2 p_3 \cdots p_s$ である. 後者の場合は $q_1 \,|\, p_2$ または $q_1 \,|\, p_3 \cdots p_s$ である. 同様な議論を続ければ q_1 は $p_1, \cdots, p_s$ のいづれかを割り切る. q_1 は素元でもあるので, 番号を付け代へて $q_1 \,|\, p_1$ である. しかるに p_1 も既約元なので **Irr** により $q_1 \sim p_1$ である. R は整域なので, 上記の両辺を $q_1 = p_1$ で割ることができて,

$$u_1 q_2 \cdots q_r = p_2 \cdots p_s, \quad u_1 \in R^\times$$

と書ける. 以下 $q_2, \cdots, q_r$ について同様に進むことができるので, 最後に $r = s$ がわかり, $u_1, \cdots, u_r \in R^\times$ によつて, $u_1 u_2 \cdots u_1 = 1$ の形の積が得られる. これは既約分解の一意性 **U2** の成立を示してゐる. □

[5] 英語の unique factorization domain（一意分解整域）の頭文字をとつたもの.

命題 7.5. PID は UFD である.

証明 7.4 を用ゐて示さう. R を任意の PID とする. 6.2 により, R の任意の元の既約分解されることを示せばよい. これを背理法で示す. いま $a \in R$ が既約元の積に分解されないとする. このとき a は既約元ではあり得ないから $a_1 \,|\, a$ なる 0 と異なる $a_1 \notin R^\times$ が存在する. いま $a = a_1 b_1$ と書くとき,

$$(a) \subsetneqq (a_1), \quad (a) \subsetneqq (b_1)$$

である. a_1 と b_1 のどちらかは既約元の積には分解されないが, 必要ならば名前を付け替へて, 分解されない方を改めて a_1 と書く. 上記 a に対しての考察を a_1 ついて行ひ, さらに同様の議論を続ければ

$$(a) \subsetneqq (a_1) \subsetneqq (a_2) \subsetneqq \cdots$$

なる無限列が得られる. しかし, これは 5.4 の後半部分により, 矛盾である. [Iy], p.129, 問題 7(i). □

演 習 問 題

7.6. R を整域とし, $a, b, c \in R$ とする. a と b が同伴であれば $a|c \iff b|c$ である. これを示せ.

7.7. 可換環 $\mathbb{Z}[\sqrt{-5}\,]$ は整域である. この環において 2 は既約元であるが, 素元ではない. 以上のことを証明せよ. (Hint : $2 \,|\, (1+\sqrt{-5})(1-\sqrt{-5})$.)

7.8. x, y を不定元として $R = \mathbb{Q}[x,y]/(x - xy)$ について答へよ.
(1) R は整域でないことを示せ.
(2) R において $x|xy,\ xy|x$ であることを示せ.
(3) R において x と xy は同伴ではないことを示せ.
(4) $Y|X$ であるが, y は単元でなく x と同伴でもないので, 既約元でない.
しかし x は素元である. 以上のことを詳しく説明せよ.

7.9. R を UFD とする. 次の問に答へよ. ([Iy] p.128, 2.6.11 より.)
(1) x を不定元とする. $R[x]$ も UFD であることを示せ.
(2) $x_1, \cdots,, x_n$ が不定元であれば, $R[x_1, \cdots, x_n]$ も UFD であることを示せ.
以上のことと 7.2 より, 特に K が体であれば $K[x_1, \cdots, x_n]$ は UFD である.

7.10. $\mathbb{Z}[x]$ が UFD であることを示せ. また $\mathbb{Z}[x]$ は PIF でないことを示せ.

§8. 1 変数多項式環

ここでは 1 変数多項式環についてまとめておく.

定義 8.1. 体 K 上の多項式 $f(x)$ と元 $\alpha \in K$ について次の定義をする. (=「代数学 1」, 11.3)
(1) $f(x)$ の x に α を代入したものを $f(\alpha)$ と書く.
(2) $f(x) \neq 0$ で $f(\alpha) = 0$ であれば, α は $f(x)$ (あるいは $f(x) = 0$) の 根 であるといはれる. これは, 0 でない $g(x) \in K[x]$ が存在して $f(x) = (x-\alpha)\, g(x)$ と書けることに他ならない[7].
(3) さらにもし, $f(x) = (x-\alpha)^m g(x)$ ($m \in \mathbb{N}$) と書けて, $g(\alpha) \neq 0$ であるならば, α は $f(x)$ の m 重根 であるといはれる. また, このとき m は根 α の 重複度 と呼ばれる.

命題 8.2. 体 K 上の多項式 $f(x) \in K[x]$ について, $\deg f(x) = n \geqq 0$ ならば $f(x) = 0$ は K の中に, 重複度も込めて高々 n 個の根を持つ. (=「代数学 1」, 11.4)

証明 $f(x) = (x-\alpha)^{m_1} g_1(x)$ $(m_1 \in \mathbb{N})$ と書かれて $g_1(\alpha) \neq 0$ であるとき, $\deg f(x) = m_1 + \deg g_1(x)$ である. このとき $f(x)$ の別の根 α_2 は $g_1(x)$ の根でなければならず, $g_1(x) = (x-\alpha_2)^{m_2} g_2(x)$ $(m_2 \in \mathbb{N},\ g_2(\alpha_2) \neq 0)$ と書かれて, $\deg f(x) = m_1 + m_2 + \deg g_2(x)$ である. これを繰り返へせば $n = \deg f(x) \geqq m_1 + m_2 + \cdots$ となるから, 主張が成立する. □

命題 8.3. 体 K 上の多項式環 $K[x]$ のどんな素 ideal も極大 ideal である. $K[x]$ の ideal $(f(x))$ が素 ideal であるとき, $f(x)$ は 素元 である. 即ち $f(x) \,|\, g_1(x)\, g_2(x)$ $(g_1(x),\, g_2(x) \in K[x])$ であれば $f(x) \,|\, g_1(x)$ または $f(x) \,|\, g_2(x)$ である. また, このとき $f(x)$ は可換環 $K[x]$ の 既約元 である. 即ち, もし $f(x)$ が $f(x) = g_1(x) g_2(x)$ と表されたならば $g_1(x)$ か $g_2(x)$ のどちらかが K に属する. この様な $f(x)$ は K 上の既約多項式 と呼ばれる.

問 8.4. 6.10 及び 8.3 を証明せよ.

定義 8.5. 最高次係数が 1 である多項式を monic と称する.

定理 8.6. (Eisenstein の既約判定法) 整域 R の素元 p, および R の商体 K について以下が成り立つ. $f(x) = c_0 x^n + c_1 x^{n-1} + \cdots + c_n \in R[x]$ について, $p \nmid c_0$, $p | c_j$ $(1 \leqq j \leqq n)$, $p^2 \nmid c_n$ であれば $f(x)$ は $K[x]$ において既約である.

証明 □

[7] 従つて, 多項式として $f(x) = 0$ なら $f(\alpha) = 0$ であるが, α が $f(x)$ の根であるときは多項式として $f(x) \neq 0$ を前提としてゐることに注意されたい.

問 8.7. Monic な多項式 $f(x)\in\mathbb{Z}[x]$ が 2 つの monic な多項式 $g(x),\ h(x)\in\mathbb{Q}[x]$ によつて $f(x)=g(x)h(x)$ と書けるとき, $g(x),\ h(x)\in\mathbb{Z}[x]$ であることを示せ.

(Hint : 一般に $G(x)\in\mathbb{Z}[x]$ の係数の正の最大公約数を $\operatorname{cont}G(x)$ と書いて $G(x)$ の 内容 と呼ぶ. $G_1(x),\ G_2(x)\in\mathbb{Z}[x]$ について $\operatorname{cont}G_1(x)G_2(x)=\operatorname{cont}G_1(x)\cdot\operatorname{cont}G_2(x)$ である. これは Gauss の補題 の特殊な場合である. さて, $g(x)$ に対して, $bg(x)\in\mathbb{Z}[x]$ となる最小の b が存在する. 同様に $h(x)$ に対して, $cg(x)\in\mathbb{Z}[x]$ となる最小の c が存在する. このとき $bcf(x)=bg(x)ch(x)$ であるから, $\operatorname{cont}bcf(x)=\operatorname{cont}bg(x)\cdot\operatorname{cont}ch(x)$ であるが, $\operatorname{cont}bg(x)=\operatorname{cont}ch(x)=1$ であるから, $\operatorname{cont}bcf(x)=1$ である. 一方, $f(x)\in\mathbb{Z}[x]$ ゆゑ $bc\,|\operatorname{cont}bcf(x)$. これより $bc=1$ でなくてはならず, $b=c=1$ であることがわかる. これで主張は示された. 尚, [N], p.105 または [M] p.85, p.205 も参照されたい.)

定理 8.8. (Gauss の補題) R を UFD とし, $K=\operatorname{frac}(R)$ とおく. Monic な多項式 $f(x)\in R[x]$ が 2 つの monic な多項式 $g(x),\ h(x)\in K[x]$ によつて $f(x)=g(x)h(x)$ と書けるとき, $g(x),\ h(x)\in R[x]$ である.

証明 (Hint : 8.7 の内容の定義をこの場合に拡張せよ. 即ち $f(x)\in R[x]$ の係数の全体が生成する ideal を $\operatorname{cont}f(x)$ と定める. これにより, 8.7 の証明を辿ることができる.) □

演 習 問 題

8.9. p を素数とする. 多項式 $x^{p-1}+x^{p-2}+\cdots+x+1$ が $\mathbb{Q}$ 上既約であることを示せ.
(Hint : $x=y+1$ とし, y の多項式として Eisenstein の既約判定法 8.6 を利用.)

8.10. 多項式 $x^5-4x+2,\ x^5-x+1,\ x^5-4x-4$ は $\mathbb{Q}$ 上既約であるか. 理由をつけて答へよ.
(Hint : 3 を法として考へよ.)

第2章　体 論

§9.　部分体, 体の拡大

前節で定義した様に, この note 全体を通じて, 特に断らない限り 体の乗法は可換とする. もし, 非可換体に言及する場合は 非可換体 と明記し, 可換か非可換かを不問にするときは 斜体 と呼んで, 区別する. (環の場合も同様で, 単に環と呼ぶのは非可換の場合も含めてゐる)

定義 9.1. 環 R の部分集合 K が R の演算で体になつてゐるとき, K を R の 部分体 といふ. このとき, R は加法の単位元 0 と乗法の単位元 1 を有し, それらが K の加法と乗法の単位元でもある. 但し, 以後の多くのこの様な状況での R は体である.

問 9.2. 部分体についての次の問に答へよ.
(1) K_1, K_2 が体 L の 2 つの部分体のとき, $K_1 \cap K_2$ も L の部分体であることを示せ.
(2) 体 L とその部分体 M_1, M_2 で, $M_1 \cup M_2$ が L の部分体にならない例を挙げよ.
(3) 体 L と部分集合 S について S を含む L の最小の部分体の存在を示せ.
(Hint : S を含む L の部分体のすべての共通部分を考へて 9.2 (1) と同様に処理.)

定義 9.3. (1) K が体 L の部分体である場合, この関係を K から見て, L を K の 拡大体 と呼ぶ. 体 L が体 K の拡大体であることを, 以後簡単に, 拡大 L/K と称す. このとき, L は K 上の vector 空間 [8] とみなせるが, その次元 $\dim_K L$ を L/K の 拡大次数 と呼び $[L:K]$ で表す. 特に体の拡大 L/K において, その拡大次数 $[L:K] < \infty$ であるとき, L/K は 有限次拡大 であるといはれる. $[L:K] = 1$, つまり $L = K$ のとき, L/K を 自明な拡大 といふ. L の部分体 M, K について, $L \supset M \supset K$ であるとき, M を L と K の (あるいは拡大 L/K の) 中間体 といふ.
(2) $\alpha_i \in L$ $(i = 1,\ 2,\ 3,\ \cdots)$ とするとき, 集合 $\{\alpha_i \,|\, i = 1, 2, 3, \cdots\}$ を含む最小な体を, この集合で 生成された体 といふ. K を L の部分体とし, K のすべての元および $\{\alpha_i\}$ で生成された体を $K(\alpha_1, \alpha_2, \cdots)$ で表し, K に $\alpha_1,\ \alpha_2,\ \cdots$ を 添加 して得られる体と呼ぶ. 特に $L = K(\alpha_1, \alpha_2, \cdots, \alpha_n)$ の場合, L を K 上 有限生成 な体といふ [9]. 同様に, K のすべての元および $\{\alpha_1, \cdots, \alpha_n\}$ を含む最小の環が存在する. これを K と $\{\alpha_1, \cdots, \alpha_n\}$ で生成された環と呼び, $K[\alpha_1, \alpha_2, \cdots, \alpha_n]$ で表す.
(3) 1 つの元 α によつて $L = K(\alpha)$ となるとき, L を K の 単純拡大 (単拡大) といふ.

問 9.4. 元 α が体 K 上の既約多項式の根であるとき, $K(\alpha) = K[\alpha]$ となることを示せ.
(Hint: α が K 上既約な多項式 $f(x) \in K[x]$ の根であるとし, 任意の $g(x) \in K[x]$, $g(\alpha) \neq 0$, について $1/g(\alpha) \in K[\alpha]$ を示せばよい. このとき $g(x)$ と $f(x)$ が互ひに素であることを示し, この 2 多項式について互除法を行ふ.)

注意 9.5. 一般には $K(\alpha) \supset K[\alpha]$ であり, 一致するとは限らない.

---

[8] 線形代数学で学んだ理論は, 一般の体上で同様に展開できる.
[9] ここで, いくつかの α_j が K に属すことも有り得る. 特に, 自明な拡大体は有限生成である. 有限生成な拡大についての重要な性質として 13.14 を参照されたい.

演 習 問 題

9.6. $\mathbb{R}(\sqrt{2}) = \mathbb{R},\ \mathbb{R}(i) = \mathbb{C}$ であることを示せ.

9.7. $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(\sqrt{3}) = \mathbb{Q}$ であることを示せ. また, $\mathbb{Q}(\sqrt{2}) \cup \mathbb{Q}(\sqrt{3})$ は $\mathbb{R}$ の部分体か.

9.8. $\mathbb{C}$ 内において, $\mathbb{Q}(\alpha) \neq \mathbb{Q}[\alpha]$ となる $\alpha \in \mathbb{C}$ を 1 つ挙げよ.

9.9. 次の体の間の包含関係を理由を付して明示せよ. 但し i は虚数単位で $i^2 = -1$.

(1) $\mathbb{Q},\ \mathbb{Q}(\sqrt{2}),\ \mathbb{Q}(\sqrt{3}),\ \mathbb{Q}(\sqrt{6}),\ \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

(2) $\mathbb{Q},\ \mathbb{Q}(\sqrt{3}\, i),\ \mathbb{Q}(\frac{-1+\sqrt{3}i}{2}),\ \mathbb{Q}(\sqrt{3},\ i)$.

9.10. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\alpha)$ となる α を 1 つ求めよ.

§10. 標 数

定義 10.1. K のいかなる部分体も単位元 1 で生成される体を含む. その体と環として同型な[10] 体を素体といふ. (この体は構造の最も簡単な体である.)

ここで, 素体の構造を見てみる. 1 を m 回加へて $m1=0$ となつたとし, m はその様な最小の正整数とする. このとき m は素数であり, さもなくば, 任意の整数 $m\neq 0$ について $m1\neq 0$ である. 実際, その様な m が素数でないとする. $m=m_1m_2$ と因数分解すれば, $m_11\cdot m_21=m1=0$ より $m_11=0$ または $m_21=0$ となつて m の最小性に矛盾する. ゆゑに m は素数である. この様に, 素数 p について $p1=0$ となる場合, 体 K の標数は p であるといひ, $m1=0\implies m=0$ となる場合, 体 K の標数は 0 であるといふ. 一般に, 体 K の標数を $\operatorname{char}K$ と書く. 標数 p の素体は p 元体 $\mathbb{Z}/p\mathbb{Z}$ と同型である. また標数 0 の素体は整域 $\{m1|m\in\mathbb{Z}\}$ の商体 1.22 に他ならず, それは有理数体 $\mathbb{Q}$ と同型である. どんな体も素体を含むから, 任意の体 K に対し K の部分体の共通部分が K に含まれる唯一の素体に他ならない. 以上を次の定理にまとめておく.

定理 10.2. (1) どんな素体も, 有理数体 $\mathbb{Q}$ または p 元体 $\mathbb{Z}/p\mathbb{Z}$ (p は素数) に同型である.
(2) 任意の体は素体を唯一つ含む.
(3) 標数 $p>0$ の体は素体 $\mathbb{Z}/p\mathbb{Z}$ を含み, 標数 0 の体は素体 $\mathbb{Q}$ を含む.

問 10.3. K を体とし $\operatorname{char}K=p>0$ とする. $a,b\in K$ について次を示せ.
(1) $pa=0$.
(2) $n\in\mathbb{Z}$ に対し, $a\neq 0$ かつ $na=0\implies p|n$.
(3) N を非負整数とするとき $(a+b)^{p^N}=a^{p^N}+b^{p^N}$.
(4) N を非負整数とするとき $a_1,\cdots,a_t\in K$ について $\left(\sum_{i=1}^{t}a_i\right)^{p^N}=\sum_{i=1}^{t}{a_i}^{p^N}$.

演 習 問 題

10.4. 3 元体 $\mathbb{F}_3=\mathbb{Z}/3\mathbb{Z}$ 上の次の多項式は既約であることを示せ.
(1) x^2+1 (2) x^4+x+2

10.5. 剰余環 $\mathbb{F}_3[x]/(x^2+1)$ は体であることを示せ. また, これは素体ではないことを示せ.

10.6. 標数 5 の素体でない体の例を 1 つ挙げよ.

10.7. `paridroid` で
```
> factor(Mod(x^27-x,3))
```
と入力してみよ. この結果からわかることを述べよ.
(iPhone で `SageMath` を使用する場合は `gp("factor(Mod(x^27-x,3))")` と入力する.)

[10] この体からの環としての同型 (1.16 を見よ) の像となり得る体のこと.

§ 11. いくつかの例

理論を展開する前に, 感覚を整へるための例を述べるが, その前に最低限の準備をする.

命題 11.1. 体 K から別の体 L への $1 \mapsto 1$ なる準同型は単射である.

証明 この準同型の核を考へる (3.4 参照). 体の ideal は $\{0\}$ であるか, さもなくばその体全体であるから, この準同型の核は $\{0\}$ でなければならない. ゆゑに, それは単射である. □

命題 11.2. 体の有限次拡大 L/K があり, 環の準同型 $\varphi : L \to L$ で, どの $a \in K$ についても $\varphi(a) = a$ となるものは, 同型である. これを L の K 上の 自己同型 と呼ぶ（第 16 節を参照）.

証明 φ は 11.1 により必然的に単射で核 $\{0\}$ の次元 $\mathrm{null}(\varphi)$ は 0 であるが, 線形代数で学んだ 次元定理 より, 像空間 $\mathrm{Im}(\varphi)$ の K 上の次元 $\mathrm{rank}(\varphi)$ は定義域 L の次元 $[L : K]$ と一致する. L は K 上の有限次元 vector 空間なので, 再び線形代数学で学んだことから, 像空間 $\mathrm{Im}(\varphi)$ は L でなければならないから全射でもある. □

$L = K(\alpha)$ のとき, L の K 上の自己同型 φ は α の写る元 $\varphi(\alpha)$ だけで定まる. 例へば $a, b \in K$ のとき $\varphi(a + b\alpha) = \varphi(a) + \varphi(b)\varphi(\alpha) = a + b\varphi(\alpha)$, $\varphi(\alpha^2) = \varphi(\alpha)^2$ 等となるし, 一般に, 任意の $K(\alpha)$ の元は K の元を係数とする α の有理式で表され, それを $f(\alpha)$ と書けば

$$\varphi\big(f(\alpha)\big) = f\big(\varphi(\alpha)\big)$$

であるからである. 以降でこの様な自己同型の, いくつかの例を述べる.

例 11.3. 拡大 $\mathbb{C}/\mathbb{R}$ に関して, $\mathbb{C}$ の $\mathbb{R}$ 上の自己同型, 即ち, 環準同型 $\varphi : \mathbb{C} \to \mathbb{C}$ で $\varphi|_{\mathbb{R}}$ が恒等写像であるものをすべて求めてみる. $-1 = \varphi(-1) = \varphi(i^2) = \varphi(i)^2$ であるから, $\varphi(i) = \pm i$, $\varphi(a + bi) = a \pm bi$.

例 11.4. 拡大 $\mathbb{Q}(i)/\mathbb{Q}$ に関して, $\mathbb{Q}(i)$ の $\mathbb{Q}$ 上の自己同型. $\varphi : \mathbb{Q}(i) \to \mathbb{C}$ を環準同型で $1 \mapsto 1$ なるものとせよ. このとき $\varphi(n) = \varphi(1 + 1 + \cdots + 1) = n\varphi(1) = n$ で, $0 = \varphi(0) = \varphi(1 + (-1)) = 1 + \varphi(-1)$ より, $\varphi(-1) = -1$. このとき $\varphi(i)^2 = \varphi(-1) = -1$ より $\varphi(i) = \pm i$.

例 11.5. 拡大 $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ に関して, $\mathbb{Q}(\sqrt{2})$ の $\mathbb{Q}$ 上の自己同型. これも $\varphi(\sqrt{2})^2 = 2$ であるから $\varphi(a + b\sqrt{2}) = a \pm b\sqrt{2}$ の 2 つだけ.

例 11.6. 拡大 $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$, 但し $\omega = \frac{-1+\sqrt{-3}}{2}$, について $\mathbb{Q}(\sqrt[3]{2}, \omega)$ の $\mathbb{Q}$ 上の自己同型.
$\varphi\big((\sqrt[3]{2})\big)^3 = \big(\varphi(\sqrt[3]{2})^3\big) = \varphi(2) = 2$ であるから, $\varphi(\sqrt[3]{2})$ は $x^3 = 2$ の解である. 同様に $\varphi(\omega)$ は $x^2 + x + 1 = 0$ の解である. よつて

(1) $\varphi(\sqrt[3]{2}) = \sqrt[3]{2}$, $\varphi(\omega) = \omega$
(2) $\varphi(\sqrt[3]{2}) = \sqrt[3]{2}$, $\varphi(\omega) = \omega^2$
(3) $\varphi(\sqrt[3]{2}) = \sqrt[3]{2}\omega$, $\varphi(\omega) = \omega$
(4) $\varphi(\sqrt[3]{2}) = \sqrt[3]{2}\omega$, $\varphi(\omega) = \omega^2$
(5) $\varphi(\sqrt[3]{2}) = \sqrt[3]{2}\omega^2$, $\varphi(\omega) = \omega$
(6) $\varphi(\sqrt[3]{2}) = \sqrt[3]{2}\omega^2$, $\varphi(\omega) = \omega^2$

の 6 通りに限られるが, これらすべてが実際に自己同型になつてゐることが確かめられる (最終的には 19.20 (4) で示される). ここで $[\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}] = 6$ であることに注意せよ.

例 11.7. 拡大 $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ において, $\mathbb{Q}(\sqrt[3]{2})$ の $\mathbb{Q}$ 上の自己同型. 上の 11.6 から, 自己同型は恒等写像以外には有り得ない. ここで $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ であることに注意せよ.

例 11.8. いま $\alpha=\sqrt{6+3\sqrt{2}+2\sqrt{3}+2\sqrt{6}}$ とおき (根号内は正), 体

$$L=\mathbb{Q}(\alpha)$$

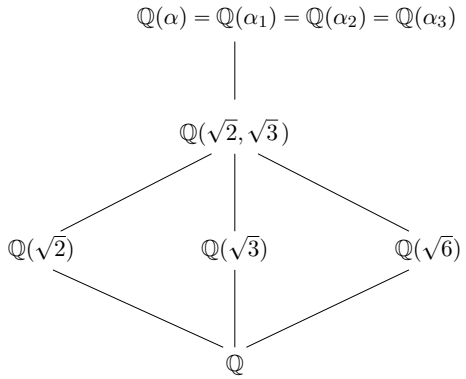
を考へる. これは有理数体 $\mathbb{Q}$ と α を含む $\mathbb{C}$ の部分体のうち最小なもののことである. つまり, α と任意の有理数について, 可能な限りの四則演算を行なひ得られた元を集めたものである. L の要素をいくつか挙げてみる. 例へば

$$L\ni\alpha^2=6+3\sqrt{2}+2\sqrt{3}+2\sqrt{6}$$

であるし, $\beta=\alpha^2-6$ とおくとき,

$$\begin{aligned}
\frac{\beta^2-54}{12}&=2\sqrt{2}+2\sqrt{3}+\sqrt{6}\in L,\\
\gamma=\beta-\frac{\beta^2-54}{12}&=\sqrt{2}+\sqrt{6}\in L,\\
\left(\beta-\frac{\beta^2-54}{12}\right)^2&=8+4\sqrt{3}\in L,\\
\frac{(\beta-\frac{\beta^2-54}{12})^2-8}{4}&=\sqrt{3}\in L,\\
\frac{\gamma(\sqrt{3}-1)}{2}&=\sqrt{2}\in L.
\end{aligned}$$

以上から $L\supset\mathbb{Q}(\sqrt{2},\sqrt{3})$ である. $\mathbb{Q}(\sqrt{2},\sqrt{3})$ は $\sqrt{2}$ と $\sqrt{3}$ を含む最小の ($\mathbb{C}$ の) 部分体である. 体 L, $\mathbb{Q}(\sqrt{2},\sqrt{3})$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}$ の間には次の図の様な包含関係がある. 図においては, 線分で結ばれた体について, より上の方にある体がより下の体を含む.



いま,

$$\begin{aligned}
\alpha_0&=\alpha,\\
\alpha_1&=\sqrt{6-3\sqrt{2}+2\sqrt{3}-2\sqrt{6}}\,,\\
\alpha_2&=\sqrt{6+3\sqrt{2}-2\sqrt{3}-2\sqrt{6}}\,,\\
\alpha_3&=\sqrt{6-3\sqrt{2}-2\sqrt{3}+2\sqrt{6}}
\end{aligned}$$

とおくとき (これらすべての根号内は正), 8 つの写像

$$\begin{aligned}
\sigma_i^{\pm}:L&\longrightarrow L\\
f(\alpha)&\longmapsto f(\pm\alpha_i)
\end{aligned}$$

はどれも自己同型である. ここに $f(x)$ は x の有理数係数の任意の有理式を表す. $\pm\alpha_i$ はどれも α の有理式で表はされる. 実際, $\alpha\,\alpha_1=\sqrt{6}$, $\alpha\,\alpha_2=(1+\sqrt{2})\sqrt{6}$, $\alpha\,\alpha_3=3\sqrt{2}+2\sqrt{3}$ であるが, $\sqrt{2}$, $\sqrt{3}$, $\sqrt{6}$ は α の有理式であるからである [11].

問 11.9. 上の記号の下で, $\mathbb{Q}(\alpha)=\mathbb{Q}(\alpha_1)=\mathbb{Q}(\alpha_2)=\mathbb{Q}(\alpha_3)$ であることを示せ.

問 11.10. 上の $\{\pm\alpha_i\,|\,i=0,\cdots,3\}$ は方程式 $f(x)=x^8-24x^6+108x^4-144x^2+36=0$ の根であることを示せ. また, 拡大次数 $[\mathbb{Q}(\alpha):\mathbb{Q}(\sqrt{2},\sqrt{3})]=2$ を証明せよ.

(Hint : `paridroid` を使ひ $f(x)$ を調べよ. 但し, 最後は手でできる証明に落し込むこと.)

[11] このことと $L\subset\mathbb{R}$ であることから, α_1, α_2, α_3 の根号内は正でなくてはならないこともわかる.

例 11.11. 最後の例は有限体についてのもの. $\mathbb{Z}/5\mathbb{Z}$ を $\mathbb{F}_5$ と略記する. いま $\alpha^3+\alpha+1=0$ なる α を考へる. この式を満たす数 α は $\mathbb{F}_5$ の中には存在しない（確かめよ）からこの α を新しい数として, α の $\mathbb{F}_5$ 上の多項式の全体

$$\mathbb{F}_5[\alpha]=\{\,a+b\alpha+c\alpha^2\,|\,a,\ b,\ c\in\mathbb{F}_5\,\}$$

を考察する[12) 13)]. これは, 自然に除法も備へてゐて, 有理式の全体 $\mathbb{F}_5(\alpha)$ と一致する, つまり

$$\mathbb{F}_5[\alpha]=\mathbb{F}_5(\alpha)$$

であることが次の様にしてわかる. 例へば

$$\begin{aligned}\frac{2+3\alpha}{1+2\alpha+3\alpha^2}&=\frac{(2+3\alpha)(1+2\alpha^5+3\alpha^{10})(1+2\alpha^{25}+3\alpha^{50})}{(1+2\alpha+3\alpha^2)(1+2\alpha^5+3\alpha^{10})(1+2\alpha^{25}+3\alpha^{50})}\\&=\frac{2\alpha^2+3}{2}=\alpha^2+4.\end{aligned}$$

ここで, 10.3(4) を使つて $\alpha^3+\alpha+1=0$ の両辺を 5 乗, 5^2 乗すると,

$$(\alpha^5)^3+\alpha^5+1=0,\quad (\alpha^{25})^3+\alpha^{25}+1=0$$

であるから, $x^3+x+1=0$ の 3 つの解が α, α^5, α^{25} であることがわかり[14)], $1+2\alpha+3\alpha^2$ の共役[15)] は, それ自身の他に $1+2\alpha^5+3\alpha^{10}$ と $1+2\alpha^{25}+3\alpha^{50}$ の全部で 3 つであることがわかる. これを上の計算において使つた. また, そのことは $\mathbb{F}_5(\alpha)$ の自己同型には $\mathbb{F}_5(\alpha)\longrightarrow\mathbb{F}_5(\alpha)$

$$\alpha\longmapsto\alpha,\quad \alpha\longmapsto\alpha^5,\quad \alpha\longmapsto\alpha^{25}$$

から定まる 3 つがあり, これ以外にはないことを意味してゐる（後の 16.3 で述べる）.

上の計算は次の様にしてもできる. x^3+x+1 と $1+2x+3x^2$ に対して $\mathbb{F}_5[x]$ における互除法を行ふと, $4(x^3+x+1)+(2x+2)(1+2x+3x^2)=1$ が得られ, $(2\alpha+2)(1+2\alpha+3\alpha^2)=1$ であり,

$$\frac{2+3\alpha}{1+2\alpha+3\alpha^2}=(2+3\alpha)(2\alpha+2)=6\alpha^2+10\alpha+4=\alpha^2+4.$$

以降, この体 $\mathbb{F}_5[\alpha]$ を $\mathbb{F}_{125}$ と記して, 125 元体と呼ぶ.

注意 11.12. 以上, 様々な例を見てきたが, どの例についても自己同型全体が写像の合成を演算として, 群をなす ことが見て取れる[16)]. このことを銘記しておいて欲しい.

演 習 問 題

11.13. 上の 11.11 における α について, $\dfrac{2\alpha+3}{2\alpha^2+3\alpha+1}$ を α の多項式で表せ.

11.14. 本文で取り上げた体 $\mathbb{F}_5(\alpha)$ について $\alpha\mapsto\alpha^5$ により定まる写像は自己同型であり, 各 $f(\alpha)\in\mathbb{F}_5(\alpha)$ を $f(\alpha)^5$ に写す写像であることを示せ.

11.15. paridroid で次の様な入力を試してみよ. 何がわかるか.

```
> a=Mod(a,a^3+a+1)
> Mod(a^125,5)
```

[12)] ここで, 高校で虚数単位を導入したときを思ひ出して欲しい. 「$i^2=-1$ となる数 i は実数の中には存在しない. そこでこの様な性質をもつ新しい数を考へて, $a+bi$ $(a,\,b\in\mathbb{R})$ なる形の数の全体を複素数と呼ぶ. 複素数についての四則演算は $i^2=-1$ 以外は極く自然に定義する」の様に導入される. ただ, その様な「新しい数」といふのが何なのかが気に掛かる. 実際, 複素数を導入した Gauss は非常に慎重にそれを導入してゐる. しかし, ここでは高校でのやり方で α を導入する.

[13)] なぜ, $a+b\alpha$ $(a,\,b\in\mathbb{F}_5)$ の全体でないのか理解できるか.

[14)] 8.2 を見よ.

[15)] 一般に代数的拡大 L/K と $\alpha\in L$ について, α と同じ既約多項式の根を α の共役であるといふ. 16.4 参照.

[16)] 次節の 12.5(2) で $\alpha^{125}=\alpha$ を示す. 「代数学 1」, 13.5(4) にも述べてある.

§ 12. 有限次拡大, 代数的拡大

定義 12.1. 拡大 L/K において $\alpha \in L$ が K 上の 0 ではないある多項式 $f(x)$ の根であるとき, α は K 上代数的であるといはれ, さうでないときは超越的であるといはれる. また L の任意の元が K 上代数的であるとき, L/K は代数的拡大である, または, L は K 上代数的であるといはれる. K の任意の元 a は $x-a$ の根であるから, もちろん K 上代数的である.

問 12.2. 体の拡大列 $K \subset M \subset L$ について答へよ.
(1) $\alpha \in L$ が K 上代数的であれば, それは M 上でも代数的であることを示せ.
(2) L/K が代数的拡大であれば L/M と M/K も代数的拡大であることを示せ.

問 12.3. M は L/K の中間体とする. M/K, L/M はともに有限次拡大とし, $\{\alpha_1, \cdots, \alpha_m\}$ を M の K 上の基底, $\{\beta_1, \cdots, \beta_l\}$ を L の M 上の基底とする. このとき $\{\alpha_i\beta_j \,|\, 1 \leqq i \leqq m,\ 1 \leqq j \leqq l\}$ は L の K 上の基底である. 特に L/K も有限次拡大であり,

$$[L:K] = [L:M][M:K] \tag{12.4}$$

が成り立つ. これらのことを示せ.

例 12.5. (1) $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 3$, $[\mathbb{Q}(\sqrt[3]{2}, i):\mathbb{Q}(\sqrt[3]{2})] = 2$, $[\mathbb{Q}(\sqrt[3]{2}, i):\mathbb{Q}] = 6$.
(2) 有限体の有限次拡大について. 有限個の元からなる体を有限体と呼ぶ. K を $\operatorname{char} K = p$ なる有限体とする. ここで, $[K:\mathbb{F}_p] = n$ とすれば, $|K| = p^n$ である[17]. 「代数学 1」(系 13.6) で学んだ様に, 0 以外の元のなす乗法群 $K^\times$ は位数 $p^n - 1$ の巡回群である. 従つて $0 \neq a \in K$ ならば $a^{p^n-1} = 1$ である. このことから K の任意の元は $a^{p^n} = a$ を満たす. 従つて $K/\mathbb{F}_p$ は代数的拡大である.

一般に, 拡大 L/K, $\alpha \in L$, および不定元 x について写像

$$\varphi : K[x] \longrightarrow L, \quad f(x) \mapsto f(\alpha)$$

を考へる. これは環準同型である. また $\operatorname{Ker}\varphi \neq \{0\}$ のときは α は代数的であり, $\operatorname{Ker}\varphi = \{0\}$ のときは α は超越的である. このいづれの状況においても, 9.3(2) の記号を使へば

$$\begin{aligned} K[\alpha] &= \operatorname{Im}\varphi = \{f(\alpha) \,|\, f(x) \in K[x]\}, \\ K(\alpha) &= \{f(\alpha)/g(\alpha) \,|\, f(x),\ g(x) \in K[x],\ g(\alpha) \neq 0\} \end{aligned} \tag{12.6}$$

となる. $K(\alpha)$ は $K[\alpha]$ の商体 (L 内で $K[\alpha]$ を含む最小の体) である. $\operatorname{Im}\varphi = K[\alpha]$ は体の部分環ゆゑ整域であるから, 準同型定理 1.21 によつて, $\operatorname{Ker}\varphi$ は素 ideal である. しかるに 6.10 で述べた通り $K[x]$ は単項 ideal 整域であるから, $\operatorname{Ker}\varphi = \{0\}$ または既約多項式 $p(x) \in K[x]$ によつて $\operatorname{Ker}\varphi = (p(x))$ となつてゐる. 6.3 と 6.10 により $(p(x))$ は $K[x]$ の極大 ideal である. 以上をまとめると
(1) $\operatorname{Ker}\varphi = \{0\}$ のとき, $K[\alpha] \simeq K[x]$, $K(\alpha) \simeq K(x)$ である[18].
(2) $\operatorname{Ker}\varphi = (p(x)) \neq \{0\}$ のとき, $K[\alpha] \simeq K[x]/(p(x))$ であり, これは体である.
特に $(p(x))$ は極大 ideal であり, $p(x)$ は $K[x]$ の既約多項式である.

命題 12.7. 有限次拡大は代数的拡大である.

証明 L/K は有限次拡大とし, $[L:K] = n$, $\alpha \in L$ とせよ. このとき $n+1$ 個の元 $\{1, \alpha, \alpha^2, \cdots, \alpha^n\}$ は K 上 1 次従属である. このことは次数が高々 n の多項式 $f(x)$ があつて $f(\alpha) = 0$ であることに他ならない. 従つて L の元はすべて K 上代数的である. □

[17] 基底 $\{v_1, \cdots, v_n\}$ を 1 つとれば, K の元は一意的に $a_1v_1 + \cdots + a_nv_n$ ($a_1, \cdots, a_n \in \mathbb{F}_p$) と書けるから.
[18] 記号 $\simeq$ は両者が環として同型であることを意味する (1.16 を見よ).

問 12.8. 拡大 L/K において, $\alpha\in L$ を K 上代数的な元として, α を根とする K 上の monic な多項式のうち次数が最も低いものを $p(x)$ とする. 次を示せ.
(1) $p(x)$ は一意的に定まる.
(2) $p(x)$ は K 上既約である.
(3) $f(x)\in K[x]$ について, $f(\alpha)=0 \iff p(x)|f(x)$ が成り立つ.

定義 12.9. 12.8 の多項式 $p(x)$ を $\mathrm{irr}\,(\alpha,K,x)$ で表し[19], これを α の K 上の最小多項式と呼ぶ.

定理 12.10. 拡大 L/K と $\alpha\in L$ について次が成り立つ.
(1) α が K 上代数的 $\iff$ $K(\alpha)=K[\alpha]$.
(2) α が K 上代数的で $\deg \mathrm{irr}\,(\alpha,K,x)=n \iff [K(\alpha):K]=n$. さらに, この両辺が成立してゐるとき, $\{1,\alpha,\alpha^2,\cdots,\alpha^{n-1}\}$ は $K(\alpha)$ の K 上の基底である.
(3) α が K 上代数的 $\iff$ $K(\alpha)/K$ は代数的拡大.

証明 (1) の ($\Rightarrow$). 任意の $f(x)\in K[x]$ について, $f(\alpha)\neq 0$ のとき $1/f(\alpha)\in K[\alpha]$ を示せばよい. $\mathrm{irr}\,(\alpha,K,x)=p(x)$ とせよ. $f(\alpha)\neq 0$ ならば, $p(x)$ の既約性により, $f(x)g(x)+h(x)p(x)=1$, $g(x)$, $h(x)\in K[x]$ となる $g(x)$, $h(x)$ が存在する. このとき $f(\alpha)g(\alpha)=1$ となる.
(1) の ($\Leftarrow$). $\alpha\in K$ なら明かなので $\alpha\notin K$ とする. このとき $1/\alpha=f(\alpha)$ ($f(x)\in K[x]$) と書かれるが, $\alpha f(\alpha)-1=0$, $xf(x)-1\in K[x]$ であり α は代数的である.
(2) の ($\Rightarrow$). もし $1,\alpha,\cdots,\alpha^{n-1}$ の間に K 上の線形関係が存在すれば α は $n-1$ 次以下の多項式の根となるから, 仮定に反する. 一方, 任意の多項式 $g(\alpha)\in K[\alpha]$ について, $g(x)$ の $\mathrm{irr}\,(\alpha,K,x)$ による剰余は $n-1$ 次式であるから, $g(\alpha)$ は $1,\alpha,\cdots,\alpha^{n-1}$ の 1 次結合で書ける. よつて, $1,\alpha,\cdots,\alpha^{n-1}$ は $K(\alpha)$ の K 上の基底をなし, $[K(\alpha):K]=n$ である.
(2) の ($\Leftarrow$). $n+1$ 個の $1,\alpha,\cdots,\alpha^n$ は 1 次従属であるから, α を根とする K 上の多項式が少なくとも 1 つ存在する. その様な多項式のうち次数が最小で monic な多項式が $\mathrm{irr}\,(\alpha,K,x)$ に他ならない. よつて α は K 上代数的である（これは 12.7 における議論に他ならない）. ここで, $\mathrm{irr}\,(\alpha,K,x)=d$ とおくと, 先に示した ($\Rightarrow$) により $[K(\alpha):K]=d$ となる. よつて $d=n$ でなければならない.
(3) の ($\Leftarrow$) は明らかである.
(3) の ($\Rightarrow$). α が K 上代数的で, $\deg \mathrm{irr}\,(\alpha,K,x)=n$ ならば, (2) より $[K(\alpha):K]=n$ である. よつて, 任意の $\beta\in K(\alpha)$ について, $1,\beta,\cdots,\beta^n$ は K 上 1 次従属である. よつて β は K 上の多項式の根であつて代数的である. □

上の考察から容易に次の定理が得られる.

定理 12.11. $f(x)\in K[x]$, $\deg f(x)>0$ とすれば, $f(x)=0$ の根を少なくとも 1 つ含む K の拡大体が存在する.

証明 $p(x)$ を $f(x)$ の 1 つの既約因子とすれば, $L=K[x]/(p(x))$ は体である. $K\ni a$ とそれを含む剰余類 $a+(p(x))$ を同一視して $K\subset L$ と考へてよい. $\alpha=x+(p(x))$ とおけば $p(\alpha)=p(x)+(p(x))=(p(x))=0_L$. 従つて $f(\alpha)=0$ である. □

[19] irr は irreducible（既約な）から採られてゐる.

例 12.12. 多項式 $x^3-2\in\mathbb{Q}[x]$ は既約であり, 対応 $x+(x^3-2)\mathbb{Q}[x]\mapsto\sqrt[3]{2}$ により

$$\mathbb{Q}[x]/(x^3-2)\simeq\mathbb{Q}(\sqrt[3]{2}).$$

同様に $\mathbb{Q}(\sqrt[3]{2}\omega)$ と対応 $x+(x^3-2)\mathbb{Q}[x]\mapsto\sqrt[3]{2}\omega$ により

$$\mathbb{Q}[x]/(x^3-2)\simeq\mathbb{Q}(\sqrt[3]{2}\omega).$$

$\mathbb{Q}(\sqrt[3]{2}\omega^2)$ についても同じ. しかし, もちろん $\mathbb{Q}(\sqrt[3]{2})\neq\mathbb{Q}(\sqrt[3]{2}\omega)$ 等である.

K の拡大体 L の元 $\alpha_1,\cdots,\alpha_n$ に対して

$$K[\alpha_1,\cdots,\alpha_n]=\{\,f(\alpha_1,\cdots,\alpha_n)\mid f(x_1,\cdots,x_n)\in K[x_1,\cdots,x_n]\,\}$$

であり, その商体が, L 内の $\alpha_1,\cdots,\alpha_n$ を含む最小の K の拡大体 $K(\alpha_1,\cdots,\alpha_n)$ に他ならない. また, $K(\alpha_1,\cdots,\alpha_{n-1},\alpha_n)=K(\alpha_1,\cdots,\alpha_{n-1})(\alpha_n)$ であることも, この記法の意味から容易にわかる.

問 12.13. 拡大 L/K において, $\alpha_1,\cdots,\alpha_n\in L$ がすべて K 上代数的ならば

$$K[\alpha_1,\cdots,\alpha_n]=K(\alpha_1,\cdots,\alpha_n)$$

となることを示せ.

定理 12.14. 拡大 L/K について次の 2 つは同値である.
(1) L/K は有限次拡大である.
(2) $L=K(\alpha_1,\cdots,\alpha_n)$ と書けて, 各 $\alpha_i\in L$ は K 上代数的である.

証明 (1)⇒(2). いま, $\alpha_1,\cdots,\alpha_n$ を K 上の vector 空間としての L の基底とせよ. このとき $L=K(\alpha_1,\cdots,\alpha_n)$ でなければならない. ゆえに, 各 α_i は 12.7 より K 上代数的である.
(2)⇒(1). 各 α_i は K 上代数的であるから, それは $K(\alpha_1,\cdots,\alpha_{i-1})$ 上でも代数的で, 12.10 (2) より $[K(\alpha_1,\cdots,\alpha_{i-1},\alpha_i):K(\alpha_1,\cdots,\alpha_{i-1})]=[K(\alpha_1,\cdots,\alpha_{i-1})(\alpha_i):K(\alpha_1,\cdots,\alpha_{i-1})]<\infty$ である. $K\subset K(\alpha_1)\subset\cdots\subset K(\alpha_1,\cdots,\alpha_{n-1})\subset L$ なる体の列を考へれば, 12.3 より

$$[\,L:K\,]=[K(\alpha_1,\cdots,\alpha_n):K(\alpha_1,\cdots,\alpha_{n-1})]\cdots[K(\alpha_1,\alpha_2):K(\alpha_1)][K(\alpha_1):K]<\infty$$

となる. □

12.14 から容易に次のことがわかる.

命題 12.15. 体の列 $K\subset M\subset L$ において L/M, M/K が共に代数的拡大であれば L/K も代数的拡大である.

証明 $\alpha\in L$ とすれば, $\alpha^n+a_1\alpha^{n-1}+\cdots+a_n=0$ となる $a_i\in M$ がある. このとき α は $N=K(a_1,\cdots,a_n)$ 上代数的で, また各 a_i は K 上代数的であるから $[N:K]<\infty$ である. 従つて $[N(\alpha):K]=[N(\alpha):N][N:K]<\infty$ となり, α は K 上代数的である. □

命題–定義 12.16. 拡大 L/K において K 上代数的な L の元の全体を M とすれば, M は体である. 従つて K 上代数的な 2 元の和, 差, 積, 商はまた K 上代数的である. この M を K の L における 代数的閉包 と呼ぶ.

証明 $\alpha,\beta\in M$ とすれば, 12.14 より $K(\alpha,\beta)$ は代数的, 従つて $\alpha\pm\beta$, $\alpha\beta\in M$, また $\beta\neq0$ なら $\alpha\beta^{-1}\in M$ となる. □

演 習 問 題

12.17. 次の各問において, 拡大 $\mathbb{C}/K$ と元 $\alpha\in\mathbb{C}$ について $\mathrm{irr}\,(\alpha,K,x)$ を求めよ.

(1) $K=\mathbb{Q}$, $\alpha=\sqrt{2}$.
(2) $K=\mathbb{Q}$, $\alpha=\sqrt{-3}$.
(3) $K=\mathbb{Q}$, $\alpha=\sqrt{3}+\sqrt{5}$.
(4) $K=\mathbb{Q}$, $\alpha=\sqrt[4]{2}$.
(5) $K=\mathbb{Q}(\sqrt{2})$, $\alpha=\sqrt[4]{2}$.
(6) $K=\mathbb{Q}$, $\alpha=\exp(\frac{2\pi i}{5})$.
(7) $K=\mathbb{Q}(\sqrt{5})$, $\alpha=\exp(\frac{2\pi i}{5})$.

12.18. 12.16 の記号のもとで, L の元で M 上の代数的な元は M の元に限ることを示せ.
(Hint : $\alpha\in L$ は M 上代数的とせよ. $\mathrm{irr}\,(\alpha,M,x)$ の係数を K に添加した体について, 12.15 を利用せよ.)

12.19. $\mathbb{F}_p$ を標数 $p>0$ の素体とせよ (つまり p は素数で $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$). 多項式 $x^2+1\in\mathbb{F}_p[x]$ が既約であるためには $p\equiv 3 \bmod 4$ であることが必要十分である. これを証明せよ.

12.20. 次の拡大次数を求めよ.

(1) $[\mathbb{C}:\mathbb{R}]$
(2) $[\mathbb{Q}(\sqrt{5}):\mathbb{Q}]$
(3) $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]$
(4) $[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}]$

12.21. 体の拡大 L/K があり, M をその中間体とせよ. $\alpha\in L$ が K 上代数的であるとせよ. このとき $[M(\alpha):M]\leqq[K(\alpha):K]$ であることを示せ.

12.22. 体の拡大 L/K と中間体 M_1, M_2 があつて $[M_1:K]=m_1$, $[M_2:K]=m_2$, $\gcd(m_1,m_2)=1$ とせよ. このとき $M_1\cap M_2=K$ であることを示せ.

12.23. 体の拡大 L/K があり, α, $\beta\in L$ とせよ. $[K(\alpha):K]=m$, $[K(\beta):K]=n$, $\gcd(m,n)=1$ ならば, $[K(\alpha,\beta):K]=mn$ であることを示せ.

12.24. 体の有限次拡大 L/K があり R は $L\supset R\supset K$ を満たし, L の演算に関して環であるとせよ. このとき R は体であることを示せ. (Hint : (12.7 と 12.10(1)) を用ゐよ.)

12.25. 無限次の代数的拡大の例を一つ挙げよ.

§ 13. 超越次数

ここでは代数的拡大でない拡大について, 後に必要となることに限つてまとめておく.

定義 13.1. 拡大 L/K があり, $\alpha_1, \cdots, \alpha_n \in L$ とする. 0 でない任意の $f(x_1,\cdots,x_n) \in K[x_1,\cdots,x_n]$ に対して $f(\alpha_1,\cdots,\alpha_n) \neq 0$ であるとき, $\alpha_1, \cdots, \alpha_n$ は K 上代数的に独立であるといひ, さうでないとき代数的に従属であるといふ.

注意 13.2. 上の 13.1 で, $n=1$ のとき, $\alpha \in L$ が K 上代数的に独立といふことは, K 上超越的であることと同じである. また $x_1, \cdots, x_n$ を n 個の不定元 (文字) とすると, $\alpha_1, \cdots, \alpha_n \in L$ が K 上代数的に独立であることは, 写像

$$\varphi : K[x_1,\cdots,x_n] \longrightarrow K[\alpha_1,\cdots,\alpha_n], \quad f(x_1,\cdots,x_n) \longmapsto f(\alpha_1,\cdots,\alpha_n)$$

が環同型であることと同値である. 体 $K(x_1,\cdots,x_n)$ は K 上の有理函数体と呼ばれるのであるが, 上の状況のとき $K(\alpha_1,\cdots,\alpha_n)$ はこの $K(x_1,\cdots,x_n)$ と同型である.

定義 13.3. L の部分集合 S に対して, その任意の有限部分集合が K 上代数的に独立であるとき, S は K 上代数的に独立であるといはれる. $S \subset L$ が K 上代数的に独立な部分集合のうち極大なものであるとき, S は L/K の超越基であるといはれる.

問 13.4. 拡大 L/K において, $\alpha_1, \cdots, \alpha_n \in L$ は K 上代数的に独立であるとする. このとき, 次のことを示せ. 但し $\beta \in L$ である.

(1) $\alpha_1, \cdots, \alpha_n, \beta$ が K 上代数的に従属 $\iff$ $K(\alpha_1,\cdots,\alpha_n,\beta)/K(\alpha_1,\cdots,\alpha_n)$ が代数的.

(2) $\{\alpha_1,\cdots,\alpha_n\}$ が L/K の超越基 $\iff$ $L/K(\alpha_1,\cdots,\alpha_n)$ が代数的.

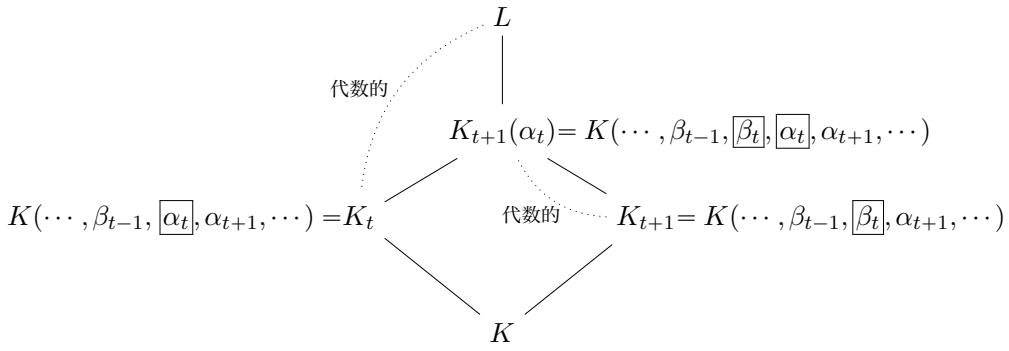
Vector 空間における基底と同様に, 超越基について次の定理が成り立つ.

定理 13.5. 拡大 L/K が有限生成ならば, L/K は有限個の元からなる超越基を持つ. その元の個数は超越基の選び方によらず一定である. この個数を L/K の超越次数と呼び, $\mathrm{trans.deg}_K L$ で表す.

証明 $L = K(\alpha_1,\cdots,\alpha_n)$ とし, $\{\alpha_1,\cdots,\alpha_n\}$ の部分集合で K 上代数的に独立なもののうち, 元の個数が最大なものを (必要ならばその番号を付け替へて) $\{\alpha_1,\cdots,\alpha_r\}$ とせよ. $M = K(\alpha_1,\cdots,\alpha_r)$ とおけば, 13.4 (1) より任意の α_i は M 上代数的で $L = K(\alpha_{r+1},\cdots,\alpha_n)$ であるから, L/M は代数的である. 従つて $\{\alpha_1,\cdots,\alpha_r\}$ は超越基であり, L/K は有限個の元からなる超越基を持つ.

さて, 上の状況で, $\{\beta_1,\cdots,\beta_s\}$ を L/K の任意の超越基とする. このとき $L/K(\beta_1,\cdots,\beta_s)$ は $K(\beta_1,\cdots,\beta_s)$ 上代数的なある $\beta_{s+1},\cdots,\beta_m \in L$ により, $L = K(\beta_1,\cdots,\beta_s,\beta_{s+1},\cdots,\beta_m)$ と書ける. 実際, $L = K(\beta_1,\cdots,\beta_s,\alpha_1,\cdots,\alpha_n)$ であり, $\alpha_1, \cdots, \alpha_n$ は ($\beta_1, \cdots, \beta_s$ の仮定から) $K(\beta_1,\cdots,\beta_s)$ 上代数的である. これらのことから $s \leqq r$ であることを示せばよい. (逆向きの不等式は $\{\alpha_1,\cdots,\alpha_n\}$ と $\{\beta_1,\cdots,\beta_m\}$ の役割を入れ替へて得られる.) 以下, 背理法による証明を行ふので $s > r$ と仮定する. このとき, $\{\alpha_j\}$ の番号を適当につけかへて, 帰納法で, 各 $t = 1, \cdots, r+1$ に対して, L が $K_t = K(\beta_1,\cdots,\beta_{t-1},\alpha_t,\cdots,\alpha_r)$ の上に代数的であること, 特に L が $K_{r+1} = K(\beta_1,\cdots,\beta_r)$ 上に代数的であることを証明する. この結論は $\{\beta_1,\cdots,\beta_s\}$ が L/K の超越基であることに矛盾するから証明が完了する. さて, まづ $t = 1$ については明らかに成り立つ. 次に L は K_t 上に代数的であると仮定する. β_t は L の元であるから K_t 上に代数的であり, 0 でない多項式 $f(x) = c_0x^m + c_1x^{m-1} + \cdots + c_m \in K_t[x]$

が存在して $f(\beta_t)=0$ となる. ここで, 左辺の各係数の分母を払ふことにより, 左辺は $\beta_1, \cdots, \beta_t, \alpha_t, \cdots, \alpha_r$ の多項式であるとしてよい. 仮定により, $\beta_1, \cdots, \beta_t$ は K 上代数的に独立であるから, $f(x)$ の係数の中に $\alpha_t, \cdots, \alpha_r$ のうちの少くとも 1 つが実際に現れなくてはならない. 番号を付け替へて, それを α_t とし, $f(\beta_t)=0$ の左辺を α_t についてまとめれば, 体 K_{t+1} の元を係数とする α_t の多項式が 0 となる, といふ自明でない関係式が得られる. よつて α_t は K_{t+1} 上に代数的である. $K_t \subset K_t(\beta_t) = K_{t+1}(\alpha_t)$ で[20] $K_{t+1}(\alpha_t)$ は K_{t+1} 上に代数的である.



以上から, 帰納法の仮定, 12.2, 12.15 によつて, L は K_{t+1} 上の代数的拡大でもである. □

例題 13.6. 体の列 $K \subset M \subset L$ において L/M が代数的拡大ならば $\mathrm{trans.deg}_K L = \mathrm{trans.deg}_K M$ が成り立つ. 但し, M/K は有限生成とする.

証明 $\{\alpha_1, \cdots, \alpha_n\}$ を M/K の超越基とし, $N = K(\alpha_1, \cdots, \alpha_n)$ とすれば, M/N は代数的拡大である (13.4(2)) が, 12.15 により, L/N も代数的拡大である. ゆゑに, 13.4(2) より $\{\alpha_1, \cdots, \alpha_n\}$ は L/K の超越基でもある. よつて $\mathrm{trans.deg}_K L = \mathrm{trans.deg}_K M$. □

13.5 の証明から, 次のことがわかる.

例題 13.7. $L = K(\alpha_1, \cdots, \alpha_n)$ で $\mathrm{trans.deg}_K L = n \geqq 1$ ならば $\{\alpha_1, \cdots, \alpha_n\}$ は K 上代数的に独立で, それゆゑ L/K の超越基である. この様な拡大を <u>純超越拡大</u> といふ.

証明 13.5 の証明の最初に示した様に, $\{\alpha_1, \cdots, \alpha_n\}$ の部分集合で K 上代数的独立なものがある. このうち, 元の個数が最大なものを (番号を付け替へて) $\{\alpha_1, \cdots, \alpha_r\}$ とすれば, これは L/K の超越基である. よつて仮定により $r = n$ となる. □

[20] 体 $K_t(\beta_t) = K_{t+1}(\alpha_t)$ は 2 つの体 K_t と K_{t+1} の合成体 K_tK_{t+1} (第 14 節で述べる) に他ならない.

演 習 問 題

13.8. ξ が K 上超越的ならば, $n \in \mathbb{N}$ に対し $[K(\xi) : K(\xi^n)] = n$ であることを示せ.

13.9. 体 k と不定元 t について, $K = k(t^5)$, $L = k(t)$ とせよ.
(1) $[L : K]$ はいくつか.
(2) $\alpha = t^2 + t + 1$ とおく. $K(\alpha) = L$ であることを示せ.
(3) t を t^5 と α の k 上の有理式で具体的に書け.
(Hint : t が $\beta = \alpha - 1$ と t^5 で表せればよい. $t\beta$, β^2, β^3, t^5 の間のうまい 1 次関係を考へよ.)

13.10. 円周率 π は $\mathbb{Q}$ 上超越的であることが知られてゐる. $\mathrm{trans.deg}_{\mathbb{Q}} \mathbb{Q}(\pi + \sqrt{\pi})$ はいくつか.

13.11. L を 環 $\mathbb{Q}[x, y]/(x^2 + y^2 - 1)$ の商体とする. $\mathrm{trans.deg}_{\mathbb{Q}} L$ はいくつか. また, 拡大 $L/\mathbb{Q}$ の超越基を 1 組求めよ.

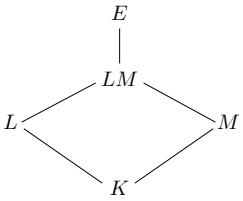
13.12. L を 環 $\mathbb{Q}[x, y, z]/(x^2 + y^3 + z^4 - 1)$ の商体とする. $\mathrm{trans.deg}_{\mathbb{Q}} L$ はいくつか. また, 拡大 $L/\mathbb{Q}$ の超越基を 1 組求めよ.

13.13. 体の拡大列 $K \subset M \subset L$ について L/M と M/K がともに有限生成であるとする. このとき $\mathrm{trans.deg}_K L = \mathrm{trans.deg}_K M + \mathrm{trans.deg}_M L$ であることを示せ.

13.14.* 体 L が部分体 $K\,(\subset L)$ 上有限生成であるとき, 任意の部分体 $K \subset M \subset L$ について, L/M も M/K も有限生成であることを示せ.
(L/M については容易. M/K については, 文献 [F], p.313, 定理 4.9 を見よ)

§ 14. 合成体

定義 14.1. (1) 拡大体 E/K において, L をその中間体, S を E の部分集合とするとき, L の元を係数とし S の有限個の元の有理式の形で表される元の全体は E/L の中間体である. これを $L(S)$ で表す. $L(S)$ は L と S を含む E の最小の部分体である. 特に M が E/K の中間体のときは $L(M)=M(L)$ となる. これを L と M の合成体と呼んで LM または ML で表す. また拡大 ML/M を拡大 L/K の M への (または, M/K による) 持ち上げと呼ぶ. LM は L と M を含む最小の部分体に他ならない.



(2) 任意の拡大 L/K とその任意の持ち上げ LM/M に関し, 拡大に関するある性質 $\boldsymbol{P}$ が L/K で満たされてゐれば, LM/M でも成り立つとき, 性質 $\boldsymbol{P}$ は持ち上げによつて保たれるといふ.

持ち上げに関して保たれる性質として次の様なものがある.

命題 14.2. 体の拡大に関する次の性質は持ち上げによつて保たれる.
(i) 代数的拡大, (ii) 有限生成, (iii) 有限次拡大, (iv) 単純拡大.

証明 拡大 L/K の持ち上げ ML/M を考へる.
(i) L/K が代数的であるとせよ. $\alpha\in ML=M(L)$ は

$$\alpha=f(\gamma_1,\cdots,\gamma_n)/g(\gamma_1,\cdots,\gamma_n),\quad f,\ g\in M[x_1,\cdots,x_n],\ \ \gamma_i\in L$$

と表されてゐる. このとき $\alpha\in M(\gamma_1,\cdots,\gamma_n)$ であるが, 各 γ_i は K 上代数的ゆゑ M 上でも代数的, 従つて 12.14 (2)⇒(1) により $M(\gamma_1,\cdots,\gamma_n)/M$ は代数的であり, α は M 上代数的.
(ii) L/K が有限生成, つまり $L=K(\alpha_1,\cdots,\alpha_n)$ と書けてゐるとせよ. このとき $ML=M(L)=M(\alpha_1,\cdots,\alpha_n)$ であるから ML/M も有限生成.
(iii) L/K が有限次拡大であれば, 12.7 により代数的拡大でもある. より強く, 12.14 (1)⇒(2) から K 上代数的な α_j $(1\leqq j\leqq n)$ によつて $L=K(\alpha_1,\cdots,\alpha_n)$ と書けてゐる. このとき (ii) と同様に $ML=M(\alpha_1,\cdots,\alpha_n)$ と書けて, 各 α_j は M 上でも代数的であるから, 再び 12.14 (2)⇒(1) により ML/M は有限次拡大である.
(iv) (ii) の証明で $n=1$ の場合を考へれば, 直ちにわかる. □

演 習 問 題

14.3. 次に挙げる 2 つの体の合成体をできるだけ簡潔な形で答へよ. また, その合成体の $\mathbb{Q}$ 上の基底と $\mathbb{Q}$ 上の拡大次数を求めよ.
(1) $\mathbb{Q}(\sqrt{2})$ と $\mathbb{Q}(\sqrt{3})$
(2) $\mathbb{Q}(\sqrt[4]{3})$ と $\mathbb{Q}(\sqrt{3})$
(3) $\mathbb{Q}(\sqrt[3]{2})$ と $\mathbb{Q}(\sqrt[3]{2}i)$
(4) $\mathbb{Q}(\sqrt{2})$ と $\mathbb{Q}(\sqrt{2}+\sqrt{3})$

14.4. 体の拡大 L/K と $\alpha_1,\cdots,\alpha_m,\beta_1,\cdots,\beta_n\in L$ について, $K(\alpha_1,\cdots,\alpha_m)$ と $K(\beta_1,\cdots,\beta_n)$ の合成体は $K(\alpha_1,\cdots,\alpha_m,\beta_1,\cdots,\beta_n)$ であることを説明せよ.

14.5. 代数的拡大 L/K の 2 つの真の中間体 M_1, M_2 で, 互ひに包含関係がなく, $[M_1M_2:M_1]<[M_2:K]$ であり, $[M_1M_2:M_1]=[M_2:M_1\cap M_2]$ となる例を挙げよ. また $[M_1M_2:M_1]<[M_2:M_1\cap M_2]$ となる例を挙げよ. (Hint : 後半は $M_1M_2=\mathbb{Q}(\sqrt[3]{2},\omega)$ となる M_1, M_2 を考へよ.)
(以上より, 一般に, 拡大次数は持ち上げによつて保たれない. 23.5 も参照.)

14.6.* 拡大 L/K の 2 つの中間体 M_1, M_2 について, $[M_1:K]=m$, $[M_2:K]=n$, $\gcd(m,n)=1$ のとき, $[M_1M_2:K]=mn$ であることを示せ. (12.23 の一般化. [F], p.68, 定理 2.16 の系(iii).)

§ 15. 代数的閉包

この節では, いくつもの体に関する種々の考察をするのに便利な代数的閉包と呼ばれる体の存在を証明する.

命題 15.1. 体 Ω について, 次の条件は互ひに同値である.
(1) $f(x)\in\Omega[x]$, $\deg f>0$ ならば, Ω は $f(x)$ の根を少くとも 1 つ含む.
(2) $f(x)\in\Omega[x]$, $\deg f>0$ ならば, $f(x)$ は $\Omega[x]$ で 1 次式の積に分解する.
(3) $\Omega[x]$ の既約多項式はすべて 1 次式または定数である.
(4) Ω の代数的拡大は Ω 以外には存在しない.

証明 (1)⇒(2). $\deg f$ に関する帰納法で容易に証明される.
(2)⇒(3). 自明.
(3)⇒(4). L/Ω を代数的拡大とせよ. $\alpha\in L$ とすれば $\mathrm{irr}\,(\alpha,\Omega,x)$ は 1 次式である. 従つて $\alpha\in\Omega$ であり, $L=\Omega$ である.
(4)⇒(1). 12.11 より $f(x)$ の根 α を含む Ω の拡大が存在する. その 1 つを L とすれば $L\supset\Omega(\alpha)$ であつて, もちろん $\Omega(\alpha)/\Omega$ は代数的拡大であるから, 仮定より $\alpha\in\Omega(\alpha)=\Omega$ となる. □

定義 15.2. 体 Ω が 15.1 の条件を満たすならば, Ω は 代数的閉体 であるといはれる.

例 15.3. (1) 複素数体 $\mathbb{C}$ は代数的閉体である (代数学の基本定理).
(2) $\overline{\mathbb{Q}}=\{\alpha\in\mathbb{C}\,|\,\alpha$ は $\mathbb{Q}$ 上代数的$\}(\subset\mathbb{C})$ は代数的閉体である (12.18 と 15.1(4) を使ふ).
円周率 $\pi=3.14159265\cdots$ や Napier の数 $e=2.7182818284590\cdots$ などは $\overline{\mathbb{Q}}$ に属さないことが知られてをり, $\overline{\mathbb{Q}}\subsetneq\mathbb{C}$ である (15.10 も参照されたい).

定義 15.4. 拡大 Ω/K が代数的拡大であり, かつ Ω が代数的閉体であるとき, Ω は K の 代数的閉包 であるとはれる.

問 15.5. L/K が代数的ならば L の代数的閉包は K の代数的閉包であることを示せ. (Hint : 12.2.)

以下では代数的閉包の存在を証明する.

定理 15.6. (E. Steinitz) 任意の体 K に対し K の代数的閉包が存在する.

これは K 上のあらゆる多項式の根を添加してできあがる最大の体が存在するといふことであるが, 当面, これを認めて証明を飛ばし先に進んでもよい. この定理の証明のためにまづ, 次のことを示す.

補題 15.7. 多項式環 $K[x]$ において, 次数が 1 以上の多項式の全体を $K[x]^*$ と表す. K の代数的拡大で, 任意の $f(x)\in K[x]^*$ がそこで少くとも 1 つ根を持つ様なものが存在する.

証明 各 $f(x)\in K[x]^*$ ごとに文字 X_f を用意し, それらの文字の全体を S とする : $S=\{X_f\,|\,f(x)\in K[x]^*\}$. また S の有限個の元に関する K 上の多項式の全体を $K[S]$ と書く. $K[S]$ はもちろん可換環である. $K[S]$ において $\{f(X_f)\,|\,f\in K[x]^*\}$ で生成される ideal を I とする. $K[S]\supsetneq I$ となることが次の様にして示される. いま $K[S]=I$ であるとすれば, $f_1(x),\cdots,f_n(x)\in K[x]^*$ と $g_1,\cdots,g_n\in K[S]$ が存在して

$$1=g_1\cdot f_1(X_{f_1})+\cdots+g_n\cdot f_n(X_{f_n}) \tag{15.8}$$

が成り立つ. $g_1, \cdots, g_n$ に現れる変数の個数は有限であるから, ある $N \in \mathbb{N}$ について, これらはすべて $K[X_{f_1}, \cdots, X_{f_n}, \cdots, X_{f_N}]$ の元としてよい. さて, 12.11 より $f_1(x) \in K[x]$ の根の 1 つ α_1 を含む拡大 L_1/K が存在する. さらに $f_2(x) \in L_1[x]$ の根の 1 つ α_2 を含む拡大 L_2/L_1 がある. 以下同様にして体の拡大列 $K \subset L_1 \subset L_2 \subset \cdots \subset L_n = L$ (と $\alpha_j \in L_j$) を考へる. このとき, もちろん L はこれら $\alpha_1, \cdots, \alpha_n$ のすべてを含む. そこで (15.8) に

$$X_{f_1} = \alpha_1, \cdots, X_{f_n} = \alpha_n, X_{f_{n+1}} = \cdots = X_{f_N} = 0$$

なる代入をすれば $1 = 0$ となり矛盾である. よつて $K[S] \supsetneqq I$ である. これにより I を含む $K[S]$ の極大 ideal が存在する. その 1 つを J とせよ. $E_K = K[S]/J$ は体であり, 自然に $K \subset E_K$ と見做せる. X_f を含む剰余類 $X_f + J$ を $\overline{X_f}$ で表す. I の定義から, 任意の $f \in K[x]^*$ に対して $f(\overline{X_f}) = 0$ となるから, E_K は所望の条件を満たす. □

証明 (**15.6** の). 上で示した様に $K[S] \supsetneqq I$ であるから, I を含む $K[S]$ の極大 ideal J がある. $E_K = K[S]/J$ は体で, $E_K \supset K$ と考へてよい. いま X_f を含む剰余類 $X_f + J$ を $\overline{X_f}$ と表せば, I の定義から任意の $f \in K[x]^*$ に対して $f(\overline{X_f}) = 0$ となり, E_K/K は 15.7 に叶ふ拡大である. $K_0 = K$ とし, 15.7 の様な E_K を 1 つとつて $E_K = K_1$ とおく. K に対して行つた手続きを K_1 に対して行ひ, E_{K_1} を得るが, それを E_2 とおく. 以下同様に手続きを行ひ $K_{i+1} = E_{K_i}$ と記せば, 体の列

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots$$

が得られる. この作り方から K_{i+1}/K_i は代数的拡大であり, 任意の $h(x) \in K_i[x]^*$ は K_{i+1} で少くとも 1 つの根を持つ. $\Omega = \bigcup_{i=0}^{\infty} K_i$ は K の拡大で, $\alpha \in \Omega$ はある K_i に含まれ, K_i/K は代数的拡大であるから Ω/K は代数的拡大である. また $h(x) = c_0 x^r + c_1 x^{r-1} + \cdots + c_r \in \Omega[x]$ が次数 1 以上であれば, ある m について, K_m は, すべての c_i $(0 \leqq i \leqq r)$ を含む. $h(x) \in K_m[x]^*$ であるから $h(x)$ は K_{m+1} 内に, つまり Ω 内に, 少くとも 1 つ根を持つ. これで Ω は代数的閉体であることがわかつた. つまり Ω は K の代数的閉包である. □

注意 15.9. Ω は体 K を含む代数的閉体とし, $\overline{K}$ を K の Ω における代数的な元全体の集合とすれば, $\overline{K}$ は K の代数的閉包である (12.18 と 15.1(4) による). この様に, 体 K を含む代数的閉体があれば, それに含まれる K の代数的閉包は一意的に定まる.

演 習 問 題

15.10. $\overline{\mathbb{Q}}$ は集合として可算濃度であることを示せ. (Hint : 各多項式 $f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n \in \mathbb{Z}[x]$ $(a_0 \geqq 1)$ に対し $n + a_0 + |a_1| + \cdots + |a_n|$ を考へて, これをもとに $\overline{\mathbb{Q}}$ の元を数へればよい.)

15.11. $\mathbb{C}$ は非可算集合であることを示し, $\overline{\mathbb{Q}} \subsetneqq \mathbb{C}$ を示せ.

15.12. $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$ であることを示せ. (Hint : Eisenstein の既約性判定定理を使ひ, いくらでも次数の高い既約多項式があることを示せ.)

§ 16. 部分体の上の同型

体 K から体 L への環準同型 $\sigma : K \to L,\ a \mapsto a^\sigma$ について, その核 $\mathrm{Ker}\,\sigma$ は K の ideal であるから K 自身であるか $\{0\}$ である. 前者の場合, つまり像が $\{0\}$ のとき, σ は 自明 であるといはれる. 後者の場合, つまり $\mathrm{Ker}\,\sigma = \{0\}$ のとき, σ は単射であるから, K は σ と通じて部分体 $\mathrm{Im}\,\sigma \subset L$ に同型である. この準同型の像 $\mathrm{Im}\,\sigma$ は通常

$$K^\sigma = \{\, a^\sigma \,|\, a \in K \,\}$$

と書かれる. このとき σ を K から L の 中への同型 といふ. 特に $\mathrm{Im}\,\sigma = L$ のときは $\sigma : K \xrightarrow{\sim} L$ と書いて, K から L への 上への同型 といふ.

定義 16.1. 体 K の 2 つの拡大 L/K と L'/K の間の同型 $\sigma : L \xrightarrow{\sim} L'$ が K の各元を不変にするとき, 即ち $\mathrm{id}_K : K \xrightarrow{\sim} K$ の拡張になつてゐるとき, σ を K 上の同型 であるといふ. 中への K 上の同型 も同様に定義される. 体 L から自身への同型 $\sigma : L \xrightarrow{\sim} L$ を L の 自己同型 といふ. また拡大 L/K に対して K 上の同型 $\sigma : L \xrightarrow{\sim} L$ を L の K 上の自己同型 といふ. これらは写像の合成を演算として群をなす. それぞれを

$$\mathrm{Aut}\, L, \qquad \mathrm{Aut}\, L/K$$

と書いて, それぞれ L の 自己同型群, K 上の自己同型群 と呼ぶ. (同型 : automorphism)

体の同型 $\sigma : K \xrightarrow{\sim} K'$ は自然に多項式環の間の環としての同型

$$K[x] \xrightarrow{\sim} K'[x] \qquad \sum_{i=0}^{n} a_i x^i \mapsto \sum_{i=0}^{n} {a_i}^\sigma x^i$$

に拡張される. これを同じ記号 σ で表して $f(x) \in K[x]$ の像を $f^\sigma(x)$ で表す. 明らかに, $p(x)$ が $K[x]$ の既約多項式ならば, $p^\sigma(x)$ は $K'[x]$ の既約多項式であり, この逆も成り立つ.

問 16.2. 次の問に答へよ.

(1) $\mathbb{Q}$ および $\mathbb{F}_p$ (p は素数) の自己同型写像は恒等写像に限ることを示せ.
(2) $\mathrm{char}\, F = p > 0$ とせよ. $\mathbb{Q}$ から F への (または F から $\mathbb{Q}$ への) 環準同型写像は, すべての元を $0 \in F$ (または $0 \in \mathbb{Q}$) に写すものだけであることを示せ.
(3) $\mathbb{Q}(\sqrt{2})$ の自己同型写像は 2 つだけ存在する. それらを記述せよ.
(4) $\mathbb{Q}(\sqrt[3]{2})$ の自己同型写像は恒等写像しかないことを示せ.
(5) $\mathbb{Q}(\sqrt[3]{2})$ から $\mathbb{C}$ の中への同型写像は 3 つだけ存在する. それらを記述せよ.

命題 16.3. $\sigma : K \xrightarrow{\sim} K'$ を体の同型とせよ. いま $L = K(\alpha)$ は $K[x]$ の既約多項式 $p(x)$ の根 α を K に添加した体とし, $L' = K'(\alpha')$ は $p^\sigma(x)$ の根 α' を K' に添加した体とする. このとき σ の拡張である同型 $\rho : L \xrightarrow{\sim} L'$ (つまり $\rho|_K = \sigma$) で α を α' に写すものが唯一つだけ存在する.

証明 $\sigma : K[x] \xrightarrow{\sim} K'[x]$ から自然に環準同型 $\overline{\sigma} : K[x]/(p(x)) \xrightarrow{\sim} K'[x]/(p^\sigma(x))$ が得られる. これは $\sigma : K \xrightarrow{\sim} K'$ の拡張で $x + (p(x)) \mapsto x + (p^\sigma(x))$ となつてゐる. 一方,

$$\tau : K[x]/(p(x)) \xrightarrow{\sim} K(\alpha),\ x + (p(x)) \mapsto \alpha\ ;$$
$$\tau' : K'[x]/(p^\sigma(x)) \xrightarrow{\sim} K'(\alpha'),\ x + (p^\sigma(x)) \mapsto \alpha'$$

はそれぞれ K 上の同型, K' 上の同型である. このとき

$$\begin{array}{ccc} K[x]/(p(x)) & \xrightarrow{\overline{\sigma}} & K'[x]/(p^\sigma(x)) \\ \downarrow \tau & & \downarrow \tau' \\ K(\alpha) & \xrightarrow{\rho} & K'(\alpha') \end{array}$$

$\rho = \tau' \overline{\sigma} \tau^{-1} : K(\alpha) \mapsto K'(\alpha')$ は求めるものである. これは α の写り先で決まるので一意的である. □

問 16.4. 体 K 上代数的な 2 元 α, α' に対して, 次の 2 つの条件は同値であることを示せ.
(1) $\mathrm{irr}\,(\alpha, K, x) = \mathrm{irr}\,(\alpha', K, x)$.
(2) K 上の同型 $\rho : K(\alpha) \xrightarrow{\sim} K(\alpha')$ で $\alpha^\rho = \alpha'$ となるものがある.

(Hint : (1)⇒(2) は 16.3 の特殊な場合 ($\sigma = \mathrm{id}_K$) である. (2)⇒(1). $p(x) = \mathrm{irr}\,(\alpha, K, x)$, $q(x) = \mathrm{irr}\,(\alpha', K, x)$ とおけば, $p(\alpha') = p(\alpha^\rho) = p(\alpha)^\rho = 0^\rho = 0$ であるから, $p(x) \,|\, q(x)$ がわかる. ここで $q(x)$ の既約性を使ふ.)

定義 16.5. 16.4 の様な性質をもつ 2 元 α, α' は K 上で共役であるといはれる.

さて, 代数的閉包の一意性は次の定理の様に述べられる.

定理 16.6. $\overline{K}, \overline{K'}$ をそれぞれ体 K, K' の代数的閉包とし, $\sigma : K \xrightarrow{\sim} K'$ は体の同型であるとせよ. このとき σ は同型 $\bar{\sigma} : \overline{K} \xrightarrow{\sim} \overline{K'}$ に拡張される. 特に K の 2 つの代数的閉包は互ひに K 上同型である.

これの証明の要点は次の通り. K に含まれない代数的な元を 1 つ添加して, 拡大体 K_1 を得ると 16.3 より, それに応じて K' のある拡大体 K_1' への K_1 からの同型が存在する. 次に, この手続きを K_1 に対して行ふ. 同様な手続きを無限に繰り返せば目的の写像が得られる. 精密な証明を以下の通り.

証明 $\overline{K}/K$ の中間体 L と, L から $\overline{K'}$ の中への同型 $\rho : L \to \overline{K'}$ であつて, σ の拡張であるものの組 (L, ρ) の全体を $\mathscr{L}$ で表す. $\mathscr{L}$ に順序を次の様に入れる :

$$(L_1, \rho_1) \leqq (L_2, \rho_2) \iff L_1 \subset L_2 \text{ かつ } \rho_2 \text{ は } \rho_1 \text{ の拡張.}$$

このとき, $\mathscr{L}$ は半順序集合で, また帰納的であることが次の様にして示される.
いま $\{(L_\lambda, \rho_\lambda) \,|\, \lambda \in \Lambda\}$ を $\mathscr{L}$ の全順序部分集合とするとき, $L = \bigcup_\lambda L_\lambda$ とおく. このとき L は体になることに注意されたい (9.2(2) と比較されたい). $\alpha \in L$ はある L_λ に属し, $\alpha^{\rho_\lambda} \in \overline{K'}$ がきまるが, 順序の定義と全順序性からこれは $\alpha \in L_\lambda$ である限り λ の選び方に依らないことが容易にわかる. そこで α に α^{ρ_λ} を対応させて, L から $\overline{K'}$ の中への同型 $\rho : L \to \overline{K'}$ が得られる. ここで $(L, \rho) \in \mathscr{L}$ かつ $(L_\lambda, \rho_\lambda) \leqq (L, \rho)$ $(\forall \lambda \in \Lambda)$ となることは作り方から明らかである. 以上から Zorn の補題によつて, $\mathscr{L}$ は極大元 (L_0, ρ_0) を持つ. このとき $L_0 = \overline{K}$ で, $\mathrm{Im}\,\rho_0 = \overline{K'}$ となることを示せばよい. いま $\overline{K} \supsetneq L_0$ とし, $\alpha \in \overline{K} - L_0$ とする. 16.3 により $\rho_0 : L_0 \to \overline{K'}$ は $\rho_1 : L_0(\alpha) \to \overline{K'}$ に拡張できる. このとき $(L_0, \rho_0) < (L_0(\alpha), \rho_1)$ となつて (L_0, ρ) の極大性に矛盾する. よつて $L_0 = \overline{K}$ である. また $\mathrm{Im}\,\rho_0 = {L_0}'$ とおけば, $\overline{K} \simeq {L_0}'$ より ${L_0}'$ は代数的閉体である. なぜなら, 任意の $f(x) \in {L_0}'[x]$ の ρ_0 による逆像 $f^{{\rho_0}^{-1}}(x)$ は $\overline{K}$ 上 1 次式だけの積に分解するから, $f(x)$ 自身はそれらの 1 次式の ρ_0 による像の積に分解するからである. 一方, $\overline{K'}/K'$ は代数的で ${L_0}' \supset K'$ であるから $\overline{K'}/{L_0}'$ も代数的で, それゆゑ ${L_0}' = \overline{K'}$ である. □

上の定理の応用として, 次のことが示される.

命題 16.7. $\sigma : K \to \Omega$ を体 K から代数的閉体 Ω の中への同型とし, L/K を任意の代数的拡大とせよ. このとき σ は L から Ω の中への同型 $\rho : L \to \Omega$ に拡張できる.

証明 $\overline{K^\sigma}$ を K^σ の Ω における代数的閉包とせよ. 15.5 により, L の任意の代数的閉包は K の代数的閉包でもあるから, それを $\overline{K}$ と書く. 16.6 により $\sigma : K \xrightarrow{\sim} K^\sigma$ は $\bar{\sigma} : \overline{K} \xrightarrow{\sim} \overline{K^\sigma}$ に拡張できる. $\bar{\sigma}$ の L への制限 $\bar{\sigma}|_L$ を L から Ω の中への写像と見做せば, これが求める ρ である. □

定義 16.8. 以後, 任意の体 K に対して記号 $\overline{K}$ によつて K の 1 つの代数的閉包を表す.

補題 16.9. (重要, 19.15 と関連) $L=K(\alpha)$ を K の単純な代数的拡大とし, $p(x)=\mathrm{irr}\,(\alpha,K,x)$ とおく. このとき, L から K の代数的閉包 $\overline{K}$ の中への K 上の同型の個数は $p(x)$ の異なる根の個数に一致する.

証明 $p(x)$ の異なる根の全体を $\alpha_1,\cdots,\alpha_r$ とする. いま $\sigma:L\to\overline{K}$ が K 上の中への同型であれば, $p(\alpha^\sigma)=p(\alpha)^\sigma=0^\sigma=0$ であるから, α の像は $\alpha_1,\cdots,\alpha_r$ のどれかでなければならない. つまり, 文中の後者の個数は r 以下である. 一方, $K(\alpha_i)\subset\overline{K}$ であるから, 16.3 より L から $\overline{K}$ の中への K 上の $\alpha\mapsto\alpha_i$ なる同型 $\sigma_i:L\to\overline{K}$ （r 個）が定まる. ゆゑに, 実際に r 個の同型が存在する. □

演 習 問 題

16.10. K を体とし, $\mathrm{char}\,K=p>0$ とする. このとき, 写像 $\sigma:K\longrightarrow K,\ \alpha\longmapsto\alpha^p$ は中への同型写像であることを示せ.

16.11. K を体, α,β を K 上代数的な元とする. 次を示せ.

(1) $\mathrm{irr}\,(\alpha,K,x)=\mathrm{irr}\,(\alpha,K(\beta),x)\iff\mathrm{irr}\,(\beta,K,x)=\mathrm{irr}\,(\beta,K(\alpha),x)$

(2) α' を α の K 上の共役元, β' を β の K 上の共役元とせよ. $\mathrm{irr}\,(\alpha,K,x)=\mathrm{irr}\,(\alpha,K(\beta),x)$ であれば, $\sigma(\alpha)=\alpha',\ \sigma(\beta)=\beta'$ となる K 上の同型写像 $\sigma:\ K(\alpha,\beta)\to K(\alpha',\beta')$ が存在する.

(Hint: (1) では $[K(\alpha,\beta):K]$ を 2 通りに表して, 最小多項式の次数と関係づけよ. (2) では 16.3 を利用する.)

16.12. 11.8 の最後に述べた 8 つの写像 $\sigma_i^{\pm}:L\to L\ (i=0,1,2,3)$ のうち, $\sigma:\ \mathbb{Q}(\sqrt{2}\,)\to\mathbb{Q}(\sqrt{2}\,),\ \sqrt{2}\mapsto-\sqrt{2}$ の拡張になつてゐるものをすべて挙げよ.

(ちなみに 11.10 の $f(x)$ は $f_1(x)=x^4-6\sqrt{2}x^2-12x^2+12\sqrt{2}+18$ と $f_2(x)=x^4+6\sqrt{2}x^2-12x^2-12\sqrt{2}+18$ とにより $f(x)=f_1(x)f_2(x)$ と因数分解され α は $f_1(x)$ の根である.)

16.13.* p を素数とする. $K,K'\subset\overline{\mathbb{F}_p}$ は $\mathbb{F}_p$ 上の有限次拡大であるとする. もし $[K:\mathbb{F}_p]=[K':\mathbb{F}_p]$ ならば $K\simeq K'$ であることを示せ.

(Hint : 24.1 を参照されたい.)

§ 17. 最小分解体

多項式の最小分解体とそれらの間の同型写像が関連する種々の問題を解く鍵となる.

定義 17.1. K を体, $f(x)\in K[x]$ とする. K の拡大体 L において $f(x)$ が 1 式のみによる積に分解されるとき L を $f(x)$ の 分解体 といふ. また L が $f(x)$ の分解体であり, かつ, K を含む L のいかなる真の部分体も $f(x)$ の分解体にならないとき, L を $f(x)$ の K 上の 最小分解体 といふ.

最小分解体は常に存在する. 実際, $\overline{K}$ は $f(x)\in K[x]$ の分解体であるが, $\overline{K}$ に含まれる $f(x)$ のすべての根を K に添加した体 $K(\alpha_1,\cdots,\alpha_n)$ は, $f(x)$ の, $\overline{K}$ に含まれる 唯一の 最小分解体である.

定理 17.2. 体の同型写像 $\sigma: K\longrightarrow K'$ があり, $f(x)\in K[x]$ とする. また L, L' はそれぞれ $f(x)$, $f^\sigma(x)$ の K 上, および K' 上の最小分解体とする. このとき, σ は同型 $\tilde{\sigma}: L\longrightarrow L'$ に拡張できる. 特に $K'=K$ とすることで K 上の最小分解体は全て互いに K 上同型であることがわかる.

証明 $\overline{K}$, $\overline{K'}$ をそれぞれ L, L' を含む K, K' の代数的閉包とすると, 16.6 により σ の拡張である同型 $\overline{\sigma}:\ \overline{K}\xrightarrow{\sim}\overline{K'}$ が存在する. いま $f(x)=c_0x^n+c_1x^{n-1}+\cdots+c_n$ $(c_i\in K)$ が $\overline{K}[x]$ において $f(x)=c_0(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ と分解されたとすれば, $L=K(\alpha_1,\cdots,\alpha_n)$ である. また $f^\sigma(x)=c_0{}^\sigma(x-\alpha_1{}^{\overline{\sigma}})(x-\alpha_2{}^{\overline{\sigma}})\cdots(x-\alpha_n{}^{\overline{\sigma}})$ であるから $L'=K'(\alpha_1{}^{\overline{\sigma}},\cdots,\alpha_n{}^{\overline{\sigma}})=L^{\overline{\sigma}}$ である. よつて $\overline{\sigma}$ の L への制限 $\overline{\sigma}|_L: L\xrightarrow{\sim}L'$ は同型を与へ, これは σ の拡張である. □

定義 17.3. 一般に $C=\{f_\lambda(x)\,|\,\lambda\in\Lambda\}\subset K[x]$ に対し, 1 つの拡大体 L/K が全ての $\lambda\in\Lambda$ について $f_\lambda(x)$ の分解体であるとき, L は C の 分解体 であるといひ, K を含む L のいかなる真の部分体も C の分解体ではないとき, L を C の K 上の 最小分解体 といふ.
また L を含む K 代数的閉包 $\overline{K}$ を決めて $S=\{\alpha\in\overline{K}\,|\,\exists\lambda\in\Lambda,\ f_\lambda(\alpha)=0\}$ とすると, $L=K(S)$ は C の K 上の 1 つの最小分解体である.

演 習 問 題

17.4. 次の各多項式の $\mathbb{Q}$ 上の因数分解, および最小分解体とその $\mathbb{Q}$ 上の拡大次数を求めよ.
(1) x^3-1 (2) x^3-2 (3) x^4+5x^2+6 (4) x^6-8

17.5. 拡大 L/K の 2 元 α, β は K 上代数的であるとせよ. $f(x)=\mathrm{irr}\,(\alpha,K,x)$, $g(x)=\mathrm{irr}\,(\beta,K,x)$ とおく. このとき $f(x)$ が $K(\beta)$ 上で既約であることと $g(x)$ が $K(\alpha)$ 上で既約であることは同値であることを示せ. (Hint : $[K(\alpha,\beta):K]$ を考へよ.)

17.6. 多項式 $f(x)=x^6-x^5-x^4-7x^3-3x^2-3x+2$ は $\mathbb{Q}$ 上既約であるか, 理由をつけて答へよ. また, $f(x)$ の最小分解体を具体的に求め, その $\mathbb{Q}$ 上の拡大次数も求めよ.

§ 18. 正規拡大

例題 18.1. 体 K とその代数的閉包 $\overline{K}$ を固定する. 中間体 $K \subset L \subset \overline{K}$ について次の (1) 〜 (4) は同値である.

(1) L から $\overline{K}$ の中への K 上の任意の同型 $\sigma : L \longrightarrow \overline{K}$ に対して, $L^\sigma = L$ である.
(2) 任意の $\sigma \in \mathrm{Aut}\,\overline{K}/K$ に対して $L^\sigma = L$ である.
(3) 任意の $p(x) \in K[x]$ に対し, $p(x)$ が既約で L 内に 1 つでも根を持てば, $p(x)$ は L 上で 1 次式の積に分解する.
(4) L はある $\{f_\lambda(x) \,|\, \lambda \in \Lambda\} \subset K[x]$ の K 上の最小分解体である.

証明 (1)⇒(2). $\sigma \in \mathrm{Aut}\,\overline{K}/K$ の L への制限 $\sigma|_L : L \to \overline{K}$ について, $L = L^{\sigma|_L} = L^\sigma$ となる.
(2)⇒(3). $\overline{K}[x]$ で $p(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$ と分解されるとし, また $\alpha_1 \in L$ とする. このとき各 α_i に対して 16.3 を使ふと, $\alpha_1 \mapsto \alpha_i$ によつて K 上の同型 $\sigma : K(\alpha_1) \tilde{\to} K(\alpha_i)$ が定まる. $K(\alpha_1)$, $K(\alpha_i) \subset \overline{K}$ であるから, これは, 16.6 により K 上の同型 $\overline{\sigma} : \overline{K} \to \overline{K}$ に拡張される. このとき $\overline{\sigma} \in \mathrm{Aut}\,\overline{K}/K$ で, $\alpha_i = \alpha_1{}^{\overline{\sigma}} \in L^{\overline{\sigma}} = L$ となり, $p(x)$ は $L[x]$ で 1 次式の積に分解される.
(3)⇒(4). L の各元 α に対し, $p_\alpha(x) = \mathrm{irr}\,(\alpha, K, x)$ とおけば, 明らかに L は $\{p_\alpha(x) \,|\, \alpha \in L\}$ の K 上の最小分解体である.
(4)⇒(1). $S = \{\alpha \in \overline{K} \,|\, \exists \lambda \in \Lambda, f_\lambda(\alpha) = 0\}$ とすると, $L = K(S)$ である. 任意に与へられた中への K 上の同型 $\sigma : L \to \overline{K}$ に対して $f_\lambda{}^\sigma(x) = f_\lambda(x)$ であるから, σ は $f_\lambda(x)$ の根の集合を不変にし, 従つて $S^\sigma = S$ である. よつて $L^\sigma = K(S^\sigma) = K(S) = L$ となる. □

定義 18.2. 代数的拡大 L/K が 18.1 の条件を満たすとき, L/K は正規拡大 (normal extension) と呼ばれる. 特に, K 上の多項式のある集合の K 上の最小分解体と K 上の正規拡大は同じ概念である.

命題 18.3. 正規拡大性について次が成り立つ.

(1) $K \subset M \subset L$ を体の列とし, L/K が正規拡大なら, L/M も正規拡大である.
(2) L_1, L_2 を $\overline{K}/K$ の中間体とする. L_1/K と L_2/K がともに正規拡大であるとすれば L_1L_2/K も正規拡大である.
(3) M と M' を L/K の中間体とせよ. M'/K が正規拡大ならば MM'/M も正規拡大である.
(つまり, 正規拡大性は持ち上げにより保たれる.)

証明 (1) L/K は代数的であるから, L を含む K の代数的閉包 $\overline{K}$ があるので, $\overline{K} = \overline{M} = \overline{L}$ としてよい. このとき $\mathrm{Aut}\,\overline{K}/K \supset \mathrm{Aut}\,\overline{M}/M$ であるから, $\sigma \in \mathrm{Aut}\,\overline{M}/M$ に対し $L^\sigma = L$. よつて 18.1(2) が成り立つのであるから L/M は正規拡大である.
(2) 任意の K 上の中への同型 $\sigma : L_1L_2 \longrightarrow \overline{K}$ について, $L_i \subset L_1L_2$ ゆゑ, 18.1(1) により $L_i{}^\sigma = L_i$ $(i = 1, 2)$ であり $(L_1L_2)^\sigma = L_1{}^\sigma L_2{}^\sigma = L_1L_2$ となる. 再び 18.1(1) より L_1L_2 は正規拡大である.
(3) $K[x]$ の部分集合 $\{f_\lambda(x) \,|\, \lambda \in \Lambda\}$ があつて, 各 $f_\lambda(x)$ は M' で 1 次式の積に分解され, S をその L における根の全体とすれば $M' = K(S)$ となつてゐる. このとき $f_\lambda(x) \in M[x]$, $MM' = MK(S) = M(S)$ であるから, MM'/M は正規拡大である. □

問 18.4. 18.3 (1) の状況において, 任意の $\alpha \in L$ について, $\mathrm{irr}\,(\alpha, M, x) \,|\, \mathrm{irr}\,(\alpha, K, x)$ であること (12.8 (3) 参照)を用いて, 18.3 (1) の別証を与へよ.

注意 18.5. 18.3 (1) に関連して, 体の拡大の列 $K \subset M \subset L$ で, L/K が正規拡大であつても, M/K は一般には正規拡大にならない. 例へば, $K = \mathbb{Q}$, $M = \mathbb{Q}(\sqrt[3]{2})$, $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$.

問 18.6. 拡大次数が 2 である拡大を 2 次拡大といふ. 次の事を示せ.
(1) 2 次拡大は正規拡大である.
(2) 有理数体 $\mathbb{Q}$ の拡大列 $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2})$ において, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ はともに正規拡大であるが, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ は正規拡大ではない.

注意 18.7. 18.6 (2) より, 一般に, 体の列 $K \subset M \subset L$ において, M/K, L/M がともに正規拡大であつても L/K は正規拡大とは限らない.

問 18.8. $L = K(\alpha_1, \cdots, \alpha_n)$ とする. すべての i について $K(\alpha_i)/K$ が正規拡大であれば, L/K も正規拡大であることを示せ.

問 18.9. $L = K(\alpha_1, \cdots, \alpha_n) \subset \overline{K}$ とする. L/K が正規拡大であるためには, すべての i について $\mathrm{irr}\,(\alpha_i, K, x)$ のどの根も L に属することが必要十分であることを示せ.

命題 18.10. 正規拡大 L/K の中間体 M について M/K は正規拡大であるためには, $\mathrm{Aut}\,L/K$ の任意の元 τ について $M^\tau = M$ となることが必要十分である.

証明 (十分性) $\sigma : M \to \overline{K}$ を任意の中への同型とせよ. 16.7 により, これは $\overline{\sigma} : L \to \overline{K}$ に延長される. L/K は正規拡大なので 18.1(1) から $L^{\overline{\sigma}} = L$ である. つまり $\overline{\sigma} \in \mathrm{Aut}\,L/K$ とみることができる. 仮定から τ として $\overline{\sigma}$ をとれば $M^\sigma = M^{\overline{\sigma}} = M$. 以上と 18.1(1) により M/K は正規拡大である.
(必要性) 任意に $\tau \in \mathrm{Aut}\,L/K$ をとる. これの値域を膨らませて $\tau : L \to \overline{K}$ とみて $\tau|_M : M \to \overline{K}$ を考へる. M/K が正規拡大といふ仮定から $M^\tau = M^{\tau|_M} = M$ が成り立つ. □

演 習 問 題

18.11. 次の代数的拡大は正規であるか否かを理由を付して答へよ. 但し $\omega = \frac{-1+\sqrt{-3}}{2}$ である.
(1) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$
(2) $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$
(3) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$
(4) $\mathbb{Q}(\omega)/\mathbb{Q}$
(5) $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$

18.12. 次の代数的拡大は正規であるか否かを理由を付して答へよ. 但し t は不定元とする.
(1) $\mathbb{F}_5(t)/\mathbb{F}_5(t^3)$
(2) $\mathbb{F}_5(t)/\mathbb{F}_5(t^4)$
(3) $\mathbb{F}_5(t)/\mathbb{F}_5(t^5)$

18.13. 体の拡大の列 $K \subset M \subset L$ で, L/K は正規拡大であるが, M/K が正規拡大でない様な, 18.5 に挙げた例とはできるだけ趣きが異る例を与へよ.

18.14. 体の列 $K \subset M \subset L$ において, M/K, L/M はともに正規拡大であるが L/K は正規拡大ではない様な, 18.7 に挙げた例とは異なる例を与へよ.

§19. 分離性

$\mathbb{Q}$ 上のいかなる既約多項式 $f(x)\in\mathbb{Q}[x]$ も重根を持たない. 同様に p を素数とするとき, $\mathbb{F}_p$ 上のいかなる既約多項式 $f(x)\in\mathbb{F}_p[x]$ も重根を持たない. しかし, 不定元 t について, 多項式 $x^p-t\in\mathbb{F}_p(t)[x]$ は $\mathbb{F}_p(t)$ の代数的閉包の中に根を持つが, それを α ($\alpha^p=t$) とすれば, x^p-t は既約であるにも拘らず, $x^p-t=(x-\alpha)^p$ と因数分解されるので, 重根を持つ. つまり既約多項式であつても重根を持つ場合がある. その様な場合についてまとめて考察しておかう, といふのがこの節の目的である.

但し, Galois 理論の様子を一通り掴むためには, 標数が 0 の場合を主にして学習するといふ道筋もあるので, 余り深入りはしないでおく.

まづ 8.1 で述べたことを思ひ出しておく. 多項式 $f(x)\in K[x]\subset\overline{K}[x]$ の $\overline{K}$ 上での分解が

$$f(x)=c(x-\alpha_1)^{m_1}(x-\alpha_2)^{m_2}\cdots(x-\alpha_r)^{m_r}\quad(c\neq0\text{ で, }\alpha_j\text{ は相異なる})$$

であるとき, 各 α_i は $f(x)$ の m_i 重根, 或いは, α_i の $f(x)$ における重複度は m_i である, といはれる.

定義 19.1. (1) 上の状況で, $m_i>1$ なる α_i は $f(x)$ の 重根 であるといはれる.
(2) 一般に x^n-a の根を a の n 乗根 と呼ぶ.

命題 19.2. $\operatorname{char}K=p>0$ ならば, K の元 a の p^e 乗根は $\overline{K}$ で唯 1 つだけ存在する.
これを $\sqrt[p^e]{a}$ または a^{1/p^e} と書く.

証明 $\operatorname{char}K=p>0$ ゆゑ, $a\in K$, $e\in\mathbb{N}$ に対して α を $x^{p^e}-a$ の 1 つの根とすれば,

$$(x-\alpha)^{p^e}=x^{p^e}-\alpha^{p^e}=x^{p^e}-a$$

となり, α は $x^{p^e}-a$ の p^e 重根である. $\overline{K}$ にて 8.2 を使へば, これ以外の根を持ち得ない. □

定義 19.3. 多項式 $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$ を形式的に微分した多項式

$$na_0x^{n-1}+(n-1)a_1x^{n-2}+\cdots+a_{n-1}$$

を $f'(x)$ または $(f(x))'$ と書き, $f(x)$ の 導函数 と呼ぶ.

問 19.4. 体 K 上の多項式 $f(x)$, $g(x)$ に対し, $(f(x)g(x))'=f'(x)g(x)+f(x)g'(x)$ を示せ.

例題 19.5. $f(x)\in K[x]$, $\alpha\in\overline{K}$ とせよ. 次の (1), (2) が成り立つことを示せ.
(1) α が $f(x)$ の重根 $\iff$ $f(\alpha)=f'(\alpha)=0$ (多項式として $f'(x)=0$ となることも有り得る).
(2) $f(x)$ が既約で $f(\alpha)=0$ とする. α が $f(x)$ の重根 $\iff$ $f'(x)=0$ (多項式として).

証明 (1) ($\Rightarrow$) $f(x)=(x-\alpha)^2g(x)$, $g(x)\in\overline{K}[x]$ とすれば,

$$f'(x)=2(x-\alpha)g(x)+(x-\alpha)^2g'(x)=(x-\alpha)(2g(x)+(x-\alpha)g'(x))$$

となり, $f'(\alpha)=0$ である. ($\Leftarrow$) α が重根でないとき, $f(x)=(x-\alpha)h(x)$, $h(\alpha)\neq0$ となり, $f'(x)=h(x)+(x-\alpha)h'(x)$ であるから, $f'(\alpha)=h(\alpha)\neq0$ である.
(2) ($\Rightarrow$) α が重根ならば $f'(\alpha)=0$ であるが $f'(x)\in K[x]$ ゆゑ, 12.8 によつて $f(x)|f'(x)$. 然るに $\deg f'<\deg f$ ゆゑ, $f'(x)=0$ である. ($\Leftarrow$) 逆に $f'(x)=0$ ならば当然 $f'(\alpha)=0$ であり, (1) より α は $f(x)$ の重根である. □

注意 19.6. 19.5 (2) は $\operatorname{char}K=p>0$ のときに意味を持つ主張である. 実際, このとき, もし $\overline{K}\ni b^{\frac{1}{p}}\notin K$ かつ $b\in K$ なる元があれば x^p-b は $K[x]$ においては既約で, $\alpha=b^{\frac{1}{p}}$ は $f(x)$ の p 重根であり, $f'(x)=px^{p-1}=0$ であることに注意せよ.

定義 19.7. $f(x)\in K[x]$ が $\overline{K}$ で重根を持たないとき, $f(x)$ は分離的であるといはれ, $\alpha\in\overline{K}$ に対し, $\mathrm{irr}(\alpha,K,x)$ が重根を持たないとき, α は K 上(じょう)分離的であるといはれる. 特に K の元は K 上分離的である. 代数的拡大 L/K において, L のすべての元が K 上分離的であるとき, L/K は分離的拡大, 或いは単に分離的であるといはれ, 体 L の部分集合についても, それが K 上に生成する拡大が分離的なとき分離的といふ. 分離的でない状況を非分離的といふ.

問 19.8. 体の列 $K\subset M\subset L$ において, L/K が分離的であれば, L/M も M/K も分離的である. これを示せ.

問 19.9. t を不定元とし, $L=\mathbb{F}_5(t)$ の部分体 $K=\mathbb{F}_5(t^5)$ を考へる. このとき, 多項式 x^5+t^5, $x^{25}+t^5\in K[x]$ はともに K 上既約で, 非分離的であることを示せ.

注意 19.10. $\mathrm{char}\,K=0$ ならば, 任意の $f(x)\in K[x]$, $\deg f(x)\geqq 1$ に対して $f'(x)\neq 0$ となるから, 19.5 (2) により, あらゆる $\alpha\in\overline{K}$ は K 上分離的である. 従つてこの場合は, 拡大体が分離的であるかどうかを気にしなくてよい.

定義 19.11. 体 K のあらゆる代数的拡大が分離的であるとき, K は完全体といはれる.

標数が 0 の体はどれも完全体である. したがつて $\mathrm{char}\,K=p>0$ の場合を問題にする.

命題 19.12. $\mathrm{char}\,K=p>0$, $f(x)\in K[x]$ を既約多項式とする. 次が成り立つ.
(1) 分離的かつ既約な $q(x)\in K[x]$ と整数 $e\geqq 0$ が存在して, $f(x)=q(x^{p^e})$ と表せる.
(2) $\gamma\in\overline{K}$, $f(x)=\mathrm{irr}\,(\gamma,K,x)$ とする. 上の q, e に関し, $\overline{K}$ において γ に K 上共役な元の個数は $\deg q$ に等しい. また γ は $f(x)$ の p^e 重根で γ^{p^e} は K 上分離的である.

証明 (1) $f(x)$ が分離的ならば $e=0$, $q(x)=f(x)$ とすればよい. $f(x)$ が非分離的ならば, 19.5(2) より $f'(x)=0$ となる. いま $f(x)=a_0+a_1x+\cdots+a_nx^n$ とすれば $f'(x)=a_1+\cdots+ia_ix^{i-1}+\cdots+na_nx^{n-1}=0$ ゆゑ $ia_i=0$ である. 従つて $p\nmid i$ ならば $a_i=0$ であり, $f(x)=a_0+a_px^p+a_{2p}x^{2p}+\cdots$ となる. $q_1(x)=a_0+a_px+a_{2p}x^2+\cdots$ とおけば $f(x)=q_1(x^p)$ で $f(x)$ の既約性から $q_1(x)$ も既約である. $q_1(x)$ が非分離的ならば, 同様にして $q_1(x)=q_2(x^p)$ となる $q_2(x)$ があり, $f(x)=q_2(x^{p^2})$ となる. これを続けてゆけば, 最後は $f(x)=q_e(x^{p^e})$ で $q_e(x)$ は分離的かつ既約となる.
(2) $\overline{K}$ 上で $q(x)=(x-\beta_1)\cdots(x-\beta_r)$ とすれば

$$f(x)=q(x^{p^e})=(x^{p^e}-\beta_1)\cdots(x^{p^e}-\beta_r)=(x-{\beta_1}^{1/p^e})^{p^e}\cdots(x-{\beta_r}^{1/p^e})^{p^e},\qquad \gamma={\beta_1}^{1/p^e}$$

となつてゐる. その異なる根の個数は r で, 各根は p^e 重根である. また $\gamma^{p^e}=\beta_1$ は分離的な多項式 $q(x)$ の根ゆゑ K 上分離的である. □

定義 19.13. 19.12 (1) で $r=\deg q$ を $f(x)$ の被約次数と呼び, p^e を $f(x)$ の非分離次数と呼ぶ. それらの積 rp^e は $n=\deg f$ に一致する. 一般に代数的拡大 L/K に対して, L から $\overline{K}$ の中への K 上の同型の個数を分離次数と呼び, $[L:K]_s$ で表す[21].

問 19.14. 19.12 の p, K, γ として, それぞれ, $p=5$, $K=\mathbb{F}_5(t)$, $\gamma=\alpha\,t^{1/25}$ (α は 11.11 のそれ) をとり, $f(x)=\mathrm{irr}\,(\gamma,K,x)$ とする. このとき 19.12 の $q(x)$, e を求めよ.
(まづ $f(x)=x^{75}+t^2x^{25}+t^3$ を示せ. これの既約性については脚注 25) が hint となるであらう.)

[21] 添字の s は separable (分離的) の最初の文字である.

単純拡大については, 次のことがわかる.

例題 19.15. 19.12 の仮定のもとで, $\mathrm{irr}\,(\alpha, K, x)$ の被約次数を r, 非分離次数を p^e とすれば,

$$r = [K(\alpha) : K]_s, \qquad [\,K(\alpha) : K\,] = [\,K(\alpha) : K\,]_s\, p^e$$

が成り立つ. 特に α が K 上分離的であるためには $[\,K(\alpha) : K\,] = [\,K(\alpha) : K\,]_s$ であることが必要十分である. $\mathrm{char}\, K = 0$ のときは, $e = 0$ であるから $0^0 = 1$ と解釈すれば上の等式は成り立つ.

証明 19.12 の記号を用ゐる. $r = [K(\alpha) : K]_s$ は 16.9 による. 順に 12.10(2), 19.12, 16.9 と使つて

$$[K(\alpha) : K] = \deg f = \deg q \cdot p^e = [K(\alpha) : K]_s\, p^e$$

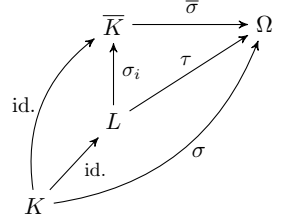
となつて正しい. ここで, 19.12 の証明から, p^e は $f(x)$ の根の重複度であるから, α が K 上分離的であることは $e = 0$ であることに他ならない. よつて後半が示された. □

例題 19.16. L/K は有限次代数的拡大で Ω は代数的閉体であるとせよ. また $\sigma : K \to \Omega$ は中への同型とする. このとき, L から Ω の中への同型 $\rho : L \to \Omega$ で σ の拡張であるものの個数は $[\,L : K\,]_s$ に等しいことを示せ. ($[\,L : K\,]_s$ は σ に依存しない数になることに注意. 19.17(1) の証明で使はれる.)

証明 16.7 により $\sigma : K \to \Omega$ の $\overline{K}$ 上への拡張が存在する. その 1 つを $\overline{\sigma} : \overline{K} \to \Omega$ とする. また $[L : K]_s = r$ とおき $\{\sigma_i \,|\, i = 1, \cdots, r\}$ を L から $\overline{K}$ への中への K 上の同型の全体とせよ. このとき

$$\{\overline{\sigma}\sigma_i \,|\, i = 1, \cdots, r\}$$

が σ の L 上への拡張 $L \to \Omega$ の全てである[22]. 実際, 一方で, これらは互ひに異る写像である. 他方, σ の任意の拡張 $\tau : L \to \Omega$ を考へる. まづ K^σ の Ω 内での代数的閉包は一意的に定まり (15.9 参照), それは $\overline{K^\sigma} = \overline{K}^{\overline{\sigma}}$ に他ならない. ここで, $L^\tau \subset \overline{K^\sigma} = \overline{K}^{\overline{\sigma}}$ であることに注意すれば, $\overline{\sigma}\sigma_i = \tau$ となる σ_i が $\overline{\sigma}^{-1}|_{\overline{K^\sigma}}\,\tau$ として存在する. よつて, L から Ω の中への同型 $\rho : L \to \Omega$ で σ の拡張であるものの個数も r である. □



id. は部分集合としての自身への恒等写像. また, 合成は矢印の辿り方によらず同じ写像である. τ の像は $\overline{\sigma}$ の像 $\overline{K}^{\overline{\sigma}} = \overline{K^\sigma}$ $(\subset \Omega)$ に含まれる.

例題 19.17. (1) 有限次拡大 L/K とその中間体 M に対して, 次が成り立つ :

$$[\,L : K\,]_s = [\,L : M\,]_s [\,M : K\,]_s.$$

(2) L/K が有限次拡大で $p = \mathrm{char}\, K$ ならば, 非負整数 e が存在して次が成り立つ :

$$[\,L : K\,] = [\,L : K\,]_s\, p^e.$$

証明 (1) $\overline{K} = \overline{M} = \overline{L} \supset L$ としてよい. $\{\sigma_i : M \to \overline{K} \mid i \in I\}$ を M から $\overline{K}$ の中への K 上の同型の全体とせよ. このとき $|I| = [\,M : K\,]_s$ である. 各 σ_i に対し $\{\rho_{ij} : L \to \overline{K} \,|\, j \in J_i\}$ をその L への拡張の全体とすれば, 各 i について 19.16 から $|J_i| = [\,L : M\,]_s$ (i に依存しない) となる. このとき $\{\rho_{ij} \,|\, i \in I, j \in J\}$ は L から $\overline{K}$ の中への K 上の同型の全体と一致するから, $[L : K]_s = \sum_{i \in I} |J_i| = \sum_{i \in I} [L : M]_s = [L : M]_s [M : K]_s$ となり, (1) が示された.

(2) 12.14 により, $L = K(\alpha_1, \cdots, \alpha_n)$ で各 α_i は K 上代数的であるとしてよい. いま, $L_0 = K$, $L_i = K(\alpha_1, \cdots, \alpha_i)$ とおき, 体の列 $K = L_0 \subset L_1 \subset \cdots \subset L_n = L$ を考へて, (12.4) を繰り返し用ゐてから 19.15 を使ひ, さらに (1) を繰り返し使へば,

$$[\,L : K\,] = \prod_{i=1}^{n} [\,L_i : L_{i-1}\,] = \prod_{i=1}^{n} [\,L_i : L_{i-1}\,]_s\, p^{e_i} = \left(\prod_{i=1}^{n} [\,L_i : L_{i-1}\,]_s \right) \cdot p^{\sum_i e_i} = [\,L : K\,]_s\, p^e$$

を得る. ここに $e = \sum_i e_i$ である. □

[22] この教科書では 2 つの写像 σ と τ の合成写像 $\tau \circ \sigma$ を $\tau\sigma$ と書くことにする.

系 19.18. 有限次拡大 L/K に対し, $[L:K] \geqq [L:K]_s$ である.

証明 19.17(2) の記号で, $p^e \geqq 1$ だから. □

例題 19.19. α が体 K 上分離的であるためには, $K(\alpha)/K$ が分離的拡大であることが必要十分である. これを証明せよ.

証明 十分性は定義から明らかである. 必要性を対偶で示す. K 上分離的でない $\beta \in K(\alpha)$ が存在する. 19.15 から, $[K(\beta):K] > [K(\beta):K]_s$ である. 19.18 と 19.17(1) により

$$[K(\alpha):K] = [K(\alpha):K(\beta)][K(\beta):K] > [K(\alpha):K(\beta)]_s[K(\beta):K]_s = [K(\alpha):K]_s.$$

ゆゑに 19.15 によつて α は K 上分離的ではない. □

有限次拡大 L/M に対し, $[L:K]_i = \dfrac{[L:K]}{[L:K]_s}$ と定め[23], L/K の 非分離次数 と呼ぶ. 従つて

$$[L:K] = [L:K]_s\,[L:K]_i$$

である. ここで 19.15 から $[L:K]_i$ は K の標数 p の冪である. また $K \subset M \subset L$ のとき,

$$[L:K]_i = [L:M]_i[M:K]_i$$

が成り立つ.

後の便宜のために, 19.19 を一般化した次の定理を示しておく.

定理 19.20. $L = K(\alpha_1, \ldots, \alpha_n)$ を K の有限次拡大とせよ. 次の 4 つは同値である.
(1) L/K は分離的拡大である.
(2) α_i $(1 \leqq i \leqq n)$ はすべて K 上分離的である.
(3) 各 α_i は $K(\alpha_1, \cdots, \alpha_{i-1})$ 上分離的である.
(4) $[L:K] = [L:K]_s$.

証明 (1)⇒(2). 分離的拡大の定義より明らかである. (2)⇒(3). $L_i = K(\alpha_1, \ldots, \alpha_i)$ とおく. α_i は K 上分離的だから, $\mathrm{irr}\,(\alpha_i, K, x)$ は重根を持たない. よつて $\mathrm{irr}\,(\alpha_i, L_{i-1}, x)$ も重根を持たない. ゆゑに α_i は L_{i-1} 上分離的である. (3)⇒(4). 19.17(2) の証明において, 各 $e_i = 0$ となるから $e = 0$ となる. (4)⇒(1). 対偶を証明する. L は K 上非分離的な元 α を含むと仮定する. 体の列 $K \subset K(\alpha) \subset L$ において 19.15 の後半と 19.18 とから,

$$[K(\alpha):K] > [K(\alpha):K]_s, \quad [L:K(\alpha)] \geqq [L:K(\alpha)]_s$$

であるから, $[L:K] > [L:K]_s$ を得る. □

補題 19.21. 体の列 $K \subset M \subset L$ において, M/K, L/M がともに分離的拡大ならば L/K も分離的拡大である. また, この逆も成り立つ.

証明 逆は 19.8 に他ならない. そこで, M/K, L/M はともに分離的であるとする. $\alpha \in L$ に対して $\mathrm{irr}\,(\alpha, M, x) = x^n + \alpha_1 x^{n-1} + \cdots + \alpha_n$ $(\alpha_i \in M)$ とすれば, これは重根を持たない. よつて, 体 $K(\alpha_1, \cdots, \alpha_n, \alpha)$ は 19.20(3) の条件をみたす. ゆゑに, 19.20 (3)⇒(1) から $K(\alpha_1, \cdots, \alpha_n, \alpha)$ は K 上分離的である. 特に α は K 上分離的で, L/K は分離的である. □

問 19.22. t を不定元とする. 次の拡大は分離的であるか否か, 理由を付けて答へよ. (18.12 参照)
(1) $\mathbb{F}_5(t)/\mathbb{F}_5(t^3)$ (2) $\mathbb{F}_5(t)/\mathbb{F}_5(t^4)$ (3) $\mathbb{F}_5(t)/\mathbb{F}_5(t^5)$

[23] i は inseparable (非分離的) の頭文字

問 19.23. M, M' が代数的拡大 L/K の中間体であるとき, 次のことを示せ.
(1) M/K が分離的ならば, MM'/M' も分離的. (即ち, 拡大の分離性は持ち上げによつて保たれる.)
(Hint : 任意の $\alpha \in MM'$ に対し, 有限個の $\alpha_1, \cdots, \alpha_n \in M$ が存在して, $\alpha \in M'(\alpha_1, \cdots, \alpha_n)$ となる.)
(2) M/K, M'/K がともに分離的ならば, MM'/K も分離的である.

代数的拡大 L/K において, K 上分離的な L の元の全体を $K^{s,L}$ で表す. ここで 19.20 (2)⇒(1) により, α, $\beta \in K^{s,L}$ ならば $K(\alpha,\beta)$ は K 上分離的で, 従つて $\alpha \pm \beta$, $\alpha\beta \in K^{s,L}$ で $\alpha\beta^{-1} \in K^{s,L}$ $(\beta \neq 0)$ となり, $K^{s,L}$ は L の部分体である. 実際 $K^{s,L}$ は K 上分離的な L/K の中間体のうち最大なものである.

定義 19.24. 上の状況において $K^{s,L}$ を K の L における 分離閉包 といふ. また $K^{s,L} = K$ となる自明でない拡大 L/K を 純非分離的拡大 であるといふ. この教科書では, 自明な拡大 K/K は分離的であるが, 純非分離的ではないものとする.

例題 19.25. 自明でない代数的拡大 L/K について, 次の 3 つは同値.
(1) L/K は純非分離的拡大である.
(2) 任意の $\alpha \in L$ に対し, $\alpha^{p^e} \in K$ となる $e \geqq 0$ がある. 但し $p = \operatorname{char} K$ で, e は α に依存してよい.
(3) $[L:K]_s = 1$.

証明 (1)⇒(2). 19.12 (2) より, ある $e \geqq 0$ に対し α^{p^e} は K 上分離的ゆゑ, $\alpha^{p^e} \in K$ となる.
(2)⇒(3). L を含む K の代数的閉包を $\overline{K}$ とし, $\sigma : L \to \overline{K}$ を中への K 上の同型とする. $\alpha \in L$ に対して $\alpha^{p^e} \in K$ とすれば $(\alpha^{p^e})^\sigma = \alpha^{p^e}$ ゆゑ, $(\alpha^\sigma - \alpha)^{p^e} = (\alpha^\sigma)^{p^e} - \alpha^{p^e} = (\alpha^{p^e})^\sigma - \alpha^{p^e} = 0$ となり, $\alpha^\sigma = \alpha$. 従つて σ は L の各元をそれ自身に写す. よつて $[L:K]_s = 1$ となる.
(3)⇒(1). K 上分離的な任意の $\alpha \in L$ について, 19.20(4) および 16.7 より,

$$[K(\alpha):K] = [K(\alpha):K]_s \leqq [L:K]_s = 1$$

ゆゑ $K(\alpha) = K$ である. つまり $\alpha \in K$ となる. ゆゑに L/K は純非分離的である. □

例題 19.26. 代数的拡大 L/K と, L における K の分離閉包 $K^{s,L}$ について次が成り立つ.
(1) $L = K^{s,L}$ であるか, または $L/K^{s,L}$ は純非分離的拡大である. つまり $(K^{s,L})^{s,L} = K^{s,L}$.
(2) L/K が有限次拡大ならば, 次の等式が成り立つ :

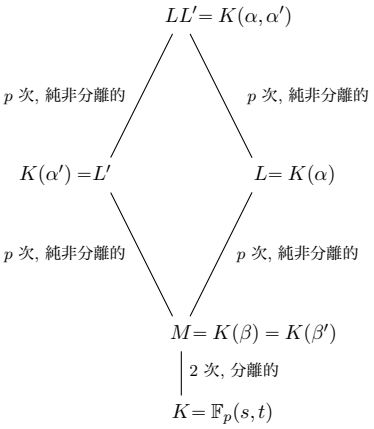
$$[L:K]_s = [K^{s,L}:K], \quad [L:K]_i = [L:K^{s,L}].$$

証明 (1) $K^{s,L}$ 上分離的な任意の $\alpha \in L$ について 19.19 (必要性) より, $K^{s,L}(\alpha)/K^{s,L}$ は分離拡大である. $K^{s,L}/K$ も分離拡大であるから, 19.21 により $K^{s,L}(\alpha)/K$ は分離拡大である. $K^{s,L} \supset K(\alpha)$ ゆゑ, 19.19 から $K(\alpha)/K$ も分離拡大である. 再び 19.19 (十分性) より α は K 上分離的である. つまり $(K^{s,L})^{s,L} \subset K^{s,L}$. 逆の包含関係は明かだから $(K^{s,L})^{s,L} = K^{s,L}$. それゆゑ $L \neq K^{s,L}$ のときは, 定義により $L/K^{s,L}$ は純非分離的拡大である.
(2) 19.17(1) によれば $[L:K]_s = [L:K^{s,L}]_s [K^{s,L}:K]_s$ である. この式において, (1) と 19.25 を使へば $[L:K^{s,L}]_s = 1$. また $K^{s,L}/K$ は分離的であるから 19.20(1)⇒(4) により $[K^{s,L}:K]_s = [K^{s,L}:K]$ となり, $[L:K]_s = [K^{s,L}:K]$ である. $[L:K]_i$ については (1) と (12.4) を使へば

$$[L:K]_i = \frac{[L:K]}{[L:K]_s} = \frac{[L:K^{s,L}][K^{s,L}:K]}{[K^{s,L}:K]} = [L:K^{s,L}]$$

となり正しい. □

例 19.27. p を奇素数とする. 標数 p の体で, 非分離的かつ正規でない拡大の例を挙げておく[24]. s と t を 2 つの不定元とし, $K=\mathbb{F}_p(s,t)$ とおく. $x^2-sx+t\in K[x]$ は K 上既約である[25] が, その 2 つの根を β, β' とおく. $M=K(\beta)(=K(\beta'))$ とする. M 上非分離的かつ既約[26] な $x^p-\beta\in M[x]$ の根を α とおき, $L=M(\alpha)$ とおく. もちろん $L=K(\alpha)$ でもある. このとき, 拡大 L/K は正規拡大ではない. 実際, もしこれが正規であれば, K 上既約[27] な $(x^p-\beta)(x^p-\beta')=x^{2p}-sx^p+t\in K[x]$ が $\mathrm{irr}\,(\alpha,K,x)$ に他ならず, $x^p-\beta'$ の根 α' が L 内に存在する. このとき $s=(\alpha+\alpha')^p$, $t=(\alpha\alpha')^p$ ゆゑ L は 2 つの異なる p 次拡大 $K(\alpha+\alpha')/K$, $K(\alpha\alpha')/K$ を含む. これより $2p=[L:K]\geqq p^2$ となつて矛盾を生じる. ゆゑに L/K は正規拡大ではない. これらの拡大を含めて図示すれば, 右の様になる. LL'/K は正規拡大である.



演 習 問 題

19.28. ($[L:K]$ と $[L:K]_s$ が異なる例) t は不定元とし, $K=\mathbb{F}_5(t^{25})$,

$$f(x)=x^{75}+t^{25}x^{50}+2\,t^{50}x^{25}-t^{75}$$

とおく. 体 $L=\mathbb{F}_{25}(t)$ は $f(x)$ の K 上の最小分解体であること示せ[28]. また $[L:K]_s$, $[L:K]_i$, $[L:K]$ はそれぞれいくつか. さらに $K^{s,L}$ を明示的に記述せよ.

19.29. $x^2+x+1\in\mathbb{F}_5[x]$ の根の 1 つを α とし t を不定元として, $K=\mathbb{F}_5(t^5)$ とおく. 拡大 $\mathbb{F}_5(\alpha,t)/K$ について以下の問に答へよ.

(1) α^5, $\alpha+\alpha^5$, $\alpha\alpha^5$ を α の $\mathbb{F}_5$ 上の 1 次以下の多項式で表せ. (参考 : 16.10)

(2) $\alpha^{25}=\alpha$ であることを示せ.

(3) 最小多項式 $f(x)=\mathrm{irr}\,(t+1,K,x)$, $g_1(x)=\mathrm{irr}\,(t+\alpha,K(t),x)$, $g_2(x)=\mathrm{irr}\,(t+\alpha,K(\alpha),x)$, $g(x)=\mathrm{irr}\,(t+\alpha,K,x)$ を求めよ.

(4) $[K(t+\alpha):K]$ と $[K(t+\alpha):K]_s$ はいくらか.

19.30. 3 つの体 $L\supset M\supset K$ について, L/M は正規拡大, M/K は純非分離的拡大であるとせよ. このとき, L/K は正規拡大であることを示せ.

19.31. M は代数的拡大 L/K の中間体であるとする. 次の問に答へよ.

(1) $(K^{s,M})^{s,L}=K^{s,L}$ であることを示せ.

(2) $K^{s,L}\subset M^{s,L}$ であることを示せ.

(3) $K\subsetneq K^{s,L}\subsetneq M^{s,L}\subsetneq L$ となる例を挙げよ.

---

[24] D. S. Dummit, R. M. Foote : Abstract Algebra（第 3 版), Wiley 社, p.652, §14.9, Exercise 3 より. 分離的かつ正規でない例は 18.12(1), 非分離的かつ正規な例は 18.12(3) にある.

[25] 一般に, 可換環 R は, その零元と単元以外のあらゆる元が既約元の積に (単元の積を無視して) 一意的に分解できるとき, 一意分解環 (UFD) と呼ばれる. 19.27 において $K[s,t]$ は UFD （[N], p.106, 定理 26.13）である. ゆゑに x^2-sx+t が可約であれば, UFD 上の多項式に関する Gauss の補題（[N], p.105, 補題 26.9(1)）により, その根の組は $\{1,t\}$ または $\{-1,-t\}$ であるから, $s=\pm(1+t)$ となり矛盾である.

[26] $\mathbb{F}_p[\beta]$ （$\mathbb{F}_p$ 上の 1 変数多項式環）内での素 ideal (β) に関する Eisenstein の判定法で示される.

[27] $\mathbb{F}_p[s,t]$ の極大 ideal (s,t) に関する Eisenstein の判定法で示される.

[28] $\mathbb{F}_{25}$ について, 詳しくは第 24 で学ぶが, ここでは $\mathbb{F}_{25}=\mathbb{F}_5[x]/(x^2+3x+3)$ と理解していただきたい.

§ 20. 分離的拡大の単純性

あとで 22.12 の証明に用ゐるために, この節では有限次の分離的拡大は単純拡大であることを証明する. 実際は, もつと一般に次の定理が成り立つ.

定理 20.1. 体 K の有限次拡大 $L=K(\alpha_1,\cdots,\alpha_{n-1},\alpha_n)$ において(12.14 に注意), α_1, …, α_{n-1} がすべて K 上分離的ならば, $L=K(\theta)$ となる $\theta\in L$ がある.

証明 K が有限体ならば L も有限体で, その乗法群 $L^\times=L-\{0\}$ は, 「代数学 1」の系 13.6 より, 巡回群である. $L^\times=\langle\theta\rangle$ とすれば, 明らかに $L=K(\theta)$ である.

また, 主張は $n=2$ のときに示されれば, 一般の場合は n に関する帰納法で示される. 実際, $K(\alpha_1,\cdots,\alpha_{n-2},\alpha_n)=K(\beta)$ となれば, $L=K(\alpha_{n-1},\beta)$ となるから, $n=2$ の場合に帰着する.

よつて以下では K を無限体とし, $L=K(\alpha,\beta)\subset\overline{K}$, α は K 上分離的であると仮定する. $[L:K]_s=m$ とし, $\sigma_i: L\to\overline{K}$ $(1\leqq i\leqq m)$ を中への異なる K 上の同型とする. このとき $i\neq j$ ならば $\alpha^{\sigma_i}\neq\alpha^{\sigma_j}$ か $\beta^{\sigma_i}\neq\beta^{\sigma_j}$ となるから, x についての多項式

$$f(x):=\prod_{i\neq j}\big((\alpha^{\sigma_i}-\alpha^{\sigma_j})+(\beta^{\sigma_i}-\beta^{\sigma_j})x\big)$$

は[29] 0 と異なる. $f(x)=0$ の根は有限個であるが, $|K|=\infty$ であるから, $f(c)\neq 0$, $c\neq 0$ なる元 $c\in K$ がある. このとき $i\neq j$ ならば

$$0\neq(\alpha^{\sigma_i}-\alpha^{\sigma_j})+(\beta^{\sigma_i}-\beta^{\sigma_j})c=(\alpha+c\beta)^{\sigma_i}-(\alpha+c\beta)^{\sigma_j}.$$

よつて $\theta=\alpha+c\beta$ とおけば

$$i\neq j\Rightarrow\theta^{\sigma_i}\neq\theta^{\sigma_j}$$

となり, θ は少なくとも m 個の K 上共役な元を持つ. 従つて $m\leqq[K(\theta):K]_s\leqq[L:K]_s=m$ となり, $[K(\theta):K]_s=[L:K]_s$ を得る. いま L, $K(\theta)$ における K の分離閉包 $K^{s,L}$, $K^{s,K(\theta)}$ について, $K^{s,K(\theta)}\subset K^{s,L}$ であるが,[30] 上の等式と 19.26(2) より

$$[K^{s,L}:K]=[L:K]_s=[K(\theta):K]_s=[K^{s,K(\theta)}:K]$$

であるから $K^{s,L}=K^{s,K(\theta)}$ を得る. このことと $\alpha\in L$ が K 上分離的であることとから, $\alpha\in K^{s,L}=K^{s,K(\theta)}\subset K(\theta)$ である. また $\beta=c^{-1}(\theta-\alpha)\in K(\theta)$ となるから $K(\alpha,\beta)\subset K(\theta)$ を得る. □

注意 20.2. 上記の証明においては α を θ で具体的に表す方法が不明であるが, m がわかる場合は, 次の様にすればよい. 1, θ, θ^2, …, θ^{m-1} は L/K の基であるが, これらを L/K の基 $\{\alpha^i\beta^j\}(\ni\alpha)$ で表すことができるから, それを解くことで得られる.

系 20.3. 有限次拡大 L/K が分離拡大であれば, それは単純拡大である.

証明 12.14 (1)⇒(2) により $L=K(\alpha_1,\cdots,\alpha_n)$ と書ける. ここで仮定より α_1, …, α_n は K 上分離的である. 従つて 20.1 により結論を得る. □

演 習 問 題

20.4. 次のそれぞれの拡大について, 単純拡大として生成する元を 1 つ求めよ.

(1) $\mathbb{Q}(\sqrt{2},\sqrt{5})/\mathbb{Q}$ (2) $\mathbb{Q}(\sqrt{2},\sqrt{3},i)/\mathbb{Q}$

[29] $f(x)\in K[x]$ となるが, ここではそれは必要ない.
[30] ここまでは α が分離的であることを一切使つてゐない.

§ 21. 完全体

前に 19.10 で述べた様に, 標数 0 の体はすべて完全体であるから, この節では $\operatorname{char} K = p > 0$ なる体 K についてのみ考へる. $\overline{K}$ を K の代数的閉包とする. また

$$K^p = \{\, a^p \,|\, a \in K \,\}, \quad K^{1/p} = \{\, a^{1/p} \in \overline{K} \,|\, a \in K \,\} = \{\, \alpha \in \overline{K} \,|\, \alpha^p \in K \,\}$$

と記すことにすると, これらは体であつて, $K^p \subset K \subset K^{1/p}$ となつてゐる.

定理 21.1. 次の 3 つの条件は同値である.
(1) K は完全体である.
(2) $K^{1/p} = K$.
(3) $K^p = K$.

証明 (1)⇒(2). 拡大 $K^{1/p}/K$ が自明でないとする. $K^{1/p}$ の定義により, 拡大 $K^{1/p}/K$ について 19.25(2) が成り立つ. よつて 19.25(1) から $K^{1/p}/K$ は純非分離的拡大となる. しかるに, K が完全体ゆゑ $K^{1/p}/K$ は純非分離的拡大ではあり得ず, 矛盾である. 従つて $K^{1/p} = K$.
(2)⇒(3). $a \in K$ を任意にとれば $a = (a^{1/p})^p$. ここで $K = K^{1/p}$ ならば $a^{1/p} \in K$ ゆゑ, $a \in K^p$ となる. ゆゑに $K \subset K^p$, 即ち $K = K^p$ である.
(3)⇒(1). $\alpha \in \overline{K}$ が K 上非分離的であれば, 19.12(1) の証明で述べたことから,

$$f(x) := \operatorname{irr}(\alpha, K, x) = (x^p)^m + a_1(x^p)^{m-1} + \cdots + a_m \quad (\, a_i \in K \,)$$

の形に書かれる. ここで各 a_i に対し $b_i{}^p = a_i$ なる $b_i \in K$ があるから

$$f(x) = (x^m + b_1 x^{m-1} + \cdots + b_m)^p$$

となり, $f(x)$ の既約性に矛盾する. よつて $\overline{K}/K$ は分離的である. □

例題 21.2. 有限体は完全体である.

証明 K を有限体とし, その標数を $p > 0$ とせよ. このとき $\sigma : K \to K$ $(a \mapsto a^p)$ は単射であるが, $|K| < \infty$ により全射となる. よつて K は 21.1 の条件を満たす. □

演 習 問 題

21.3. p を素数, t を不定元とせよ. 体 $\mathbb{F}_p(t)$ の上の非分離的拡大体を 1 つ挙げ, この体が完全体でないことを示せ. さらに 21.1 (2), (3) が成り立たないことを確認せよ.

21.4. p を素数, t を不定元とせよ. $K = \bigcup_{n=1}^{\infty} \mathbb{F}_p(t^{1/p^n})$ は完全体であることを示せ.

(注意 : K を含む K の代数的閉包 $\overline{K}$ において, K は $\mathbb{F}_p(t)$ 上非分離的な元の全てを集めたもの.)

§ 22. Artin の定理

ここでは次節に述べる Galois の基本定理の証明の核心部分となる事柄を述べる.

定義 22.1. 代数的拡大 L/K (有限次とは限らない) が分離的かつ正規であるとき, これを Galois 拡大 と呼び, $\mathrm{Aut}\,L/K$ をその Galois 群 と呼んで $\mathrm{Gal}\,(L/K)$ で表す.

命題 22.2. M, M' を拡大 L/K の中間体とせよ. M'/K が Galois 拡大ならば MM'/M も Galois 拡大である. さらに M/K も Galois 拡大ならば MM'/K は Galois 拡大.

証明 前半は, 正規性も分離性も拡大に関する持ち上げによつて保たれる (18.3 (3) と 19.23 (1)) からである. 後半は 18.3(2) と 19.23(2) からわかる. □

定義 22.3. 一般に拡大 L/K に対して, $G=\mathrm{Aut}\,L/K$ とおく.
(1) G の部分群 H をとり固定する. このとき, L の部分集合 L^H を次の様に定める :

$$L^H=\{\,\alpha\in L\mid \alpha^\sigma=\alpha\ \ (\forall\sigma\in H)\,\}.$$

これは L/K の中間体になる. これを L における H の 不変体 (または 固定体) と呼ぶ.
(明らかに $L^G\supset K$ だが, L/K が Galois 拡大の時は $L^G=K$ (22.7 (2) 参照.))
(2) 逆に, 拡大 L/K の中間体 M に対して, G の部分集合 G^M を次の様に定める :

$$G^M=\{\,\sigma\in G\mid \alpha^\sigma=\alpha\ \ (\forall\alpha\in M)\,\},\quad (\text{特に } G^K=G).$$

これは G の部分群であり, G における M の 不変群 (または 固定群) と呼ばれる.

問 22.4. 上の集合 L^H が体であり, G^M が G の部分群であることを示せ.

例題 22.5. M が Galois 拡大 L/K の中間体であれば, L/M はまた Galois 拡大であることを示せ.

証明 $L/M=ML/M$ ゆゑ L/M は L/K の持ち上げであり, 22.2 により Galois 拡大である. □

例題 22.6. 拡大 L/K について, $\mathrm{Aut}\,L/M=(\mathrm{Aut}\,L/K)^M$ となることを示せ. L/K が Galois 拡大のときは, 22.5 とこのことを合はせて $\mathrm{Gal}\,(L/M)=\mathrm{Gal}\,(L/K)^M$ が成り立つ.

証明 $\mathrm{Aut}\,L/M\subset\mathrm{Aut}\,L/K=G$ であるが, $\sigma\in G$ に対し $\sigma\in\mathrm{Aut}\,L/M\iff\alpha^\sigma=\alpha\ (\forall\alpha\in M)\iff\sigma\in G^M$ となる. □

命題 22.7. L/K を有限次 Galois 拡大, $G=\mathrm{Gal}\,(L/K)$ とする. 次が成り立つ.
(1) $[L:K]=[L:K]_s=|G|$.
(2) $L^G=K$. さらに一般的に L/K の中間体 M について $\boxed{L^{G^M}=M}$.

証明 (1) 拡大 L/K は分離だから 19.20 の (1) と (4) の同値性により $[L:K]=[L:K]_s$. また, L を含む K の代数的閉包を $\overline{K}$ とし, $\sigma:L\to\overline{K}$ を $\overline{K}$ の中への K 上の同型とすれば, 正規性により $L^\sigma=L$ となる. よつて σ の終域を L に制限して $\sigma:L\xrightarrow{\sim}L$ なる $\mathrm{Gal}\,(L/K)$ の元が得られる. 逆に $\mathrm{Gal}\,(L/K)\ni\rho:L\xrightarrow{\sim}L$ の終域を $\overline{K}$ に拡張すれば中への K 上の同型 $\rho:L\to\overline{K}$ が得られる. 従つて $|\mathrm{Gal}\,(L/K)|=[L:K]_s$ である.
(2) $K\subset L^G\subset L$ で, 22.5 により L/L^G は Galois 拡大で, $\mathrm{Gal}\,(L/L^G)\underset{22.6}{=}G^{L^G}=G$ (G は L^G の元を動かさないから) であり, (1) より $[L:L^G]\underset{(1)}{=}|\mathrm{Gal}(L/L^G)|=\left|G^{L^G}\right|=|G|\underset{(1)}{=}[L:K]$ ゆゑ, $L^G=K$ である. 次に, まづ 22.6 より $G^M=\mathrm{Gal}(L/M)$ である. L/K を L/M に取り換へると, G が G^M に変る. これについて同じ議論を行へば後半を得る : $L^{G^M}=L^{\mathrm{Gal}(L/K)^M}\underset{22.6}{=}L^{\mathrm{Gal}(L/M)}\underset{\text{直前と同様の推論}}{=}M$. □

問 22.8. 22.3 の状況で L/K が, 正規でなく分離的な拡大の場合, 正規かつ非分離的な拡大の場合のそれぞれについて, $L^G \supsetneqq K$ である様な例を与へよ.

問 22.9. $L=\mathbb{Q}(\sqrt[3]{2},\omega)$ (但し $\omega=\frac{-1+\sqrt{-3}}{2}$) と $K=\mathbb{Q}$ について,

(1) L/K が Galois 拡大であることを示せ.

(2) 以下 $G=\mathrm{Gal}(L/K)$ とおく. G の要素をすべて記述せよ.

(3) $M_0=\mathbb{Q}(\sqrt[3]{2})$, $M_1=\mathbb{Q}(\sqrt[3]{2}\omega)$, $M_2=\mathbb{Q}(\sqrt[3]{2}\omega^2)$ について G^{M_0}, G^{M_1}, G^{M_2} を求めよ.

(4) $\sigma\in G$ を $\sqrt[3]{2}\longmapsto\sqrt[3]{2}\omega$, $\omega\longmapsto\omega$ で定まる元とし, H を σ で生成される G の部分群とせよ: $H=\langle\sigma\rangle$. このとき L^H を求めよ.
(Hint : L/K の基底として $\{\omega,\omega^2,\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2,\sqrt[3]{2}^2\omega,\sqrt[3]{2}^2\omega^2\}$ がとれることを利用せよ.)

(5) $\tau\in G$ を $\sqrt[3]{2}\longmapsto\sqrt[3]{2}$, $\omega\longmapsto\omega^2$ で定まる元とし, D を τ で生成される G の部分群とせよ: $D=\langle\tau\rangle$. このとき L^D を求めよ.
(Hint : L/K の基底として $\{1,\sqrt[3]{2},\sqrt[3]{2}^2,\omega,\sqrt[3]{2}\omega,\sqrt[3]{2}^2\omega\}$ がとれることを利用せよ.)

定理 22.10. (Artin の定理) L が 体, G が $\mathrm{Aut}\,L$ の有限部分群, $K=L^G$ のとき, 次が成り立つ.

(1) L/K は有限次 Galois 拡大である.

(2) $\mathrm{Gal}\,(L/K)=G$.

(3) $[L:K]=|G|$.

注意 22.11. $|G|=\infty$ のときは, 22.10 の (1), (2), (3) は必ずしも成立しない. 22.19 参照.

この定理を示すために次の補題を用意する.

補題 22.12. 代数的拡大 L/K は分離的とし, n を固定された自然数とする. このとき, すべての $\alpha\in L$ に対して $[K(\alpha):K]\leqq n$ が成り立つならば, $[L:K]\leqq n$ である.

証明 L/K が有限次拡大であることは仮定されてゐないので, 少し工夫が要る. $[K(\alpha):K]$ が最大となる $\alpha\in L$ を 1 つ選び, $[K(\alpha):K]=m$ とおく. (もちろん $m\leqq n$ である.) もし $L\neq K(\alpha)$ ならば, $\beta\in L-K(\alpha)$ をとれ. L/K は分離的拡大なので 19.8 により $K(\alpha,\beta)/K$ は分離的な代数的拡大であつて, 20.3 より, ある $\gamma\in L$ によつて $K(\alpha,\beta)=K(\gamma)$ と書ける. このとき $[K(\gamma):K]=[K(\alpha,\beta):K]>[K(\alpha):K]=m$ となるので, α の選び方に反する. よつて $L=K(\alpha)$ であり, 結論を得る □

これを用ゐて 22.10 の証明を行ふ.

証明 任意に $\alpha\in L$ とる. α を含む G 軌道[31] を $\alpha^G=\{\alpha=\alpha_1,\alpha_2,\cdots,\alpha_r\}$ とし,

$$f(x)=\prod_{i=1}^{r}(x-\alpha_i)=x^r+c_1x^{r-1}+\cdots+c_r$$

とおく. 任意の $\sigma\in G$ について $\{\alpha_1{}^\sigma,\alpha_2{}^\sigma,\cdots,\alpha_r{}^\sigma\}=\{\alpha_1,\alpha_2,\cdots,\alpha_r\}(=\alpha^G)$ であることに注意されたい. このとき, $r\leqq|G|$ で, 任意の $\sigma\in G$ に対して $f^\sigma(x)=\prod_{i=1}^{r}(x-\alpha_i{}^\sigma)=f(x)$ となるから, 各 $c_i\in L^G=K$ となり, $f(x)\in K[x]$ である. $f(\alpha)=0$ であるから, $\mathrm{irr}\,(\alpha,K,x)|f(x)$ である. ここで $f(x)$ は重根を持たないから α は K 上分離的ゆゑ, 19.7 によつて L/K は分離的拡大である. また $\mathrm{irr}\,(\alpha,K,x)$ は L 上で 1 次式の積に分解でき, α は L の任意の元であつたから, 18.1(3), 18.2 により L/K は正規拡大, よつて Galois 拡大である. 上の議論から $[K(\alpha):K]=\deg\mathrm{irr}\,(\alpha,K,x)\leqq r\leqq|G|$ $(\forall\alpha\in L)$ であり, 22.12 により $[L:K]\leqq|G|$. よつて L/K は有限次拡大である. 一方 $G\subset\mathrm{Gal}(L/K)$ で, 22.7(1) より $[L:K]=|\mathrm{Gal}(L/K)|$ であるから $G=\mathrm{Gal}(L/K)$ で $[L:K]=|G|$ である. □

[31] 群 G が集合 X に 作用 (34.1 を見よ) してゐるとし, $\alpha\in X$ とせよ. 集合 $\{\alpha^g\,|\,g\in G\}$ を α の G 軌道 といひ, 通常 α^G と記す. 任意の $\tau\in G$ に対し $(\alpha^G)^\tau=\alpha^G$ が成り立つことは容易に証明される.

演 習 問 題

22.13. 体 K 上の代数的な元 α と $\alpha+1$ が K 上共役であれば, $\operatorname{char} K \neq 0$ であることを示せ.

22.14. 有限次拡大 L/K に対し, 次の問に答へよ.
(1) L を含む K の最小の正規拡大（L/K の K 上の 正規閉包 と呼ばれる）が存在することを示せ.
(2) L/K が分離的拡大のとき, L を含む K の最小の有限次 Galois 拡大（L/K の K 上の Galois 閉包 と呼ばれる）が存在することを示せ.

22.15. p を素数, $f(x)=x^p-x-1\in\mathbb{F}_p[x]$ とする.
(1) $f(x)=0$ の 1 つの根を α とせよ. このとき, $\operatorname{Aut}\mathbb{F}_p(\alpha)/\mathbb{F}_p$ は $\alpha\mapsto\alpha+r$ $(r=0,1,\cdots,p-1)$ で尽くされることを示せ. （Hint: $\alpha+1=\alpha^p$ であることと 10.3. ）
(2) 多項式 $f(x)$ は $\mathbb{F}_p$ 上既約であること, および $\mathbb{F}_p(\alpha)/\mathbb{F}_p$ が Galois 拡大であることを示せ.
（この拡大 $\mathbb{F}_p(\alpha)/\mathbb{F}_p$ は Artin-Schreier の拡大 と呼ばれるものの一つである. ）

22.16. 体 $L=\mathbb{Q}(\sqrt{2},\sqrt{3})$ を考へる. 次の問に答へよ.
(1) 拡大 $L/\mathbb{Q}$ が Galois 拡大であることを示せ, さらに, 任意の a, b, c, $d\in\mathbb{Q}$ に対して,
$$\sigma: a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\mapsto a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6},$$
$$\tau: a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}\mapsto a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6}$$
は L の $\mathbb{Q}$ 上の自己同型であり, $\operatorname{Gal}(L/\mathbb{Q})=\{\mathrm{id},\sigma,\tau,\sigma\tau\}$ であることを示せ.
(2) $\operatorname{Gal}(L/\mathbb{Q})$ の部分群を全て求めよ.
(3) (2) の各部分群について, その不変体を求めよ.

22.17. $\zeta=\exp(2\pi i/7)$ とし, $L=\mathbb{Q}(\zeta)$, $\alpha=\zeta+\zeta^{-1}$ とする. 次の問に答へよ. 但し, 解答する順序は必ずしも番号順でなくてよい.
(1) $\operatorname{irr}(\zeta,\mathbb{Q},x)=x^6+x^5+x^4+x^3+x^2+x+1$ であることを示せ. （Hint: 8.9 を見よ）
(2) $\sigma:\zeta\mapsto\zeta^3$ は L の $\mathbb{Q}$ 上の自己同型を与へることを示せ.
(3) (2) の σ について, α^σ を α の有理式で書け. それを $\varphi(\alpha)$ とするとき, $\alpha^{\sigma^2}=\varphi(\varphi(\alpha))$, $\alpha^{\sigma^3}=\alpha$ であることを示せ.
(4) (2) の σ は $\mathbb{Q}(\alpha)$ の $\mathbb{Q}$ 上の自己同型を与へることを示し, 拡大 $\mathbb{Q}(\alpha)/\mathbb{Q}$ が Galois 拡大であること, および $\operatorname{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ は位数 3 の巡回群であることを示せ.
(5) $\operatorname{irr}(\alpha,\mathbb{Q},x)=x^3+x^2-2x-1$ であることを示せ.
(6) $[L:\mathbb{Q}(\alpha)]$ および $[\mathbb{Q}(\alpha):\mathbb{Q}]$ はいくつか.

22.18. $\mathbb{Q}$ に係数を持つ既約多項式 $f(x)$ の $\mathbb{Q}$ 上の最小分解体を K とするとき, Galois 群 $\operatorname{Gal}(K/\mathbb{Q})$ は `paridroid` で簡単に求められる. 以下の入力を試してみよ. 返される結果の意味を調べて, 解読せよ. (Hint: 有限群は完全に分類されてゐる. いくつかの分類記号の流儀が存在し, それが返り値になつてゐる.)
(1) `> polgalois(x^4-4*x-1)`
(2) `> polgalois(x^4+x^3+x^2+x+1)`
(3) `> polgalois(x^5-2*x^4+x^3+x^2-x+1)`
(4) `> polgalois(x^5-2)`

22.19. 22.10 の状況で G が無限群であるときは, L/K が代数的拡大とならない例を挙げる. 不定元 t をとり, $L=\mathbb{Q}(t)$ とし, G を $t^\sigma=t+1$ で定められる同型 $\sigma: L\to L$ で生成される群とする. G は無限群である. このときの $(K=)\,L^G$ は何か.

§ 23. Galois の基本定理

拡大 L/K の中間体の全体を $\mathscr{F}(L/K)$ で表し, 群 G の部分群の全体を $\mathscr{G}(G)$ で表す[32]. このとき, 次の定理が我々が目標としてきたものである.

定理 23.1. (Galois の基本定理 1) L/K を有限次 Galois 拡大とし, $G=\mathrm{Gal}(L/K)$ とする. このとき, G の部分群にその不変体を対応させる写像

$$\varphi:\mathscr{G}(G)\longrightarrow\mathscr{F}(L/K),\qquad H\longmapsto L^H$$

は全単射で, 逆写像は $\varphi^{-1}(M)=G^M=\mathrm{Gal}(L/M)$ で与へられる. 従つて

$$H=\varphi^{-1}(\varphi(H))=G^{L^H}=\mathrm{Gal}(L/L^H),\quad M=\varphi(\varphi^{-1}(M))=L^{G^M}$$

が成り立つ. 特に $[L:L^H]=|H|$ である.

注意 23.2. (1) $\{1\}<H_1<H_2<G$ ならば $L^{H_1}\supset L^{H_2}$ であるから, 上の φ は包含関係を逆転させる全単射である.
(2) 全射性の証明には 22.7(2) を用ゐる. 単射性の証明には 22.10 (Artin の定理) が必要である.

証明 $M\in\mathscr{F}(L/K)$ に対し, 22.5 より, L/M は Galois 拡大で $\mathrm{Gal}(L/M)=G^M$ であるから, 22.7(2) により $M=L^{G^M}=\varphi(G^M)$. よつて φ は全射である.
次に 22.10 (Artin の定理) により, $H\in\mathscr{G}(G)$ に対し, L/L^H は Galois 拡大で, $\mathrm{Gal}(L/L^H)=H$, $[L:L^H]=|H|$ となる. 一方 22.6 により, L/K の中間体 M に対し $\mathrm{Gal}(L/M)=G^M$ である. よつて $H\in\mathscr{G}(G)$ に対して $\boxed{H=\mathrm{Gal}(L/L^H)=G^{L^H}}$ となる. 特に $H_1,H_2\in\mathscr{G}(G)$ で $L^{H_1}=L^{H_2}$ ならば, $H_1=G^{L^{H_1}}=G^{L^{H_2}}=H_2$ となつて φ は単射である. □

定理 23.3. (Galois の基本定理 2) 有限次 Galois 拡大 L/K と $M\in\mathscr{F}(L/K)$ について, 次の 3 つが成り立つ.
(1) $\tau\in\mathrm{Gal}(L/K)$ に対し, $\tau\,\mathrm{Gal}(L/M)\tau^{-1}=\mathrm{Gal}(L/M^\tau)$.
(2) M は K の Galois 拡大 $\iff$ $\mathrm{Gal}(L/M)\lhd\mathrm{Gal}(L/K)$.
(3) (2) の両側が成り立つとき, $\sigma\mapsto\sigma|_M$ によつて, 次の群の同型が得られる:

$$\mathrm{Gal}(L/K)/\mathrm{Gal}(L/M)\simeq\mathrm{Gal}(M/K).$$

証明 (1) 一般に $M\in\mathscr{F}(L/K)$, $\tau\in G=\mathrm{Gal}(L/K)$ に対して

$$\begin{aligned}G^{M^\tau}&=\{\sigma\in G\,|\,\alpha^\sigma=\alpha\ (\forall\alpha\in M^\tau)\}=\{\sigma\in G\,|\,(\beta^\tau)^\sigma=\beta^\tau\ (\forall\beta\in M)\}\\&=\{\sigma\in G\,|\,\beta^{\tau^{-1}\sigma\tau}=\beta\ (\forall\beta\in M)\}=\{\tau\rho\tau^{-1}\in G\,|\,\beta^\rho=\beta\ (\forall\beta\in M)\}=\tau G^M\tau^{-1}\end{aligned}$$

である. ($\tau\rho\tau^{-1}\in G\iff\rho\in\tau^{-1}G\tau=G$ に注意)
(2) ($\Rightarrow$) M/K は正規拡大ゆゑ, (18.10 から) すべての $\tau\in G$ に対して $M^\tau=M$ となる. よつて $\tau G^M\tau^{-1}=G^{M^\tau}=G^M$ となり, $G^M\lhd G$ である.
(2) ($\Leftarrow$) 任意の $\tau\in G$ に対して $G^M=\tau G^M\tau^{-1}=G^{M^\tau}$ であるから, 23.1 から $M^\tau=M$ である. それゆゑ, 18.10 により M/K は正規拡大である. 分離拡大であることは 19.8 による.
(3) $\sigma\in G$ の M への制限 $\sigma|_M$ は $\mathrm{Gal}(M/K)$ の元であるから, 写像 $\iota:G\to\mathrm{Gal}(M/K)$, $\sigma\mapsto\sigma|_M$ が定義される. ι は群の準同型であり, 16.7 より全射である. その核は $G^M=\mathrm{Gal}(L/M)$ に他ならない. よつて群論の 第 1 準同型定理 により $\mathrm{Gal}(L/K)/\mathrm{Gal}(M/K)=G/G^M\simeq\mathrm{Gal}(M/K)$ である. □

[32] $\mathscr{F}$ は F の, $\mathscr{G}$ は G の script 体.

問 23.4. 23.1 の記号と仮定の下で, M, $M' \in \mathscr{F}(L/K)$ とする. 次の (1), (2) を示せ.

(1) $G^{MM'} = G^M \cap G^{M'}$.

(2) $G^{M\cap M'} =$“G^M と $G^{M'}$ で生成される部分群”.

(Hint: $M \cap M' = \{\alpha \in L \,|\, \alpha^\sigma = \alpha \ (\forall \sigma \in$“右辺”$)\}$ を示し 23.1 を用ゐる.)

特に $G^M \lhd G$ または $G^{M'} \lhd G$ であれば, 右辺は $G^M G^{M'} (= G^{M'} G^M)$ である.

命題 23.5. 体 M, M' は有限次拡大 L/K の中間体であるとする. M'/K が Galois 拡大であれば MM'/M も Galois 拡大であり,

$$\mathrm{Gal}\,(MM'/M) \simeq \mathrm{Gal}\,(M'/M \cap M').$$

この時, 特に $[MM' : M] = [M' : M \cap M']$ である.

証明 22.2 より, MM'/M は Galois 拡大. 22.5 より $M'/M \cap M'$ も Galois 拡大なので, 各 $\sigma \in \mathrm{Gal}\,(MM'/M)$ の制限 $\sigma|_{M'}$ は $\mathrm{Gal}\,(M'/M \cap M')$ の元である. ゆゑに, 写像

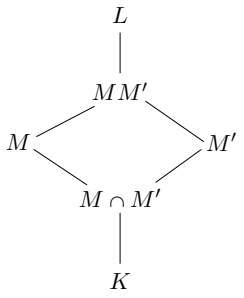
$$f : \mathrm{Gal}\,(MM'/M) \to \mathrm{Gal}\,(M'/M \cap M'), \quad \sigma \mapsto \sigma|_{M'}$$

が得られるが, これは群の準同型である. 各 $\sigma \in \mathrm{Gal}\,(MM'/M)$ は M' の元の像で決まるから, f は単射である. 次に $H = \mathrm{Im}\, f$ とおくと,

$$\begin{aligned} {M'}^H &= \{\alpha \in M' \,|\, \alpha^\sigma = \alpha \ (\forall \sigma \in H)\} \\ &= \{\alpha \in M' \,|\, \alpha^\sigma = \alpha \ (\forall \sigma \in \mathrm{Gal}\,(MM'/M))\} \end{aligned}$$

である. 一方, 22.6 と 22.7(2) の後半 (あるいは 23.1) より

$$M = \{\alpha \in MM' \,|\, \alpha^\sigma = \alpha \ (\forall \sigma \in \mathrm{Gal}\,(MM'/M))\}.$$



従つて ${M'}^H = M \cap M'$. 拡大 $M'/(M \cap M')$ について 23.1 を使へば, $H = \mathrm{Gal}\,(M'/M \cap M')$ であり, f は全射でもあることがわかる. □

定義 23.6. Galois 拡大 L/K は, $\mathrm{Gal}\,(L/K)$ が Abel 群であるとき, Abel 拡大であるといはれ, $\mathrm{Gal}\,(L/K)$ が巡回群であるとき, 巡回拡大であるといはれる.

命題 23.7. 体 M, M' は有限次拡大 L/K の中間体であるとする. M, M' がともに K の Abel 拡大ならば, MM'/K も Abel 拡大である.

証明 22.2 後半より MM'/K は Galois 拡大であり, 23.3(2) より $G = \mathrm{Gal}\,(MM'/K)$ について $G^{M'} \lhd G$, $G^M \lhd G$ である. また, 23.3(3) より $G/G^{M'} \simeq \mathrm{Gal}\,(M'/K)$, $G/G^M \simeq \mathrm{Gal}\,(M/K)$ で, これらは仮定から Abel 群である. ゆゑに, 交換子群について $[G,G] \subset G^M$ かつ $[G,G] \subset G^{M'}$ であり [33], $[G,G] \subset G^M \cap G^{M'} \overset{23.4(1)}{=\!=} G^{MM'} = \{1\}$ であり, G は Abel 群である. □

例 23.8. 体 K 上の分離的な n 次の多項式 $f(x)$ の $\overline{K}$ 内の根を $\alpha_1, \cdots, \alpha_n$ とする. このとき $f(x)$ の最小分解体 $L = K(\alpha_1, \cdots, \alpha_n)$ の K 上の Galois 群 $G = \mathrm{Gal}\,(L/K)$ を多項式 $f(x)$ の K 上の Galois 群と呼ぶ. $\sigma \in G$ について $f^\sigma(x) = f(x)$ であるから, σ は n 個の元からなる集合 $\{\alpha_1, \cdots, \alpha_n\}$ に置換 [34] $\sigma' = \begin{pmatrix} \alpha_1 & \cdots & \alpha_n \\ {\alpha_1}^\sigma & \cdots & {\alpha_n}^\sigma \end{pmatrix} \in S_n$ (S_n は n 次対称群 [35]) として作用 (§34.1 参照) するので, 単射 $\varphi : G \longrightarrow S_n$ が定まる. ゆゑに G は S_n の部分集合と同型で, 特に $[L : K] = |G| \leqq n!$ である.

[33] 一般に, 群 G と $H \lhd G$ について, G/H が Abel 群であるためには, 交換子群について $[G,G] \subset H$ であることが必要十分である. 即ち, 交換子群 $[G,G]$ は, G/H が Abel 群となる様な最大の $H \lhd G$ に一致する.

[34] 「代数学 1」, §1 を見よ. ここでは $\{1, \cdots, n\}$ の代りに $\{\alpha_1, \cdots, \alpha_n\}$ の置換を考へてゐる.

[35] 「代数学 1」, §1 を見よ.

例題 23.9. $f(x)\in K[x]$ は分離的であるとする. G を $f(x)$ の K 上の Galois 群とする. また, $\{\alpha_1,\cdots,\alpha_n\}$ を $f(x)$ の $\overline{K}$ における根の全体とする. このとき, 次を示せ :

$f(x)$ が既約多項式 $\iff$ G が $\{\alpha_1,\cdots,\alpha_n\}$ 上に 可移的 [36] に作用する.

証明 ($\Rightarrow$) 背理法で示す. α_1 をとり, α と記す. $\{\alpha_1,\cdots,\alpha_n\}$ における α の G 軌道を, 番号を付け替へて, $\alpha^G=\{\alpha_1,\cdots,\alpha_m\}$ とする. このとき $m\leqq n$ である. いま $g(x)=\prod_{j=1}^{m}(x-\alpha_j)$ とおくと, G は α^G にも作用するから, $g^\sigma(x)=g(x)$ である. つまり $g\in K[x]$. もし $m<n$ ならば, $f(x)$ の既約性に反する. ($\Leftarrow$) は 16.4(2)$\Rightarrow$(1) を使へばよい. 細部は演習問題 23.12 として残しておく. □

例題 23.10. $\mathbb{Q}$ 上の多項式 $f(x)=x^4+10x^2+23$ の最小分解体を L とする. 拡大 $L/\mathbb{Q}$ の Galois 群 $G=\mathrm{Gal}(L/\mathbb{Q})$ と G の部分群のすべて, および, $L/\mathbb{Q}$ の部分体のすべてを求め, それら包含関係と 23.1（Galois の定理 1）による対応を図示せよ.

解答 方程式 $f(x)=0$ は x^2 の多項式としての判別式が 2 なので $\mathbb{Q}$ 上既約である. 或いは, 係数を 3 を法としてみた $f(x)\bmod 3\,(\in\mathbb{F}_3[x])$ が既約なので, $f(x)$ 自身が既約である. 2 次方程式の解の公式から, $x^2=-5\pm\sqrt{2}<0$. ゆゑに $x=\pm i\sqrt{5\pm\sqrt{2}}$. そこで $\alpha=i\sqrt{5+\sqrt{2}}$, $\beta=i\sqrt{5-\sqrt{2}}$ とおけば,

$$L=\mathbb{Q}\big(\alpha,-\alpha,\beta,-\beta\big)=\mathbb{Q}\big(\alpha,\beta\big)$$

で, $\sqrt{2}\in L$ である. ここで Galois 群 G の元は, 23.8 によつて, $\{\alpha,-\alpha,\beta,-\beta\}$ の置換であるが, 23.9 により $\alpha\longmapsto\beta$ なる G の元 σ が存在する. $\sigma(\alpha^2)=\beta^2$ ゆゑ $\sigma(\sqrt{2})=-\sqrt{2}$ である. ゆゑに σ は β を $\pm\alpha$ のどちらかに写さざるを得ないが, $f(x)$ の既約性から $x^2+5\mp\sqrt{2}$ も $\mathbb{Q}(\sqrt{2})$ 上既約であるから, 16.3 によつて, そのどちらに写してもよい. また, $\alpha\longmapsto-\alpha$ なる元 τ も存在し, それは β を $\pm\beta$ のどちらかに写さざるを得ない. 16.3 により, そのどちらに写すものも存在する. そこで,

$$\sigma:\alpha\longmapsto\beta,\ \ \beta\longmapsto-\alpha\quad\text{および}\quad\tau:\alpha\longmapsto-\alpha,\ \beta\longmapsto\beta$$

とおき, これらの合成を調べてみると,

$$\begin{aligned}
\tau\sigma^2\tau=\sigma^2&:\alpha\longmapsto-\alpha,\ \ \beta\longmapsto-\beta,\\
\tau\sigma\tau=\sigma^3&:\alpha\longmapsto-\beta,\ \ \beta\longmapsto\alpha,\\
\sigma^3\tau=\tau\sigma&:\alpha\longmapsto\beta,\quad\beta\longmapsto\alpha,\\
\tau\sigma^3=\sigma\tau&:\alpha\longmapsto-\beta,\ \ \beta\longmapsto-\alpha,\\
\tau\sigma^2=\sigma^2\tau&:\alpha\longmapsto\alpha,\ \ \beta\longmapsto-\beta
\end{aligned}$$

で, $\sigma^4=\tau^2=(\sigma\tau)^2=(\tau\sigma)^2=1$ である. よつて

$$G=\{1,\ \sigma,\ \tau,\ \sigma^2,\ \sigma^3,\ \tau\sigma,\ \sigma\tau,\ \sigma^2\tau\}.$$

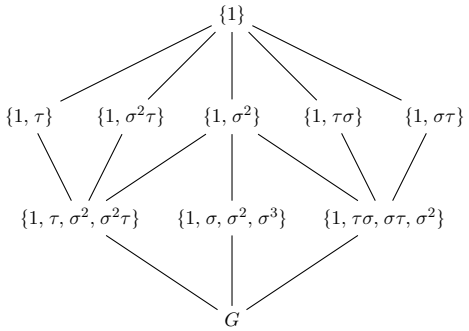
また, $\alpha\cdot(-\alpha)=-5+\sqrt{2}$, $\beta\cdot(-\beta)=-5-\sqrt{2}$ より

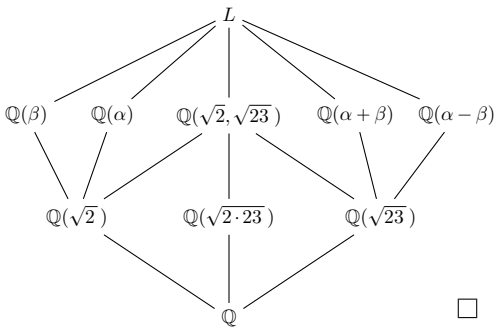
$$\tau(\sqrt{2}\,)=\sqrt{2},\quad\sigma(\sqrt{2}\,)=-\sqrt{2}.$$

$\alpha\beta=-\sqrt{23}$ より $\sqrt{23}\in L$ であつて

$$\sigma(\sqrt{23}\,)=\tau(\sqrt{23}\,)=-\sqrt{23}.$$

一方, G の部分群を調べれば, 右上の 10 個になることがわかる. それらに 23.1（Galois の定理 1）で対応する部分体は右の様になる.





□

[36] 推移的 ともいふ. 34.1 を見よ.

例 23.11. $\zeta=\exp(2\pi i/15)$, $L=\mathbb{Q}(\zeta)$ とおく. ζ は $x^{15}-1=0$ の根であり, 他の根は ζ の冪乗で表されるから, L は $x^{15}-1$ の最小分解体であり, 従つて, $L/\mathbb{Q}$ は Galois 拡大である. $G=\mathrm{Gal}(L/\mathrm{Q})$ とおく. 上のことから, 任意の $\sigma\in G$ について, $\sigma(\zeta)=\zeta^{i(\sigma)}$ となる $i(\sigma)\in\mathbb{Z}$ が存在するが, $\zeta^{15}=1$ なので, $i(\sigma)\in\mathbb{Z}/15\mathbb{Z}$ とみなせる. しかも, σ は集合 $S=\{1,\,\zeta,\cdots,\zeta^{14}\}$ を不変に保つ ($\sigma(S)=S$) から, $i(\sigma)\in(\mathbb{Z}/15\mathbb{Z})^\times$ でなくてはならない. また, それらすべてが実際に G の元を与へる. 「代数学 1」で学んだ通り, それは $\varphi(15)=8$ 個の元からなる. 23.9 により,

$$G=\{\,\zeta\mapsto\zeta^i\,|\,i\in(\mathbb{Z}/15\mathbb{Z})^\times\,\}$$

である. 従つて

$$\mathrm{irr}(\zeta,\mathbb{Q},x)=\prod_{\sigma\in G}(x-\zeta^{i(\sigma)}).$$

ちなみに, pari/GP で `factor(x^15-1)` として出力される因子の中に 8 次の因子は唯一つで

$$\mathrm{irr}(\zeta,\mathbb{Q},x)=x^8-x^7+x^5-x^4+x^3-x+1$$

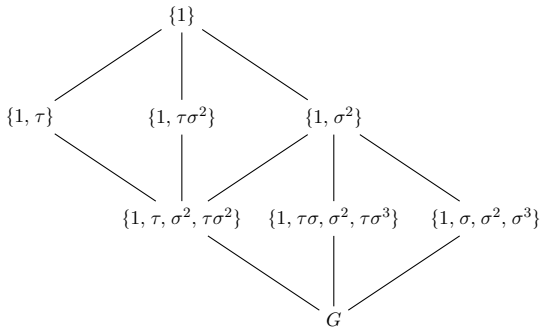
とわかる. さらに「代数学 1」の 9.9 と 9.10 から, $(\mathbb{Z}/15\mathbb{Z})^\times$ は 2 つの巡回群の直積として, $(\mathbb{Z}/3\mathbb{Z})^\times\times(\mathbb{Z}/5\mathbb{Z})^\times$ と同一視できて,

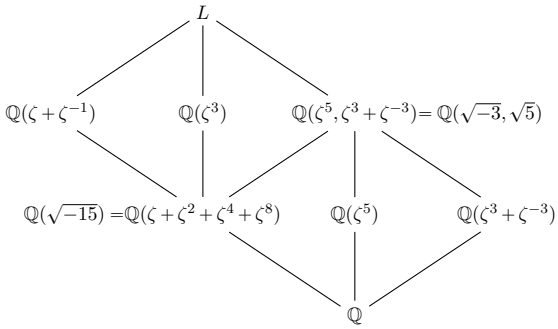
$$(\mathbb{Z}/15\mathbb{Z})^\times=\langle -1,\,2\rangle.$$

ここで $\sigma:\zeta\mapsto\zeta^2$, $\tau:\zeta\mapsto\zeta^{-1}$ と記すと, $\sigma\tau=\tau\sigma$ であり, これらの記法の対応は以下通り.

1	2	4	7	8	11	13	14
1	2	2^2	$(-1)\,2^3$	2^3	$(-1)\,2^2$	$(-1)\,2$	-1
1	σ	σ^2	$\tau\sigma^3$	σ^3	$\tau\sigma^2$	$\tau\sigma$	τ

「代数学 1」の 4.6 を使へば巡回群の部分群は求められるので, G の部分群は容易に求められる. G の部分群と 23.1（Galois の定理 1）で対応する体は, 下記の様になる. 生成元の不変性や拡大次数を確認されたい.





以上は, 一般な理論を使つて系統的な仕方で求めることもできる. それに関しては, 27.4 の証明, および 32.6 を読まれたい.

演 習 問 題

23.12. 23.9 の ($\Leftarrow$) の細部を含めて証明せよ.
(Hint: $f(x)=g(x)h(x)$, $g(x)$, $h(x)\in K[x]$, $\deg g(x)>0$, $\deg h(x)>0$ と分解されたとする. このとき, 仮定を使つて $g(x)$ の任意の根は $h(x)$ の根でもあることを示せ.)

23.13. 次の $\zeta\in\mathbb{C}$ について $\mathbb{Q}(\zeta)/\mathbb{Q}$ が Galois 拡大であることを示せ. さらに, $\mathrm{Gal}\,(\mathbb{Q}(\zeta)/\mathbb{Q})$ とそのすべての部分群を記述し, および, それらに対応する $\mathbb{Q}(\zeta)/\mathbb{Q}$ の中間体を求めよ.
(1) $\zeta=\exp\dfrac{2\pi i}{8}$ (2) $\zeta=\exp\dfrac{2\pi i}{5}$ (3) $\zeta=\exp\dfrac{2\pi i}{12}$

23.14. $\alpha=\sqrt{6+3\sqrt{2}+2\sqrt{3}+2\sqrt{6}}$ とおく. 11.8 の拡大 $\mathbb{Q}(\alpha)/\mathbb{Q}$ は Galois 拡大である. その理由を述べよ. そこでの記号で ${\sigma_1}^+=\sigma$, ${\sigma_2}^+=\tau$ とおき, $G=\mathrm{Gal}\,\big(\mathbb{Q}(\alpha)/\mathbb{Q}\big)$ を σ, τ で記述せよ. また, この拡大に関し, 23.1 の φ で, G の交換子群 $D(G)=[G,G]$ に対応する中間体を求めよ. さらに, G のすべての部分群, および, それぞれに対応する中間体を求めよ.

23.15. 有限次 Abel 拡大 L/K とその中間体 M について次のことを示せ.
(1) L/M と M/K も Abel 拡大である.
(2) M' も L/K の中間体とする. M/K が Abel 拡大のとき, MM'/M' も Abel 拡大である.

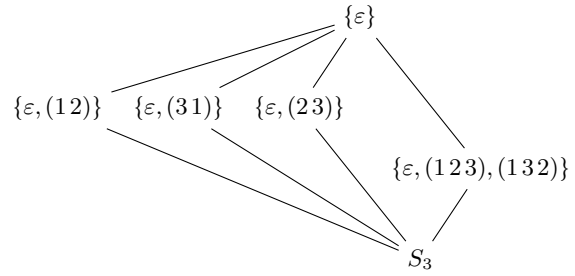
23.16. K を体とし, $a\in K$ について $b=1+a^2\in K$ が K の元の平方ではないとする. このとき $\mathrm{char}\,K\neq 2$ で $K(\sqrt{b+\sqrt{b}}\,)/K$ は 4 次の巡回拡大であることを示せ.
(Hint: $\beta=\sqrt{b+\sqrt{b}}$ とおく. $[K(\beta):K]=4$ が確かめられれば, $\beta^\sigma=-\sqrt{b-\sqrt{b}}$ なる $\mathrm{Gal}\,\big(K(\beta)/K\big)$ の元 σ が存在する. このとき β^{σ^2}, β^{σ^3} を調べよ.)

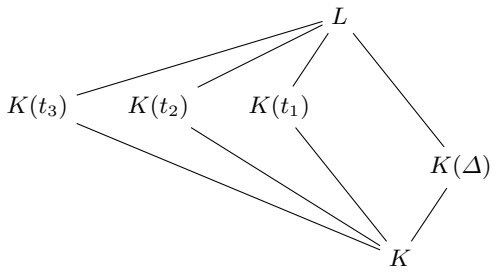
23.17. 多項式 $f(x)=x^3-6x+2$ について問に答へよ.
(1) $f(x)=0$ の解を $\omega=\frac{-1+\sqrt{3}i}{2}$ と平方根号 $\sqrt{\ }$, $\sqrt[3]{\ }$ および四則演算だけで表せ.
(Hint: 恒等式 $x^3+y^3+z^3-3xyz=(x+y+z)(x+\omega y+\omega^2 z)(x+\omega^2 y+\omega z)$ を利用する.)
(2) $f(x)$ の最小分解体を L とし, $K=\mathbb{Q}(\omega)$ とする. $\mathrm{Gal}\,(L/K)$ が $\{1,2,3\}$ に関する 3 次対称群 S_3 と次の対応で同型であることを示せ. 即ち, $f(x)=0$ の 3 つの解を t_1, t_2, t_3 とするとき, $\sigma\in S_3$ を ${t_i}^\sigma=t_{\sigma(i)}$ で $\mathrm{Gal}\,(L/K)$ の元と見做して, $S_3\simeq\mathrm{Gal}\,(L/K)$.
(Hint: $\Delta=(t_1-t_2)(t_2-t_3)(t_3-t_1)$ を求め, $K(\Delta)$ に対応する $\mathrm{Gal}\,(L/K)$ の部分群を考察せよ.)
(3) $H=\{\varepsilon,(12)\}<S_3$ に対応する体 M を求めよ. $\tau=(13)$ のとき

$$(\ \tau\,\mathrm{Gal}\,(L/M)\tau^{-1}=\ )\quad \tau H\tau^{-1}=\mathrm{Gal}\,(L/M^\tau)$$

であることを確かめよ.

参考のために, 以上の内容を図示しておく.





§ 24. 有限体

有限体についてまとめておく.

命題 24.1. p を任意の素数とし, n を任意の自然数とする. このとき $|F| = p^n$ なる有限体 F が存在する. この様な F は素体 $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ 上の, 多項式 $x^{p^n} - x$ の最小分解体に同型である. 従つて, その様な体 F は同型を度外視して一意的に存在する. また $[F : \mathbb{F}_p] = n$ である.

証明 $\overline{\mathbb{F}_p}$ を $\mathbb{F}_p$ の代数的閉包とし, $F = \{\, \alpha \in \overline{\mathbb{F}_p} \,|\, \alpha^{p^n} = \alpha \,\}$ とおけば, F が体になることは容易に確かめられる. F は多項式 $f(x) = x^{p^n} - x$ の根の全体で, $f'(x) = -1$ と $f(x)$ の共通根は存在しないから $f(x)$ は重根を持たず, $|F| = p^n$ となる. 一方 K を元の個数が p^n の任意の有限体とせよ. 12.5(2) により K は $x^{p^n} - x$ の $\mathbb{F}_p$ の最小分解体で $K \simeq F$ となる. 最後に, F は p 元体 $\mathbb{F}_p$ 上の次元 $[F : \mathbb{F}_p]$ の vector 空間であるから $|F| = p^{[F:\mathbb{F}_p]}$. ゆゑに $[F : \mathbb{F}_p] = n$ である. □

上の 24.1 で得られた体 F を $\mathbb{F}_{p^n}$ で表す. 特に $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ である. 以後, 素体 $\mathbb{F}_p$ の代数的閉包 $\overline{\mathbb{F}_p}$ を 1 つ決めて固定し, あらゆる $\mathbb{F}_{p^n}$ $(n \in \mathbb{N})$ は $\overline{\mathbb{F}_p}$ の部分体であるものとする :

$$\mathbb{F}_{p^n} = \{\, \alpha \in \overline{\mathbb{F}_p} \,|\, \alpha^{p^n} = \alpha \,\}, \quad [\mathbb{F}_{p^n} : \mathbb{F}_p] = n.$$

例題 24.2. 次を示せ. $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m} \iff n|m$.

証明 $(\Rightarrow)$ $[\mathbb{F}_{p^m} : \mathbb{F}_{p^n}] = d$ とすれば, $|\mathbb{F}_{p^m}| = |\mathbb{F}_{p^n}|^d = p^{nd}$ であるから $m = nd$ となる.
$(\Leftarrow)$ $m = nd$ $(d \in \mathbb{N})$ とし, $q = p^n$ とおけば $p^m = q^d$ である. $\alpha \in \mathbb{F}_q$ とすれば $\alpha^q = \alpha$. よつて $\alpha^{q^d} = \alpha$ となり $\alpha \in \mathbb{F}_{q^d}$ を得る. □

有限体についての基本的性質は次の定理の様にまとめられる.

定理 24.3. $q = p^n$ (p は素数, $n \in \mathbb{N}$) とせよ. 次が成り立つ.
(1) $\mathbb{F}_q$ の乗法群 $\mathbb{F}_q{}^\times = \mathbb{F}_q - \{0\}$ は位数 $q-1$ の巡回群である.
(2) $\mathbb{F}_q$ は完全体である.
(3) $\mathbb{F}_{q^d}/\mathbb{F}_q$ は Galois 拡大であり, $\mathrm{Gal}\,(\mathbb{F}_{q^d}/\mathbb{F}_q)$ は巡回群で

$$\sigma : \mathbb{F}_{q^d} \longrightarrow \mathbb{F}_{q^d}, \quad \alpha \longmapsto \alpha^q$$

とおくと $\mathrm{Gal}\,(\mathbb{F}_{q^d}/\mathbb{F}_q) = \langle \sigma \rangle$.

証明 (1) は「代数学 1」の 13.5(2) で示した. (2) は 14.2 で示した.
(3) まづ (2) より, この拡大は分離的である. また $\mathbb{F}_{q^d}$ は $x^{q^d} - x \in \mathbb{F}_p[x]$ の最小分解体であるから $\mathbb{F}_{q^d}/\mathbb{F}_p$ は正規拡大であり, よつて $\mathbb{F}_{q^d}/\mathbb{F}_q$ も正規拡大である. 以上より, $\mathbb{F}_{q^d}/\mathbb{F}_q$ は Galois 拡大である. $\alpha \in \mathbb{F}_{q^d}$ に対し $\sigma(\alpha) = \alpha$, つまり $\alpha^q = \alpha$ ならば α は $x^q - x$ の根なので 24.1 の後半により, $\alpha \in \mathbb{F}_q$ である. 逆に $\alpha \in \mathbb{F}_q$ ならば (1) により $\alpha^q = \alpha$ である. 即ち $\mathbb{F}_{q^d}$ に対する巡回群 $\langle \sigma \rangle$ の不変体が $\mathbb{F}_q$ である. $L = \mathbb{F}_{q^d}$ と $G = \langle \sigma \rangle$ について, 22.10(2) を使へば結論を得る. □

上の 24.3 (1) で $\mathbb{F}_q{}^\times = \langle \gamma \rangle$ と書いたとき, γ を有限体 $\mathbb{F}_q$ の 原始根 と呼ぶ. 24.3 で $n = 1$ の場合は, 「代数学 1」で学んだ原始根の概念に一致する. また, $\mathbb{F}_q$ は $\mathbb{F}_p$ に γ を添加して得られる : $\mathbb{F}_q = \mathbb{F}_p(\gamma)$.

演 習 問 題

24.4. p を素数, $n = 2^2 \cdot 3^3 \cdot 5$ とする. $G = \mathrm{Gal}\,(\mathbb{F}_{p^n}/\mathbb{F}_p)$ を求め, その構造を記せ. G の部分群とそれらに対応する拡大 $\mathbb{F}_{p^n}/\mathbb{F}_p$ の中間体を求めよ.

24.5. p を素数とせよ. K を $\mathbb{F}_p$ の m 次拡大体, L を K の n 次拡大体とせよ.
(1) 乗法群 $L^\times$ の生成元を g とする. $K^\times$ の生成元の 1 つを g で表せ.
(2) L の $\mathbb{F}_p$ 上の自己同型 σ は $\sigma(g) = g^\nu$ となる $\nu \in \mathbb{Z}$ によつて定まる. L の $\mathbb{F}_p$ 上の互ひに異るすべての自己同型を ν の値を示して記述せよ. そのうち, L の K 上の自己同型であるものを ν の値を示して記述せよ.

24.6. p を素数とする. $f(x) \in \mathbb{F}_p[x]$ は $\mathbb{F}_p$ 上既約で $\deg f(x) = m$ とせよ. このとき $n \in \mathbb{N}$ について, $f(x) \,|\, (x^{p^n} - x)$ であるためには $m \,|\, n$ であることが必要十分である. これを示せ.
（このことと $x^{q^m} - x$ の分離性から, $x^{q^m} - x$ は $\mathbb{F}_q[x]$ 内の次数が m の約数である様なあらゆる monic 既約多項式を渡る積に一致する. ）

24.7. q が素数 p の冪で $\mathbb{F}_q = \mathbb{F}_p(\gamma)$ のとき γ は必ず ${\mathbb{F}_q}^\times$ の原始根であるか.[37)]
(Hint : 原始根の個数と拡大体の生成元となる元の個数を比較せよ.)

[37)] $\mathbb{F}_p$ 上の既約多項式 $f(x)$ の根が $f(x)$ の最小分解体の原始根であるとき $f(x)$ は 原始根多項式 と呼ばれる.

§25. Hilbert の定理 90

この節では, 次節の 26.1 の証明に必要な Hilbert の定理 90 と呼ばれる事実について解説する.

定義 25.1. L/K は n 次の分離的拡大とし, L を含む K の代数的閉包を $\overline{K}$ とする. いま L から $\overline{K}$ の中への K 上の同型の全体を $\sigma_i : L \to \overline{K}$ $(i = 1, \cdots, n)$ とするとき, $\alpha \in L$ に対して

$$\mathrm{N}_{L/K}(\alpha) = \prod_{i=1}^{n} \alpha^{\sigma_i}, \quad \mathrm{Tr}_{L/K}(\alpha) = \sum_{i=1}^{n} \alpha^{\sigma_i},$$

と定義し, それぞれ拡大 L/K の norm, trace と呼ぶ.

問 25.2. $\gamma \in \overline{K}$ が K 上分離的で, 任意の $\sigma \in \mathrm{Aut}\overline{K}/K$ に対して $\gamma^\sigma = \gamma$ となれば $\gamma \in K$ であることを示せ. (これを 25.3 (1) の証明で用ゐる.)

例題 25.3. L/K は n 次の分離的拡大とする.

(1) $\mathrm{N}_{L/K} : L^\times \to K^\times$ $(\alpha \mapsto \mathrm{N}_{L/K}(\alpha))$ は乗法群の準同型で,
$\mathrm{Tr}_{L/K} : L \to K$ $(\alpha \mapsto \mathrm{Tr}_{L/K}(\alpha))$ は K 加群としての準同型 (即ち, 任意の $\alpha, \beta \in L$ と任意の $a \in K$ について $\mathrm{Tr}_{L/K}(\alpha+\beta) = \mathrm{Tr}_{L/K}(\alpha) + \mathrm{Tr}_{L/K}(\beta)$, $\mathrm{Tr}_{L/K}(a\alpha) = a\,\mathrm{Tr}_{L/K}(\alpha)$ を満たす) である.

(2) M を L/K の中間体とすれば,

$$\mathrm{N}_{L/K} = \mathrm{N}_{M/K}\mathrm{N}_{L/M}, \quad \mathrm{Tr}_{L/K} = \mathrm{Tr}_{M/K}\mathrm{Tr}_{L/M}.$$

(3) $\alpha \in L$, $\mathrm{irr}\,(\alpha, K, x) = x^m + a_1 x^{m-1} + \cdots + a_m$ とすれば, 拡大 $K(\alpha)/K$ について

$$\mathrm{N}_{K(\alpha)/K}(\alpha) = (-1)^m a_m, \quad \mathrm{Tr}_{K(\alpha)/K}(\alpha) = -a_1.$$

証明 25.1 と同じく K 上の中への同型の全体を $\sigma_i : L \to \overline{K}$ $(i = 1, \cdots, n)$ と書く.
(1) 任意の $\sigma \in \mathrm{Aut}\overline{K}/K$ に対して $\{\sigma\sigma_1, \cdots, \sigma\sigma_n\} = \{\sigma_1, \cdots, \sigma_n\}$ となる. 従つて $\alpha \in L$ に対して $\mathrm{N}_{L/K}(\alpha)$, $\mathrm{Tr}_{L/K}(\alpha)$ はともに σ で不変であり, K 上分離的である. 従つて 25.2 から, これらは共に K の元である. また $\mathrm{N}_{L/K}$, $\mathrm{Tr}_{L/K}$ がそれぞれ乗法, 加法を保つことは明らかである. さらに定義から $a \in K$ について $\mathrm{Tr}_{L/K}(a\alpha) = a\mathrm{Tr}_{L/K}$ となるから Tr は K 加群の間の準同型である.
(2) $[L : M] = r$, $[M : K] = s$ とし, $\rho_j : L \to \overline{K}$ $(j = 1, \cdots, r)$ を中への M 上の同型, $\tau_k : M \to \overline{K}$ $(k = 1, \cdots, s)$ を $\overline{K}$ の中への K 上の同型とせよ. 各 τ_j は K 上の同型 $\overline{\tau_j} : \overline{K} \xrightarrow{\sim} \overline{K}$ に拡張できるが, このとき $\overline{\tau_k}\rho_j : L \to \overline{K}$ は K 上の異なる同型で, $\{\sigma_i\} = \{\overline{\tau_k}\rho_j\}$ となる. よつて $\alpha \in L$ に対して, $\mathrm{N}_{L/K}(\alpha) = \prod_k (\prod_j \alpha^{\rho_j})^{\overline{\tau_k}} = \mathrm{N}_{M/K}(\mathrm{N}_{L/M}(\alpha))$ となる. Trace についても同様である.
(3) $\mathrm{irr}\,(\alpha, K, x) = (x - \alpha_1)\cdots(x - \alpha_m)$ とすると, m 個の K 上の同型 $\rho_i : K(\alpha) \to \overline{K}$ $(\alpha \mapsto \alpha_i)$ があり,

$$\mathrm{N}_{K(\alpha)/K}(\alpha) = \prod_{i=1}^{m} \alpha_i = (-1)^m a_m, \quad \mathrm{Tr}_{K(\alpha)/K}(\alpha) = \sum_{i=1}^{m} \alpha_i = -a_1$$

となる. □

補題 25.4. （Artin の定理） $\sigma_i : L \to \Omega$ $(i = 1, \cdots, n)$ は体 L から体 Ω の中への異る同型写像とする. このとき $\alpha_1, \cdots, \alpha_n \in \Omega$ に対し

$$\alpha_1 \theta^{\sigma_1} + \cdots + \alpha_n \theta^{\sigma_n} = 0 \ (\forall \theta \in L) \implies \alpha_1 = \cdots = \alpha_n = 0.$$

この性質を, $\{\sigma_i\}$ は L 上 1 次独立である, と称する.

証明 ある $(\alpha_1, \cdots, \alpha_n) \neq (0, \cdots, 0)$ に対して, 上の左側の関係式が成り立つとして, その様な関係式の内で $\alpha_i \neq 0$ なる i の個数が最小なものを更めて（必要ならば番号を付け変へて）

$$\alpha_1 \theta^{\sigma_1} + \alpha_2 \theta^{\sigma_2} + \cdots + \alpha_r \theta^{\sigma_r} = 0 \ (\forall \theta \in L), \quad \alpha_i \neq 0 \ \ (1 \leqq i \leqq r) \tag{25.5}$$

とする. もちろん $r \geqq 2$ で, 仮定により $\sigma_1 \neq \sigma_2$ ゆゑ, $\gamma^{\sigma_1} \neq \gamma^{\sigma_2}$ となる $\gamma \in L$ がある. (25.5) から

$$\alpha_1 \gamma^{\sigma_1} \theta^{\sigma_1} + \alpha_2 \gamma^{\sigma_2} \theta^{\sigma_2} + \cdots + \alpha_r \gamma^{\sigma_r} \theta^{\sigma_r} = 0 \ (\forall \theta \in L) \tag{25.6}$$

を得る. (25.5) を γ^{σ_1} 倍して (25.6) を差し引けば

$$\alpha_2 (\gamma^{\sigma_1} - \gamma^{\sigma_2}) \theta^{\sigma_2} + \cdots + \alpha_r (\gamma^{\sigma_1} - \gamma^{\sigma_r}) \theta^{\sigma_r} = 0 \ (\forall \theta \in L)$$

となるが, $\alpha_2(\gamma^{\sigma_1} - \gamma^{\sigma_2}) \neq 0$ であるから, これは (25.5) の項数 r の最小性に反する. □

問 25.7. L/K を有限次分離的拡大とすれば, $\mathrm{Tr}_{L/K}(\theta) \neq 0$ となる $\theta \in L$ がある. 従つて $\mathrm{Tr}_{L/K}(L) = K$ となることを示せ. （25.13 も参照されたい.）

さて, 次がこの節で目標とした定理である.

定理 25.8. （Hilbert の定理 90） L/K は巡回拡大で $\mathrm{Gal}(L/K) = \langle \sigma \rangle$ とせよ.
(1) $\mathrm{N}_{L/K}(\alpha) = 1 \iff \alpha = \beta^{1-\sigma} (= \beta(\beta^{\sigma})^{-1})$ となる $\beta \in L$ が存在する.
(2) $\mathrm{Tr}_{L/K}(\alpha) = 0 \iff \alpha = \beta - \beta^{\sigma}$ となる $\beta \in L$ が存在する.

注意 25.9. “定理 90” といふ名称は, Hilbert が前世紀までの数論の成果を集大成して著した論文 Zahlbericht (1897) における定理の番号に由来する.

証明 $[L : K] = n$ とする.
(1) ($\Leftarrow$). $\mathrm{N}_{L/K}(\alpha) = \alpha^{1+\sigma+\cdots+\sigma^{n-1}} = \beta^{(1-\sigma)(1+\sigma+\cdots+\sigma^{n-1})} = \beta^{1-\sigma^n} = 1$ となり正しい.
($\Rightarrow$). 25.4 を $1 (= \mathrm{id}_L), \sigma, \cdots, \sigma^{n-1}$ に適用して, ある $\theta \in L$ について

$$\theta + \alpha\theta^{\sigma} + \alpha^{1+\sigma}\theta^{\sigma^2} + \cdots + \alpha^{1+\sigma+\cdots+\sigma^{n-2}}\theta^{\sigma^{n-1}} \neq 0 \tag{25.10}$$

となる. 上の左辺を β とおけば, $\mathrm{N}_{L/K}(\alpha) = 1$ ゆゑ $\alpha\beta^{\sigma} = \beta$, 従つて $\alpha = \beta^{1-\sigma}$ を得る.
(2) 一般に $\mathrm{Tr}_{L/K}(\theta) = \theta + \theta^{\sigma} + \cdots + \theta^{\sigma^{n-1}}$ である.
($\Leftarrow$). $\mathrm{Tr}_{L/K}(\beta - \beta^{\sigma}) = (\beta + \beta^{\sigma} + \cdots + \beta^{\sigma^{n-1}}) - (\beta^{\sigma} + \beta^{\sigma^2} + \cdots + \beta^{\sigma^n}) = 0.$
($\Rightarrow$). 25.7 により $\mathrm{Tr}_{L/K}(\theta) \neq 0$ となる $\theta \in L$ がある. これを使ひ,

$$\beta = \{\alpha\theta^{\sigma} + (\alpha + \alpha^{\sigma})\theta^{\sigma^2} + \cdots + (\alpha + \alpha^{\sigma} + \cdots + \alpha^{\sigma^{n-2}})\theta^{\sigma^{n-1}}\} \mathrm{Tr}_{L/K}(\theta)^{-1}$$

とおく. このとき $\theta^{\sigma^n} = \theta$ であることと仮定 $0 = \mathrm{Tr}_{L/K}(\alpha) = \alpha + \alpha^{\sigma} + \cdots + \alpha^{\sigma^{n-1}}$ より

$$\begin{aligned} \alpha + \beta^{\sigma} &= \{\alpha \mathrm{Tr}_{L/K}(\theta) + \alpha^{\sigma}\theta^{\sigma^2} + \cdots + (\alpha^{\sigma} + \alpha^{\sigma^2} + \cdots + \alpha^{\sigma^{n-1}})\theta^{\sigma^n}\} \mathrm{Tr}_{L/K}(\theta)^{-1} \\ &= \{\alpha(\theta + \theta^{\sigma} + \cdots + \theta^{\sigma^{n-1}}) + \alpha^{\sigma}\theta^{\sigma^2} + \cdots + ((\alpha^{\sigma} + \alpha^{\sigma^2} + \cdots + \alpha^{\sigma^{n-2}})\theta^{\sigma^{n-1}}) \\ &\qquad + (\alpha^{\sigma} + \alpha^{\sigma^2} + \cdots + \alpha^{\sigma^{n-2}} + \alpha^{\sigma^{n-1}})\theta\} \mathrm{Tr}_{L/K}(\theta)^{-1} = \beta \end{aligned}$$

となる. 最後の等号では, 仮定 $\mathrm{Tr}_{L/K}(\alpha) = 0$ を使つた. □

注意 25.11. α と θ に関する (25.10) の左辺の式を Lagrange の分解式と呼ぶ.

演 習 問 題

25.12. p を素数, $x^p - x - 1 = 0$ の根の 1 つ $\alpha \in \overline{\mathbb{F}_p}$ をとり, $K = \mathbb{F}_p(\alpha)$ とおく [38].

(1) このとき拡大 $K/\mathbb{F}_p$ は $\sigma : \beta \mapsto \beta + 1$ で定まる自己同型が生成する p 次巡回拡大となることを示し, $\mathrm{irr}\,(\alpha, \mathbb{F}_p, x) = x^p - x - 1$ および $\mathrm{N}_{K/\mathbb{F}_p}(\alpha) = 1$ を示せ.

(2) $p = 2, 5, 7$ のときに, (1) の σ について $\alpha = y^{1-\sigma}$ となる $y \in K$ を求めよ.

25.13. 一般の有限次拡大 L/K については, 体の中への相異なる同型 $K \longrightarrow \overline{K}$ の全体を $\sigma_1, \cdots, \sigma_r$ とするとき, $\alpha \in L$ に対して

$$\mathrm{Tr}_{L/K}(\alpha) = [L : K]_i \sum_{j=1}^{r} \alpha^{\sigma_j}$$

と定める. このとき, L/K は分離的 $\iff \exists \alpha \in L,\ \mathrm{Tr}_{L/K}(\alpha) \neq 0,$ である. これを証明せよ.
（これは 25.7 の逆を含む. ）

25.14. L/K を有限体の有限次拡大とせよ. $\mathrm{Tr}_{L/K}$ は全射であることを 25.8(2)（Hilbert の定理 90） を使つて証明せよ.
（Hint : $K = \mathbb{F}_q$ とせよ. $\mathrm{Tr}_{L/K}$ は加法に関して準同型であることに注意すれば, 25.8(2) より, $\#\mathrm{Ker}(\mathrm{Tr}_{L/K}) = |L|/q$ がわかる. これより $\#\mathrm{Im}(\mathrm{Tr}_{L/K}) = q$ がわかる. ）

[38] 22.15 と一部重複.

§ 26. Kummer 拡大

25.8 を用ゐて次の定理が得られる.

定理 26.1. (単純 Kummer 拡大) 体 K は 1 の原始 n 乗根 ζ を含むとせよ. 従つて, 特に $\gcd(\mathrm{char}\,K, n) = 1$ である. このとき次が成り立つ.

(1) L/K が n 次の巡回拡大ならば, $\beta \in K$ が存在して $L = K(\beta)$ かつ $\mathrm{irr}\,(\beta, K, x) = x^n - a$ $(a \in K)$ となる.

(2) 逆に $a \in K$ に対して, 多項式 $x^n - a$ の 1 つの根 $\sqrt[n]{a}$ をとつて $L = K(\sqrt[n]{a})$ とおけば, L/K は d 次の巡回拡大である. ここで d は $d|n$, $(\sqrt[n]{a})^d \in K$ を満たすある自然数.

証明 (1) $G = \mathrm{Gal}\,(L/K) = \langle\sigma\rangle$ とする. $\mathrm{N}_{L/K}(\zeta^{-1}) = \zeta^{-n} = 1$ であるから, 25.8(1) より $\zeta^{-1} = \beta^{1-\sigma}$, 即ち $\beta^\sigma = \beta\zeta$ となる $\beta \in L$ が存在する. このとき, 仮定により 1 の n 乗根 $1, \zeta, \cdots, \zeta^{n-1}$ はすべて異なるから, $\beta,\ \beta^\sigma = \beta\zeta,\ \beta^{\sigma^2} = \beta\zeta^2,\ \cdots,\ \beta^{\sigma^{n-1}} = \beta\zeta^{n-1}$ はすべて異なり, 従つて $n \leqq [K(\beta) : K]_s \leqq [K(\beta) : K]$ となる. 一方 $L \supset K(\beta)$, $[L : K] = n$ であるから $L = K(\beta)$ となる. また $(\beta^n)^\sigma = \beta^n\zeta^n = \beta^n$ であるから, $\beta^n \in L^G = K$. $a = \beta^n$ と書けば $\beta = \sqrt[n]{a}$ $(a \in K)$ である. また, 12.10(2) から $\mathrm{irr}\,(\sqrt[n]{a}, K, x) = x^n - a$ も示された.

(2) $\gamma = \sqrt[n]{a}$ とおく. このとき $\gamma, \gamma\zeta, \cdots, \gamma\zeta^{n-1}$ はすべて, 互ひに異なり, かつ $x^n - a$ の根であるから $x^n - a = \prod_{i=0}^{n-1}(x - \gamma\zeta^i)$ となり, これは分離的である. $\mathrm{irr}\,(\gamma, K, x) | x^n - a$ であるから γ は K 上分離的で, γ の K 上の共役はすべて $\gamma\zeta^i$ の形の元であるから, それらは $L = K(\gamma)$ に含まれる. 従つて L/K は Galois 拡大である. その Galois 群を $G = \mathrm{Gal}\,(L/K)$ とする. $\sigma \in G$ について $\gamma^\sigma = \gamma\zeta^{i(\sigma)}$ $(i(\sigma) \in \{0, 1, \cdots, n-1\})$ の形に書ける. σ は γ の像 γ^σ によつて定まるから写像 $G \to \langle\zeta\rangle$ $(\sigma \mapsto \zeta^{i(\sigma)})$ は単射準同型である. よつて G は位数 n の巡回群 $\langle\zeta\rangle$ の部分群と同型であり, それ自身も巡回群である. ゆゑに $|G| = d$ とすれば $d|n$ である. ここで更めて G の生成元を σ と書いて $G = \langle\sigma\rangle$ とすれば, $(\zeta^{i(\sigma)})^d = 1$ であるから, $(\gamma^d)^\sigma = (\gamma^\sigma)^d = \gamma^d(\zeta^{i(\sigma)})^d = \gamma^d$. よつて $\gamma^d \in L^G = K$ である. □

注意 26.2. 体 K は 1 の原始 n 乗根を含むとする. K 上のいくつかの多項式 $f_j(x) = x^n - a_j$ $(1 \leqq j \leqq r)$ を考へる [39]. これらの根を K に添加してできる拡大 $K(\sqrt[n]{a_1}, \cdots, \sqrt[n]{a_r})/K$ を Kummer 拡大と呼ぶ. 26.1 で述べた拡大は $r = 1$ の場合なので, ここでは 単純 Kummer 拡大と呼ぶこととした.

[39] これらは K 上分離的である.

§ 27. 円分体

体 K の代数的閉包 $\overline{K}$ を 1 つ決めて固定する. $\overline{K}$ 内の 1 の n 乗根の全体を U_n で表す. U_n は多項式 x^n-1 の根の全体であり, 一般に位数 n 以下の巡回群である (「代数学 1」, 系 13.6).

命題 27.1. 1 の n 乗根の個数について次のことが成り立つ.
(1) $\operatorname{char} K = 0$ のとき $|U_n| = n$.
(2) $\operatorname{char} K = p > 0$ のとき, $n = p^r m$, $\gcd(p,m) = 1$ とすれば, $U_n = U_m$ で $|U_n| = m$.
(3) 1 の n 乗根は K 上分離的である.

証明 $f(x) = x^n - 1$ とすれば $f'(x) = nx^{n-1}$. 従つて $\operatorname{char} K = p$, $n|p$ なる場合を除けば, $f(x)$ は重根を持たず, $|U_n| = n$ となる. また, (2) の場合は $x^n - 1 = (x^m-1)^{p^r}$ となり, $x^m - 1$ は重根を持たないから $U_n = U_m$, $|U_n| = m$ である. さらに 1 の n 乗根はどれも, 分離的多項式 $x^m - 1$ の根であるから K 上分離的である. □

定義 27.2. 体 K に対し, 位数 n の元 $\zeta \in K^\times$ を 1 の <u>原始</u> n <u>乗根</u> と呼ぶ.

このとき $U_n = \langle \zeta \rangle$ で $\gcd(i,n) = 1$ ならば ζ^i もまた 1 の原始 n 乗根である. $L = K(U_n)$ は多項式 $x^n - 1$ の最小分解体であり, K の正規拡大である. このとき ζ は K 上分離的であるから, L/K は分離的である. 従つて L/K は Galois 拡大である.

定義 27.3. 体 M がある $K(U_n)/K$ の中間体であるとき, M を K 上の <u>円分体</u> といふ.

命題 27.4. 体 K 上の円分体は K の Abel 拡大である.

証明 Abel 群の部分群はすべて正規であり, それにより剰余類群も Abel 群なので, Galois の基本定理 23.3 により, $L = K(U_n)$ が K 上の Abel 拡大であることを示せばよい. 27.1 を踏まへれば $|U_n| = n$ としてよい. $U_n = \langle \zeta \rangle$, $G = \operatorname{Gal}(L/K)$ とおく. $\sigma \in G$ について $\zeta^\sigma = \zeta^{i(\sigma)}$ なる $i(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^\times$ が定まるが, これにより G は $(\mathbb{Z}/n\mathbb{Z})^\times$ の部分群と同型であることがわかる. ゆゑに G は Abel 群である. 次に M を L/K の中間体とし, $H = G^M$ (M による不変群) とする. このとき G が Abel 群ゆゑ, $H \lhd G$ であるから M/K は 23.3 (2) より Galois 拡大で, 23.3 (3) より $\operatorname{Gal}(M/K) \simeq G/H$ である. G が Abel 群だから, これは Abel 群である. □

注意 27.5. 後に, 32.6 において, $\operatorname{Gal}(\mathbb{Q}(U_n)/\mathbb{Q})$ と $(\mathbb{Z}/n\mathbb{Z})^\times$ が同型であることが示される.
体 $\mathbb{Q}(U_n)$ は (円の) <u>n 分体</u> と呼ばれる.

§ 28. 代数的に解ける方程式

この節では, 特に断らない限り, 体はすべて標数 0 であるとする. 従つて常に $\mathbb{Q}$ を含む. また 26.1 と同様に $\sqrt[n]{a}$ は $x^n - a$ の根の 1 つを表すものとする.

定義 28.1. 有限次拡大 E/K に対して, その中間体の列

$$K = E_0 \subset E_1 \subset \cdots \subset E_r = E \tag{28.2}$$

があつて, $0 \leqq i \leqq r-1$ なる各 i に対して $\operatorname{irr}(\sqrt[n_i]{a_i}, E_i, x) = x^{n_i} - a_i$ であつて

$$E_{i+1} = E_i(\sqrt[n_i]{a_i}) \quad (a_i \in E_i)$$

となつてゐるとき, E/K は冪根による拡大であるといふ. また, この様な拡大体の元は K 上で根号表示できる といふ.

注意 28.3. 冪乗根号の定義によれば $\frac{-1+\sqrt{-3}}{2} = \sqrt[3]{1}$ と書けるが, 左辺の方がより根源的な記述である. 一般の原始 n 乗根が $\sqrt[n]{1}$ 以外のより根源的な記述を持つか否かは自明ではない. この定義中の条件 $\operatorname{irr}(\sqrt[n_i]{a_i}, K, x) = x^{n_i} - a_i$ は, その様なより根源的な記述を前提とするために入れてある. 我々は, この既約性に拘(こだは)るがゆゑに, 最終的な到達点 28.15 までの議論がかなり複雑になる. 文献 [N] では, この条件を入れない議論しかされてゐない.

定義 28.4. 体 $\mathbb{Q}(a_0, a_1, \cdots, a_n)$ 上の多項式 $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ に対して, その根がすべて $\mathbb{Q}(a_0, a_1, \cdots, a_n)$ 上で根号表示できるとき, 方程式 $f(x) = 0$ は代数的に解ける といはれる.

このことは, 方程式 $f(x) = 0$ の解がすべて $f(x)$ の係数 a_0, a_1, $\cdots$, a_n に四則演算 $(+, -, \times, \div)$ と冪根をとるといふ操作 $\sqrt[n]{\ }$ を有限回行つて得られることを意味してゐる. さらにこのことはまた, $f(x)$ の $K' = \mathbb{Q}(a_0, a_1, \cdots, a_n)$ 上の最小分解体が, K' のある冪根による拡大体に含まれることに他ならない.

問 28.5. 次のことを示せ.

(1) 体の列 $K \subset M \subset L$ において, M/K, L/M がともに冪根による拡大ならば L/K も冪根による拡大である.

(2) L/K を冪根による拡大とし, $\overline{K}$ を L を含む K の代数的閉包とする. K 上の中への同型 $\sigma : L \to \overline{K}$ に対し, L^σ/K も冪根による拡大である.

(3) 拡大 L/K で, L は K 上の冪根拡大体 E に含まれるが (つまり L の元はすべて K 上で根号表示できるにも拘らず), L/K 自体は冪根による拡大ではない様な例を挙げよ.
(Hint : 第 30 節の最後を参照.)

(4) L, M が拡大 $\overline{K}/K$ の中間体で, L/K が冪根による拡大であるにも拘らず ML/M が冪根による拡大にならない例を挙げよ. また, L/K と M/K が共に冪根による拡大であるにも拘らず, LM/K が冪根による拡大にはならない例を挙げよ.

注意 28.6. $n \in \mathbb{N}$ に対し, $\mathbb{Q}$ の代数的閉包 $\overline{\mathbb{Q}}$ 内の 1 の n 乗根の全体を U_n で表す. $\mathbb{Q}(U_n)/\mathbb{Q}$ は常にある冪根による拡大に含まれるが, それ自体が冪根による拡大になるとは限らない ($n = 7$ の場合が反例. 28.19 参照. 1 の原始 7 乗根を表すのに $\sqrt{-3}$ つまり 1 の原始 3 乗根が必要であるが $U_7 \not\ni U_3$.). しかし, 後の 28.8 の様に, ある $n \in \mathbb{N}$ に対し, N を 1, 2, $\cdots$, n の最大公倍数とすれば, $\mathbb{Q}(U_N)/\mathbb{Q}$ は冪根による拡大になる. 28.8 は 28.15 の証明に必要である.

定義 28.7. 有限群 G の部分群 G_i からなる列で

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{1\}$$

となるものを 正規列 と呼ぶ.

補題 28.8. K を体とする. 自然数 n に対し, 1 の原始 m 乗根 ($m = 1, 2, \cdots, n$) の全てからなる集合を Γ_n ($\subset \overline{K}$) とすれば, $K(\Gamma_n)/K$ は冪根による拡大である.

証明 n に関する帰納法で示す. $K_n = K(\Gamma_n)$ とおく. $K = K_1 = K_2$, $K_3 = K(\sqrt{-3})$, $K_4 = K(\sqrt{-1})$ については主張は正しい. $n \geqq 5$ とし $n-1$ まで主張が成り立つてゐるとせよ. ζ_n を 1 の原始 n 乗根の 1 つとする. このとき $K_n = K_{n-1}(\zeta_n)$ であるから, K_n は K_{n-1} の Abel 拡大であつて, $[K_n : K_{n-1}] \leqq \varphi(n) < n$ である (27.4 より). Abel 群 $G_0 := \mathrm{Gal}\,(K_n/K_{n-1})$ は有限巡回群の直積 $H_1 \times H_2 \times \cdots \times H_r$ と表される (有限 Abel 群の構造定理). ここで

$$G_i = \{1\} \times \cdots \times \{1\} \times H_{i+1} \times \cdots \times H_r \ (< G_0) \quad (0 \leqq i \leqq r)$$

とおけば, G_0 の正規列 $G_0 \rhd G_1 \rhd \cdots \rhd G_{r-1} \rhd G_r = \{1\}$ が得られて, $G_{i-1}/G_i \cong H_i$ となつてゐる. 各 $1 \leqq i \leqq r$ について, K_n と K_{n-1} の中間体で, G_i に対応するものを L_i とする. 特に $L_0 = K_{n-1}$, $L_r = K_n$. G_0 は Abel 群だから $G_i \lhd G_0$ で, L_i は L_0 の Galois 拡大, $\mathrm{Gal}\,(L_i/L_0) \cong G_0/G_i$ であり, L_{i-1} が L_i と L_0 の中間体で部分群 $G_{i-1}/G_i < G_0/G_i$ に対応するものである. 即ち, $\mathrm{Gal}\,(L_i/L_{i-1}) \cong G_{i-1}/G_i \cong H_i$ で L_i は L_{i-1} の巡回拡大である (23.1, 23.3 参照). $|H_i| = m_i$ と記すと $m_i = [L_i : L_{i-1}] \leqq [K_n : K_{n-1}] < n$ であるから, K_{n-1} は (従つて L_{i-1} は) 1 の原始 m_i 乗根を含み, $L_i = L_{i-1}(\alpha_i)$, $\mathrm{irr}\,(\alpha_i, L_{i-1}) = x^{m_i} - a_i$ ($a_i \in L_{i-1}$) の形に表される (26.1 より). これで K_n が K_{n-1} の冪根による拡大であることが示された. K_{n-1} に関する帰納法の仮定より K_n が K の冪根による拡大であることがわかり, 帰納法の証明が完了する. □

以下では方程式の代数的可解性と Galois 群の可解性の関係を考へる.

定義 28.9. 有限群 G が 可解群 であるとは, 正規列 $G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{1\}$ が存在して, G_i/G_{i+1} ($0 \leqq i \leqq n-1$) が Abel 群になることをいふ. もちろん Abel 群は可解群である.

問 28.10. S_2, S_3, S_4 が可解群であることを示せ. (以下 28.14 まで, [N] の 16.1 節, [Iy] の §1.11)

問 28.11. 可解群の部分群は可解群であることを示せ.

問 28.12. 可解群から別の群への準同型の像は可解群であることを示せ.

問 28.13. 可解群 G に対し, 正規列 $G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{1\}$ で全ての G_i/G_{i+1} ($0 \leqq i \leqq n-1$) が素数位数の巡回群となるものが存在することを示せ.

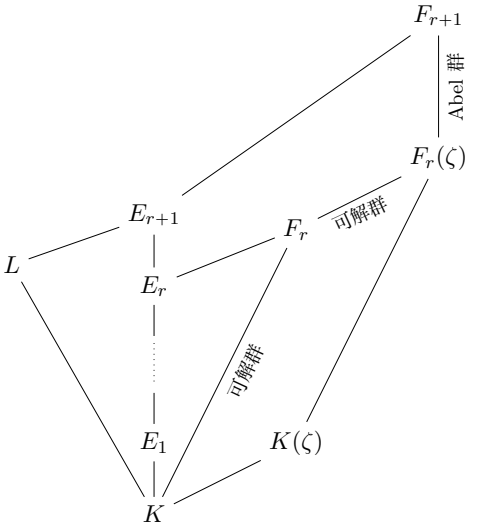
問 28.14. 群 G と $N \lhd G$ に対し, N と G/N がともに可解群ならば, G も可解群であることを示せ. (このことから, L/K が Galois 拡大であり, 中間体 M についても M/K が Galois 拡大のとき, $\mathrm{Gal}\,(L/M)$ と $\mathrm{Gal}\,(M/K)$ が可解群であれば $\mathrm{Gal}\,(L/K)$ も可解群であることが帰結される.)

定理 28.15. L/K が有限次拡大のとき, 次の 2 つは同値である.
(1) L を含む冪根による拡大 E/K がある.
(2) L を含む有限次 Galois 拡大 F/K で $\mathrm{Gal}(F/K)$ が可解群となるものがある.

証明 (1)⇒(2). 冪根による拡大 E/K を与へる体の列の長さ r による数学的帰納法で, (2) の様な拡大 F/K が存在することを示す.
Step 1 まづ, $r=0$ のときは $L=E$ であり, $F=E$ とすれば $\mathrm{Gal}(F/K)=\{1\}$ となる. ゆゑに, この場合は (1)⇒(2) が成り立つ.
Step 2 $r\geqq 0$ とし, 冪根による拡大 E/K を与へる体の列の長さが r までは (1)⇒(2) が正しいと仮定する. いま体の列

$$K=E_0\subset E_1\subset\cdots\subset E_r\subset E_{r+1}=E,$$
$$E_{i+1}=E_i(\sqrt[n_i]{a_i})\quad(\exists a_i\in E_i)$$

があつて $L\subset E$ となつてゐる. 一方, 主張 (1) の E/K として, この体の列の部分



$$K=E_0\subset E_1\subset\cdots\subset E_r$$

を考へ, L として E_r 自身を考へれば, 帰納法の仮定より E_r を含む K の Galois 拡大 F_r があつて, $\mathrm{Gal}(F_r/K)$ が可解群になつてゐる.
Step 3 ζ を 1 の原始 n_r 乗根とする. $K(\zeta)/K$ も F_r/K も Galois 拡大であるから 22.2 の後半により, $F_r(\zeta)/K$ は Galois 拡大であり, 23.3(2) と (3) から, $\mathrm{Gal}(F_r(\zeta)/K)\rhd\mathrm{Gal}(F_r(\zeta)/F_r)$ で, この 2 群の剰余類群は可解群 $\mathrm{Gal}(F_r/K)$ と同型であり, 27.4 から $\mathrm{Gal}(F_r(\zeta)/F_r)$ は Abel 群, 従つて可解群だから, $\mathrm{Gal}(F_r(\zeta)/K)$ も可解群である (28.14).
Step 4 さて, $a_r\in E_r\subset F_r$ で, 各 $\sigma\in\mathrm{Gal}(F_r/K)$ について,

$$x^{n_r}-{a_r}^{\sigma}=\prod_{\nu=0}^{n_r-1}\left(x-\sqrt[n_r]{{a_r}^{\sigma}}\,\zeta^{\nu}\right)$$

である. ここで $\mathrm{Gal}(F_r/K)=\{\sigma_1,\cdots,\sigma_N\}$ と記すこととし, 次の体を考へる :

$$F_{r+1}=F_r\left(\zeta,\sqrt[n_r]{{a_r}^{\sigma_1}},\cdots,\sqrt[n_r]{{a_r}^{\sigma_N}}\right).$$

Step 5 拡大 F_{r+1}/K が所望の Galois 拡大体 F/K の 1 つである. それを示さう. まづ, $F_{r+1}/F_r(\zeta)$ は Abel 拡大 $F_r(\zeta,\sqrt[n_r]{{a_r}^{\sigma_i}})/F_r(\zeta)$ 達の合成体ゆゑ, 23.7 より, Abel 拡大, 従つて $\mathrm{Gal}(F_{r+1}/F_r(\zeta))$ は可解群である. また F_{r+1} は多項式

$$\prod_{\sigma\in\mathrm{Gal}(F_r/K)}\left(x^{n_r}-{a_r}^{\sigma}\right)\in K[x]$$

の最小分解体であるから F_{r+1}/K は Galois 拡大であり, 明らかに

$$E_{r+1}=E_r\left(\sqrt[n_r]{a_r}\right)\subset F_r\left(\sqrt[n_r]{a_r}\right)\subset F_{r+1}$$

である. Step 3 より拡大 $F_r(\zeta)/K$ は Galois であり, それゆゑ $\mathrm{Gal}(F_{r+1}/K)\rhd\mathrm{Gal}(F_{r+1}/F_r(\zeta))$ である (23.3(2)). この 2 群の剰余類群は可解群 $\mathrm{Gal}(F_r(\zeta)/K)$ に同型で, $\mathrm{Gal}(F_{r+1}/K)$ も可解群 (28.14). 従つて, 体の列の長さが $r+1$ でも (1)⇒(2) は正しい.

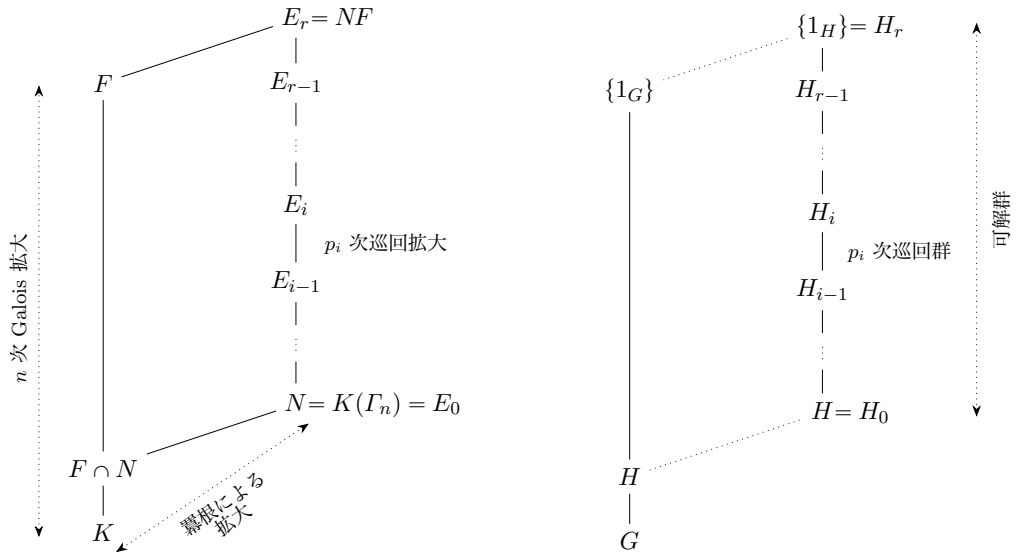
(2)⇒(1). 仮定の F を含む K の代数的閉包を $\overline{K}$ とする. また $G=\mathrm{Gal}(F/K)$, $|G|=n$ とし, $\overline{K}$ において 28.8 の記号で Γ_n による拡大を $N=K(\Gamma_n)$ とおく. このとき Galois 拡大 F/K の N による持ち上げ NF/N も Galois 拡大で, その Galois 群 $H=\mathrm{Gal}(NF/N)$ は G のある部分群と同型である (23.5). よつて H は可解群 (28.11) で, 正規列

$$H=H_0\rhd H_1\rhd\cdots\rhd H_r=\{1\},\quad (\,H_i/H_{i+1}\text{ は位数が素数の巡回群 (}\ p_i\text{ 次とする)})$$

が存在する (28.13). $E_i=(NF)^{H_i}$ とおけば, 上の正規列に対応して NF/N の中間体の列

$$K\subset N=E_0\subset E_1\cdots\subset E_r=NF$$

を得る. E_{i+1}/E_i は p_i 次の巡回拡大で, $p_i=[E_{i+1}:E_i]\,\big|\,[NF:N]\,\big|\,n$ であるから 1 の原始 p_i 乗根は N に, 従つて E_i に含まれ, 26.1 より, $E_{i+1}=E_i(\sqrt[p_i]{a_i})$ となる $a_i\in E_i$ が存在する.



このとき $\deg\mathrm{irr}(\sqrt[p_i]{a_i},E_i,x)=[E_{i+1}:E_i]=p_i$ ゆゑ, $\mathrm{irr}(\sqrt[p_i]{a_i},E_i,x)=x^{p_i}-a_i$ でなければならない. 一方 28.8 によれば, N/K は冪根による拡大であるから, 28.5 (2) より $E=NF$ は求める拡大体である. □

注意 28.16. 我々の冪根による拡大の定義は [N] の本のそれと異るため, 冪根による拡大の持ち上げが冪根による拡大になるとは限らないし, いくつかの冪根による拡大の合成体が再び冪根による拡大になるとも限らない (28.5 (1), (2)). これが原因で 28.15 の証明が複雑になつてしまふ. この証明は [Iy] に書かれてゐるものである.

上の定理から容易に次の定理が得られる.

定理 28.17. 体 K は元 $a_0,\cdots,a_n$ により $K=\mathbb{Q}(a_0,a_1,\cdots,a_n)$ となつてゐるとする. $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_n$ の K 上の最小分解体を L とする. 次の 2 つは同値.
(1) 方程式 $f(x)=0$ は代数的に解ける.
(2) Galois 群 $\mathrm{Gal}(L/K)$ は可解群である.

証明 (1)⇒(2). 定義から (1) の主張は, K の冪根による拡大 E で L を含むものがあることと同値である. 28.15 より, このとき L を含む K の Galois 拡大 F/K で $\mathrm{Gal}(F/K)$ が可解群となるものがある. 28.12 により $\mathrm{Gal}(L/K)$ も可解群. (2)⇒(1) は 28.15 より明らか. □

演 習 問 題

28.18. 方程式 $x^6+x^5+x^4+x^3+x^2+x+1=0$ の根は四則演算, 平方根号, 3 乗根号によつて書けることを示せ. 具体的な表示は要求しない.

28.19. 22.17 で調べた $\alpha=\exp(2\pi i/7)+\exp(-2\pi i/7)$ に関する事を既知として次の問に答へよ.
(1) $\mathbb{Q}(\alpha)/\mathbb{Q}$ は Galois 拡大で, $\mathrm{Gal}\,(\mathbb{Q}(\alpha)/\mathbb{Q})$ は位数 3 の巡回群であることを示せ.
(2) α を四則演算と根号 $\sqrt{\ }$, $\sqrt[3]{\ }$ だけで表せ. $\Big($ 答 : $\alpha=\frac{1}{3}\Big(-\sqrt[3]{\frac{-7+21\sqrt{-3}}{2}}-\sqrt[3]{\frac{-7-21\sqrt{-3}}{2}}-1\Big)$. $\Big)$

28.20. 方程式 $x^5-2=0$ の $\mathbb{Q}$ 上の最小分解体を K とする. $\mathrm{Gal}\,(K/\mathbb{Q})$ はどの様な群か.
(Hint : $\zeta=\exp(2\pi i/5)$ とおく. σ,τ を $\sqrt[5]{2}^{\,\sigma}=\sqrt[5]{2}\,\zeta$, $\zeta^\sigma=\zeta$, $\sqrt[5]{2}^{\,\tau}=\sqrt[5]{2}$, $\zeta^\tau=\zeta^2$ で定めると $\sigma,\tau\in\mathrm{Gal}\,(K/\mathbb{Q})$ であり, $\mathrm{Gal}\,(K/\mathbb{Q})=\langle\sigma,\tau\rangle$.)

28.21. 1 の原始 11 乗根について考へる.[40] $\zeta=\exp(2\pi i/11)$, $\rho=\exp(2\pi i/5)$ とおく. 以下, すべての数は複素数体 $\mathbb{C}$ の元であるとする. まづ

$$V_1=\sqrt[5]{\tfrac{11}{4}\big(89+25\sqrt{5}-5\sqrt{-5-2\sqrt{5}}+45\sqrt{-5+2\sqrt{5}}\,\big)}=3.31568\cdots+i\,0.07884\cdots,$$
$$V_2=\sqrt[5]{\tfrac{11}{4}\big(89+25\sqrt{5}+5\sqrt{-5-2\sqrt{5}}-45\sqrt{-5+2\sqrt{5}}\,\big)}=3.31568\cdots-i\,0.07884\cdots,$$
$$V_3=\sqrt[5]{\tfrac{11}{4}\big(89-25\sqrt{5}-5\sqrt{-5+2\sqrt{5}}-45\sqrt{-5-2\sqrt{5}}\,\big)}=3.19787\cdots-i\,0.87953\cdots,$$
$$V_4=\sqrt[5]{\tfrac{11}{4}\big(89-25\sqrt{5}+5\sqrt{-5+2\sqrt{5}}+45\sqrt{-5-2\sqrt{5}}\,\big)}=3.19787\cdots+i\,0.87953\cdots$$

とおく. ここで 5 乗根は 5 つづつ存在するが, 明確にするため, 上の様に虚数部分の絶対値が最も小さいものを選ぶことにした. 但し $\sqrt{-5+2\sqrt{5}}$ と $\sqrt{-5-2\sqrt{5}}$ の虚数部分はともに正にとつてゐる. 以下の問に答へよ.

(1) $V_1V_2=V_3V_4=11$ であることを示せ.
(2) $y=\zeta+\zeta^{-1}$ とおくと y は
$$y^5+y^4-4y^3-3y^2+3y+1=0$$
を満足することを示せ.
(3) (2) の y は
$$y=-\tfrac{1}{5}(1+V_1\,\rho^3+V_2\,\rho^2+V_3\,\rho^2+V_4\,\rho^3)\quad(=2\cos(\tfrac{2\pi}{11})=1.68250\cdots)$$
と書けることを示せ.

以上より $\zeta^2-y\zeta+1=0$ を解いて ζ の冪根表示が得られる.[41]

[40] この話題について Ian Stewart : Galois theory §21.1 に記述があるが, (4th ed. までの全てに) 多くの誤りを含む. Olaf Neumann : *Cyclotomy: From Euler through Vandermonde to Gauss*, Leonhard Euler: Life, Work and Legacy, Robert E. Bradley and C. Edward Sandifer (Editors), pp. 323-362 に正確な記述がある.
[41] この状況で $\mathbb{Q}(\zeta)/\mathbb{Q}$ が冪根による拡大 $\mathbb{Q}(V_1,V_2,V_3,V_4,\rho)/\mathbb{Q}$ の中間体であることがわかるが, この拡大 $\mathbb{Q}(\zeta)/\mathbb{Q}$ は冪根による拡大になつてゐるであらうか.

§ 29. 一般代数方程式

$a_1,\ a_2,\ \cdots,\ a_n$ は体 K 上で代数的に独立であるとする. このとき, これらを係数とする多項式 $g(x)=x^n+a_1x^{n-1}+\cdots+a_n$ を体 K 上の n 次一般多項式と呼び, 方程式 $g(x)=0$ を n 次一般方程式といふ. 2 次の一般方程式 $x^2+a_1x+a_2=0$ は代数的に解けて, 解の公式

$$x=\frac{-a_1\pm\sqrt{{a_1}^2-4a_2}}{2}$$

が知られてゐる. 3 次や 4 次の一般方程式も代数的に解けてその解の公式も与へられてゐる. しかるに 5 次以上の一般方程式は代数的には解けず, その様な解の公式は存在しない. これを最初に証明したのは N.H. Abel である. 以下, 28.17 を用ゐて一般方程式の可解性を調べる.

いま $t_1,\ t_2,\ \cdots,\ t_n$ は体 K 上代数的に独立であるとし, $L=K(t_1,\cdots,t_n)$ とおく. L は変数 $t_1,\ \cdots,\ t_n$ に関する有理函数体と呼ばれるものである. $\{1,2,\cdots,n\}$ 上の対称群を S_n とすれば S_n の元 σ は ${t_i}^\sigma=t_{\sigma(i)}$ とおいて $\{t_1,\cdots,t_n\}$ の置換を引き起す. さて, K の各元を不変にして, それ以外の元には置換 σ を施すことによつて L/K の自己同型が得られる. それも σ で表すこととし $S_n<\operatorname{Aut}L/K$ とみなす. L における S_n の不変体を

$$F=L^{S_n}=K(t_1,\cdots,t_n)^{S_n}$$

と書けば, 22.10 により L/F は S_n を Galois 群とする Galois 拡大に他ならない. F に属する多項式は $t_1,\ \cdots,\ t_n$ の対称式と呼ばれ, そのうち次の形の式を基本対称式と呼ぶ:

$$s_1=t_1+t_2+\cdots+t_n,\quad s_2=\sum_{i<j}t_it_j,\quad \cdots,\ s_n=t_1t_2\cdots t_n.$$

明らかに $K(s_1,s_2,\cdots,s_n)\subset F\subset L$ で, 22.10(3) により $[L:F]=|S_n|=n!$ であるが, 次のことが成り立つ.

例題 29.1. 上の記号の元で
(1) $K(s_1,\cdots,s_n)=F$.
(2) $s_1,\ \cdots,\ s_n$ は K 上代数的に独立である.

証明 (1) $[L:K(s_1,\cdots,s_n)]\leqq n!$ となることを示せばよい. n に関する帰納法で証明する. $n=1$ のときは明らかである. $M=K(s_1,\cdots,s_n)$ とし

$$f(x)=\prod_{i=1}^{n}(x-t_i)=x^n-s_1x^{n-1}+\cdots+(-1)^ns_n$$

とおけば $f(x)\in M[x],\ f(t_n)=0$ であるから $[M(t_n):M]\leqq n$ である. 一方 $N=K(t_n)$ とおけば, $L=N(t_1,\cdots,t_{n-1})$ である. いま $t_1,\ \cdots,\ t_{n-1}$ に関する基本対称式を ${s_1}',\ \cdots,\ {s_{n-1}}'$ とすれば

$$s_1={s_1}'+t_n,\quad s_j=t_n{s_{j-1}}'+{s_j}'\quad(2\leqq j\leqq n-1),\quad s_n={s_n}'t_n$$

となるから, $K(s_1,\cdots,s_n,t_n)=K({s_1}',\cdots,{s_{n-1}}',t_n)$ となり, $M(t_n)=N({s_1}',\cdots,{s_{n-1}}')$ を得る. 帰納法の仮定により $[L:M(t_n)]\leqq[L:K({s_1}',\cdots,{s_{n-1}}')]\leqq(n-1)!$ である. よつて

$$[L:M]=[L:M(t_n)][M(t_n):M]\leqq(n-1)!\,n=n!$$

となる.
(2) L/F は代数的であるから, 13.6 により $\operatorname{trans.deg}_K F=\operatorname{trans.deg}_K L=n$ となる. このとき (1) から, n 個の元 $s_1,\ \cdots,\ s_n$ は K 上代数的に独立でなければならない. □

29.1 から次の定理が得られる.

定理 29.2. $g(x)=x^n+a_1x^{n-1}+\cdots+a_n$ を体 K の一般多項式 (従つて a_1, $\cdots$, a_n は K 上代数的独立) とし, E を $N=K(a_1,\cdots,a_n)$ 上の $g(x)$ の最小分解体とする. このとき E/N は n 次対称群 S_n と同型な Galois 群をもつ Galois 拡大である.

証明 29.1 で示した様に, t_1, $\cdots$, t_n は K 上代数的に独立とし, これらに関する基本対称式を s_1, $\cdots$, s_n とするとき, $L=K(t_1,\cdots,t_n)$ は $F=K(s_1,\cdots,s_n)$ 上の Galois 拡大で $\mathrm{Gal}\,(L/F)=S_n$, また s_1, $\cdots$, s_n は K 上代数的に独立である. 従つて K 上の同型 $\sigma\colon N\xrightarrow{\sim}F$ $(a_i\mapsto(-1)^is_i)$ があり, この写像で一般多項式 $g(x)$ は

$$g^\sigma(x)=x^n-s_1x^{n-1}+\cdots+(-1)^ns_n=\prod_{i=1}^n(x-t_i)$$

に写される. L は $g^\sigma(x)$ の F 上の最小分解体であるから, σ は $\overline{\sigma}\colon E\xrightarrow{\sim}L$ に拡張される (17.2 による). このとき $\varphi\colon \mathrm{Gal}\,(E/N)\to\mathrm{Gal}\,(L/F)$ $(\rho\mapsto\overline{\sigma}\rho\overline{\sigma}^{-1})$ は同型写像である. よつて $\mathrm{Gal}\,(E/N)\simeq S_n$ である. □

29.2 と 28.17 から次の定理が得られる.

定理 29.3. (Galois の定理) 体 K 上の n 次の一般方程式 $x^n+a_1x^{n-1}+\cdots+a_n=0$ は $n\leqq 4$ のとき, しかもそのときに限つて代数的に解ける.

証明 対称群 S_n は $n\leqq 4$ のときは可解群であるが, $n\geqq 5$ ならば非可解群であつた (29.6 で示される[42]). $x^n+a_1x^{n-1}+\cdots+a_n$ は素体 $\mathbb{Q}$ 上の一般多項式でもある. よつて 29.2 で $K=\mathbb{Q}$ とおけば, 28.17 から主張が導かれる. □

演 習 問 題

$n\geqq 5$ のとき n 次対称群 S_n が可解群でないことを以下に従つて示せ.

29.4. $S_n=\langle(1\ 2),(1\ 3),\cdots,(1\ n)\rangle$ であることを示せ.
(Hint : $(i\ j)=(1\ i)(1\ j)(1\ i)$ であることと, S_n が互換の全体で生成されることを使ふ.)

29.5. A_n を n 次交代群[43] とする. $n\geqq 3$ のとき, $A_n=\langle(1\ 2\ 3),\ (1\ 2\ 4),\ \cdots,\ (1\ 2\ n)\rangle$ であることを示せ. (Hint : A_n が 2 個の互換の積の全体から生成されること, 29.4, および $(1\ 2)(1\ j)=(1\ 2\ j)^2$, $(1\ i)(1\ j)=(1\ 2\ i)(1\ 2\ j)^2$ $(3\leqq i,3\leqq j)$ であることを使ふ.)

29.6. $n\geqq 5$ とする. H は A_n の正規部分群で, A_n/H は Abel 群であるとせよ. 次の問に答へよ. 但し, i, j, k はどれも 1 でも 2 でもなく, 互ひに異る任意の数字の組である.

(1) $(1\ 2\ k)=(1\ i\ k)(k\ 2\ j)(1\ i\ k)^{-1}(k\ 2\ j)^{-1}$ を確かめよ.
(2) $(1\ 2\ k)\in H$ であることを示せ. (Hint : 仮定より $H\supset[A_n:A_n]$.)
(3) $H=A_n$ を示し, A_n が可解群でないことを確認せよ.

29.7. $n\geqq 5$ とする. S_n は可解群でないことを示せ (Hint : 28.11).

[42] 代数学 3 で既習かも知れない.
[43] S_n に属して, その符号が 1 である置換, つまり, 偶数個の互換の積で表される置換のすべてからなる S_n の部分群のこと.

§ 30. 3 次の一般方程式の解法

a, b, c を不定元として, 3 次の一般方程式

$$f(x) = x^3 + ax^2 + bx + c = 0 \tag{30.1}$$

の解の公式を求めてみる. (30.1) の 3 つの解を t_1, t_2, t_3 とおく. 以下, $\omega = \frac{-1+\sqrt{-3}}{2}$, $K = \mathbb{Q}(a,b,c)$, $L = K(t_1,t_2,t_3)$ とする. 以下, 第 29 節の記号に従ふ. 29.3 が得られたといつても, そこから直ちに解の公式を書き下せるわけではなく, 別途, 作業が必要である. まづ, $S_3 = \mathrm{Gal}(L/K)$ とその部分群 $A_3 = \{\varepsilon,\ (1\ 2\ 3),\ (1\ 3\ 2)\}$ について, の正規列

$$S_3 \rhd A_3 \rhd \{1\}$$

において S_3/A_3 も A_3 も Abel 群であるから, 確かに S_3 は可解群である. このとき, $\Delta = (t_1 - t_2)(t_2 - t_3)(t_3 - t_1)$ を不変にする元の全体が A_3 に一致する. もちろん $\Delta^2 \in K$ の筈であるが, 少し計算すれば $\Delta^2 = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$ を得る. 上の正規列に対応して, 体の拡大列 $L \supset K(\Delta) \supset K$ ($[K(\Delta) : K] = 2$) があるが, 28.17 により, L/K は冪根による拡大に含まれる筈である. 実際に, その様な冪根拡大を構成してみる. その際,

$$\beta = t_1 + \omega t_2 + \omega^2 t_3, \quad \gamma = t_1 + \omega^2 t_2 + \omega t_3$$

を考へることが鍵となる. $-a = t_1 + t_2 + t_3 \in K$ であるから, $K(\beta,\gamma,\omega) \supset L$ がわかるが, 体 $L(\omega) = K(\beta,\gamma,\omega)$ は K 上の冪根による拡大として記述できるのである. これは 12 次拡大である. 少し計算すれば $\beta\gamma = a^2 - 3b$, $\beta^3 + \gamma^3 = -2a^3 + 9ab - 27c$ を得,

$$K(\beta,\gamma,\omega) = K(\beta,\omega) = K(\gamma,\omega)$$

がわかる. また β^3 と γ^3 は y の 2 次方程式

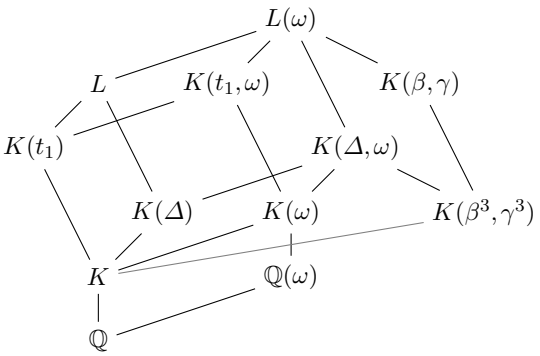
$$y^2 - (-2a^3 + 9ab - 27c)y + (a^2 - 3b)^3 = 0$$

の 2 根である. また $f'(t_1) = 3{t_1}^2 + 2at_1 + b = (t_1 - t_2)(t_1 - t_3)$ で $t_2 - t_3 = -\Delta/f'(t_1) \in K(\Delta,t_1)$, $t_2 + t_3 = -a - t_1 \in K(t_1)$ だから t_2, $t_3 \in K(\Delta,t_1)$ がわかり $L = K(\Delta,t_1)$ である.

もちろん $f(t_1) = {t_1}^3 + a{t_1}^2 + bt_1 + c = 0$ であるから, $[L : K(\Delta)] = 3$ であり, L は $K(\Delta)$ 上の vector 空間としての基底 $\{1, t_1, {t_1}^2\}$ を持つ. また

$$\omega \notin L = \mathbb{Q}(t_1,t_2,t_3)$$

であることに注意されたい. つまり L は K 上の冪根による拡大に含まれるのであるが, L 自身は冪根による拡大にはならない.



例題 30.2. （Cardano の公式） 体 K 上の方程式 $x^3+px+q=0$ （$p,\,q\in K$）の解は,

$$\beta+\gamma,\quad \omega\beta+\omega^2\gamma,\quad \omega^2\beta+\omega\gamma \tag{30.3}$$

で与へられることを示せ. 但し, ω は 1 の原始 3 乗根で,

$$\beta=\sqrt[3]{-\frac{q}{2}+\sqrt{\Big(\frac{q}{2}\Big)^2+\Big(\frac{p}{3}\Big)^3}},\quad \gamma=\sqrt[3]{-\frac{q}{2}-\sqrt{\Big(\frac{q}{2}\Big)^2+\Big(\frac{p}{3}\Big)^3}}.$$

解答 前 page の説明の記号で $a=0,\,b=p,\,c=q$ なので, β^3 と γ^3 は 2 次方程式

$$y^2+27qy-27p^3=0$$

の 2 解である. ここに, この方程式の判別式は $(27q)^2+4\cdot 27p^3\,(=-27\Delta^2)$ で,

$$\begin{aligned}\beta^3,\ \ \gamma^3&=\tfrac{1}{2}\big(-27q\pm\sqrt{(27q)^2+4\cdot 27p^3}\big)\\&=3^3\bigg(-\frac{q}{2}\pm\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}\bigg).\end{aligned}$$

但し, $\beta\gamma=-3p$ を満たす様な, ある 3 乗根を選べば,

$$t_1+\omega\,t_2+\omega^2\,t_3=\beta,\quad\ \ t_1+\omega^2\,t_2+\omega\,t_3=\gamma$$

となる. このとき $t_1+t_2+t_3=0$ と合はせて (30.3) の 3 根が得られる. □

注意 30.4. (1) 30.2 の 1 例として

$$(x-1)(x-2)(x+3)=x^3-7x+6=0$$

のとき $(\frac{q}{2})^2+(\frac{p}{3})^3=-\frac{100}{27}$ で,

$$\begin{aligned}\sqrt[3]{-\frac{q}{2}\pm\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}&=\sqrt[3]{-3\pm\frac{10}{3\sqrt{3}}\,i}=\sqrt{\frac{-9\sqrt{3}\pm 10\,i}{3\sqrt{3}}}=\frac{\sqrt[3]{-9\sqrt{3}\pm 10\,i}}{\sqrt{3}}\\&=\frac{\sqrt[3]{(\sqrt{3}\pm 2\,i)^3}}{\sqrt{3}}=\frac{\sqrt{3}\pm 2\,i}{\sqrt{3}}\ \ (3\text{ 乗根を 1 つ選んだ})\end{aligned}$$

なので, 3 つの有理数解 $2,\,-3,\,1$ が

$$\frac{\sqrt{3}+2\,i}{\sqrt{3}}+\frac{\sqrt{3}-2\,i}{\sqrt{3}},\quad \omega\,\frac{\sqrt{3}+2\,i}{\sqrt{3}}+\omega^2\,\frac{\sqrt{3}-2\,i}{\sqrt{3}},\quad \omega^2\,\frac{\sqrt{3}+2\,i}{\sqrt{3}}+\omega\,\frac{\sqrt{3}-2\,i}{\sqrt{3}}$$

なる表示で得られる.

(2) 30.2 の計算から, 与へられら 3 次方程式が, 3 つの実根を持つ場合, $\Delta^2>0$ である. このとき, $-27\Delta^2<0$ であるから, (30.3) の表示の 3 乗根号の内部が虚数である. このことは, Cardano の公式では, 実根を表すのに, どうしても虚数を用いる必要があることを示してゐて, 古来, 還元の不可能性などと呼ばれてゐる.

演 習 問 題

30.5. 本文での説明と 23.17 を参考に, 3 次方程式 $x^3+x+1=0$ の解を四則演算と冪根のみで表せ.

30.6. 一般に 3 次の monic な既約多項式 $f(x)=x^3+ax^2+bx+c\in\mathbb{Q}[x]$ について, その Galois 群は A_3 (3 次巡回群, $\lhd S_3$) または S_3 と同型になり, そのことは上記の Δ が $\mathbb{Q}$ 内の平方元であるか否かで, 判定できる. このことを示せ.

§ 31. 4 次の一般方程式の解法

4 次一般方程式の解法を述べる. a, b, c, d を不定元として $K = \mathbb{Q}(a, b, c, d)$ とおき, K 上の 4 次多項式 $f(x) = x^4 + ax^3 + bx^2 + cx + d$ を考へる. t_1, t_2, t_3, t_4 を $f(x) = 0$ の根として, $L = K(t_1, t_2, t_3, t_4)$ とおく. 以下, 第 29 節の記号を踏襲してゐる. 4 次対称群 S_4 の正規列

$$S_4 \rhd A_4 \rhd V \rhd H \rhd \{1\}$$

を考へる. 但し, $V = \{\varepsilon, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$, $H = \{\varepsilon, (1\ 2)(3\ 4)\}$ である. V が存在してゐるのは幸運である. ここで S_4/A_4, A_4/V, V/H, H はどれも Abel 群である. いま

$$\Delta = (t_1 - t_2)(t_1 - t_3)(t_1 - t_4)(t_2 - t_3)(t_2 - t_4)(t_3 - t_4) \quad (f(x) \text{ の } \underline{\text{判別式}} \text{ と呼ぶ})$$

とおくと, $\Delta^2 \in K$ である. $\mathrm{Gal}(L/K) = S_4$ とみて, 上の正規列に対応する体の拡大列は

$$K \subset K(\Delta) \subset K(t_1t_2 + t_3t_4, t_1t_3 + t_2t_4, t_1t_4 + t_2t_3) \subset K(t_1t_2 + t_3t_4) \subset K(t_1, t_2, t_3, t_4)$$

である (★). ここで $\alpha = t_1t_2 + t_3t_4$, $\beta = t_1t_3 + t_2t_4$, $\gamma = t_1t_4 + t_2t_3$ とおく. これらの基本対称式は a, b, c, d の $\mathbb{Q}$ 上の多項式の筈であるが,

$$\alpha + \beta + \gamma = b, \quad \alpha\beta + \beta\gamma + \gamma\delta = ac - 4d, \quad \alpha\beta\gamma = a^2d - 4bd + c^2$$

が, いくらかの計算ののち得られる. それゆゑ α, β, γ は K 上の 3 次方程式

$$g(y) = y^3 + by^2 - (ac - 4d)y + (a^2d - 4bd + c^2) = 0$$

の根として得られる. この方程式は, 第 30 節の方法で解ける. ここで, 容易に確かめられる

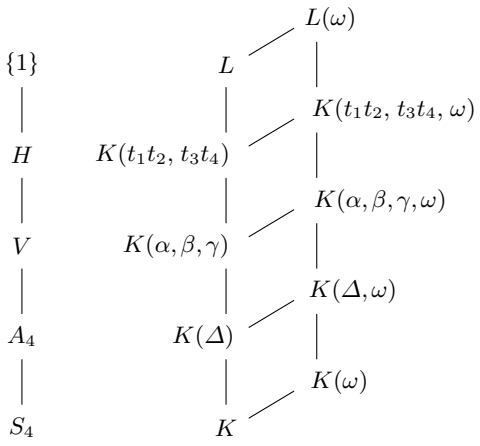
$$(\alpha - \beta)(\beta - \gamma)(\gamma - \alpha) = -\Delta$$

に注意せよ. さらに $t_1t_2 + t_3t_4 = \alpha$, $(t_1t_2)(t_3t_4) = d$ より t_1t_2 と t_3t_4 が 2 次方程式 $z^2 - \alpha z + d = 0$ の解として得られる. $(t_1 + t_2)t_3t_4 + (t_3 + t_4)t_1t_2 = -c$ と $t_1 + t_2 + t_3 + t_4 = -a$ から $t_1 + t_2, t_3 + t_4 \in K(t_1t_2, t_3t_4)$ がわかる :

$$K(t_1t_2, t_3t_4, t_1 + t_2, t_3 + t_4) = K(t_1t_2, t_3t_4).$$

$t_1 + t_2$ と t_1t_2 の値から 2 次方程式を解いて t_1 と t_2 が得られる. また, $t_3 + t_4$ と t_3t_4 の値から t_3 と t_4 が得られるが, これは $t_1t_2t_3 + \cdots + t_2t_3t_4 = -c$ と t_1, t_2, $t_3 + t_4$, t_3t_4 の値から 1 次方程式を解いても得られるから, 体の拡大は生じない.

ここで 1 つ注意をしておく. 3 次一般方程式の解法では, 1 の原始 3 乗根 ω を添加する必要があつた. しかし, この解法では, 正規列の隣接したどの 2 つの群の剰余類群にも 4 次巡回群が含まれないから, $i = \sqrt{-1}$ を添加する必要がない. 以上を図にまとめておく.



演 習 問 題

31.1. 本文中の (★) が正しいことを示せ.

31.2. 本文で説明した方法に沿つて, 4 次方程式 $x^4 + x + 1 = 0$ を解き, 解を四則演算と冪根のみで表せ.

§ 32. 円分多項式

以下, 本節では有理数体 $\mathbb{Q}$ 上の円分体を考察する. 1 の原始 n 乗根 ζ を 1 つ固定し,

$$\Phi_n(x) = \prod_{\substack{0<r<n \\ \gcd(r,n)=1}} (x-\zeta^r)$$

とおく. これは 1 のすべての原始 n 乗根を根とする多項式で, n 次 円分多項式 と呼ばれる.

例 32.1. 円分多項式 $\Phi_n(x)$ の例を挙げておく. 素数 p については

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

である. その他を少し計算してみれば

$$\begin{aligned}
&\Phi_1(x) = x-1, \quad \Phi_4(x) = x^2+1, \quad \Phi_6(x) = x^2-x+1, \quad \Phi_8(x) = x^4+1, \\
&\Phi_9(x) = x^6+x^3+1, \quad \Phi_{10}(x) = x^4-x^3+x^2-x+1, \quad \Phi_{12}(x) = x^4-x^2+1, \\
&\Phi_{14}(x) = x^6-x^5+x^4-x^3+x^2-x+1, \quad \Phi_{15}(x) = x^8-x^7+x^5-x^4+x^3-x+1, \\
&\Phi_{16}(x) = x^8+1, \quad \Phi_{18}(x) = x^6-x^3+1, \quad \Phi_{18}(x) = x^8-x^6+x^4-x^2+1, \quad \cdots\cdots
\end{aligned}$$

と, 係数が ± 1 のみになる様に見えるが, 反例がある :

$$\begin{aligned}
\Phi_{105}(x) = {} & x^{48}+x^{47}+x^{46}-x^{43}-x^{42}-\boxed{2}x^{41}-x^{40}-x^{39}+x^{36}+x^{35}+x^{34} \\
& +x^{33}+x^{32}+x^{31}-x^{28}-x^{26}-x^{24}-x^{22}-x^{20}+x^{17}+x^{16}+x^{15} \\
& +x^{14}+x^{13}+x^{12}-x^9-x^8-\boxed{2}x^7-x^6-x^5+x^2+x+1.
\end{aligned}$$

命題 32.2. 円分多項式について次が成り立つ
(1) $\deg \Phi_n(x) = \varphi(n)$ (Euler の函数).
(2) $x^n - 1 = \prod_{d|n} \Phi_d(x)$.
(3) $\Phi_n(x) \in \mathbb{Z}[x]$.

証明 (1) は明かである. また 1 の n 乗根の任意の 1 つをとれば, それは, 唯 1 つのある約数 $d|n$ に対して 1 の原始 d 乗根であるから, (2) が成り立つ. (3) を n の帰納法で示す. いま

$$x^n - 1 = \Phi_n(x)\, f(x), \qquad f(x) = \prod_{d|n,\, d<n} \Phi_d(x) \tag{32.3}$$

とすれば, 帰納法の仮定により $f(x) \in \mathbb{Z}[x]$. また $f(x)$ の最高次の係数は 1 であるから, それは 原始多項式 [44] である. (32.3) を利用しての, n に関する数学的帰納法から $\Phi_n(x) \in \mathbb{Q}[x]$ となることが示されるから, 下記の 32.4 により $\Phi_n(x) \in \mathbb{Z}[x]$ がわかる. □

問 32.4. R を UFD (一意分解環) とし, K をその商体とせよ. $f(x), g(x) \in R[x]$ で $g(x) \in R[x]$ は原始多項式であるとせよ. $K[x]$ において $f(x) = g(x)\,h(x)$ $(h(x) \in K[x])$ と分解されれば, $h(x) \in R[x]$ である.

[44] $g(x) = a_0x^n + a_{n-1}x^{n-1} + \cdots + a_n$ の係数の最大公約数が 1, $\gcd(a_0, \cdots, a_n) = 1$, であること.

定理 32.5. $\Phi_n(x)$ は $\mathbb{Q}[x]$ において既約な多項式である. 即ち $\Phi_n(x) = \mathrm{irr}\,(\zeta, \mathbb{Q}, x)$.

証明 ζ を 1 の原始 n 乗根とし, $f(x)$ を ζ を根とする既約かつ原始的な $\mathbb{Z}$ 上の多項式とする. このとき $f(x)\,|\,x^n-1$ で, 32.4 から $x^n-1 = f(x)g(x)$ となる $g(x) \in \mathbb{Z}[x]$ がある. いま p を n と互ひに素な任意の素数とすれば, $f(\zeta^p) = 0$ となることが次の様にして示される. これの否定 $f(\zeta^p) \neq 0$ を仮定する. このとき $g(\zeta^p) = 0$ でなくてはならない. $g(x^p)$ は ζ を根にもつから $g(x^p) = f(x)h(x)$ となる $h(x) \in \mathbb{Z}[x]$ が存在する. いま任意の元 $a \in \mathbb{Z}$ に対し, 対応する剰余類を $\overline{a} \in \mathbb{F}_p$ と記し, 任意の多項式 $\varphi(x) \in \mathbb{Z}[x]$ に対し, その係数を対応する剰余類に置き替へたものを $\overline{\varphi}(x)$ と書くことにする. このとき $\overline{a}^{\,p} = \overline{a}$ に注意すれば,

$$\overline{f}(x)\overline{h}(x) = \overline{g}(x^p) = \overline{g}(x)^p$$

であるから, $\overline{f}(x)$ と $\overline{g}(x)$ は共通根を持つ. 従つて $\mathbb{F}_p$ 上で $x^n-1 = \overline{f}(x)\overline{g}(x)$ は重根を持ち, これは仮定 $\gcd(p,n) = 1$ に矛盾する. 上のことを用ゐて, 一般に $\gcd(r,n) = 1$ ならば ζ^r は $f(x)$ の根になることが, r の素因数の個数に関する帰納法で示される. 従つて $\Phi_n(x) | f(x)$ となるが, $f(x)$ は既約であるから $f(x) = c\Phi_n(x)$ $(c \in \mathbb{Q}^\times)$ となつて $\Phi_n(x)$ も既約である. □

系 32.6. 1 の n 乗根全体のなす群を $U_n \subset \overline{\mathbb{Q}}$ とおく. $\mathrm{Gal}\,(\mathbb{Q}(U_n)/\mathbb{Q})$ は $(\mathbb{Z}/n\mathbb{Z})^\times$ と同型である.

証明 27.4 の証明の前半で述べた通り $\mathrm{Gal}\,(\mathbb{Q}(U_n)/\mathbb{Q})$ は $(\mathbb{Z}/n\mathbb{Z})^\times$ の部分群と同型である. しかるに, $\mathbb{Q}(U_n)$ は $\Phi_n(x)$ の最小分解体であるから, 32.5 と 32.2 (1) により, $\mathrm{Gal}\,(\mathbb{Q}(U_n)/\mathbb{Q})$ の位数は $\varphi(n)$ であり, これは $(\mathbb{Z}/n\mathbb{Z})^\times$ の位数に他ならない. ゆゑに, この 2 群は同型でなければならない. □

問 32.7. ζ を 1 の原始 n 乗根とする. $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$ を示せ.

演 習 問 題

32.8. 任意の $n \in \mathbb{N}$ をとれ. このとき $p \equiv 1 \mod n$ なる素数 p が無数に存在することを次の方針で示せ. $\{p_1, p_2, \cdots, p_k\}$ をその様な素数の任意の集合とせよ (空集合でも良い). $a = np_1p_2\cdots p_k$ とおいて $\Phi_n(a)$ を考察する. 次の問に答へよ.

(1) $\Phi_n(a)$ は $1, -1$ ではないことを示せ.

(Hint : 複素数平面における絶対値と $\Phi_n(x)$ の定義.)

(2) $q > 1$ を $\Phi_n(a)$ の 1 つの素因子とせよ. このとき $q \equiv 1 \mod n$ であることを示せ.

(Hint : m を $a \in (\mathbb{Z}/q\mathbb{Z})^\times$ とみたときの位数とせよ. $\Phi_n(a) | a^n - 1$ であるから $a^n \equiv 1 \mod q$. ゆゑに $m | n$. ここで $m < n$ と仮定する. 一方 $a^m - 1 = \prod_{d|m} \Phi_d(a) \equiv 0 \mod q$ であるからある $d | m$ について $\Phi_d(a) \equiv 0 \mod q$. しかも $\Phi_n(a) \equiv 0 \mod q$ であるから, 結局 a は $x^n - 1 = \prod_{d|n} \Phi_d(a) \in \mathbb{F}_q[x]$ の重根である. 19.5(1) によれば $na^{n-1} \equiv 0 \mod q$ でなければならない. しかるに $q \nmid a$, $n | a$ より $q \nmid n$ でなければならないので, 矛盾が生ずる. よつて $m = n$. Fermat の小定理から $m = n$ は $q-1$ の約数でなければならず, $q - 1 \equiv 0 \mod n$.)

(3) 上の q は集合 $\{p_1, p_2, \cdots, p_k\}$ に含まれないことを示せ. (Hint : $q | \Phi_n(a) \equiv \pm 1 \mod a$.)

以上から, 限りなく $p \equiv 1 \mod n$ なる素数 p を見出すことができるから, その様な素数は無限に存在する.

第 3 章　付 録

§ 33.　集合と写像

定義 33.1. 集合 A に対し, 任意の元 a, b, $c \in A$ に関して, 次の 3 つの条件を満たす関係 $\leqslant$ が与へられてゐるとせよ:
O1. $a \leqq a$ （反射律）,
O2. $a \leqq b$, $b \leqq a \implies a = b$ （非対称律）,
O3. $a \leqq b$, $b \leqq c \implies a = c$ （推移律）.
このとき A は順序 $\leqslant$ が定義された順序集合, 或いは半順序集合 であるといはれる. 便宜上 $a \leqq b$ と $b \geqq a$ とも記す. さらに $a \leqq b$ で $a \neq b$ であることを $a < b$ と記す.
順序集合 A の部分集合 B は A に定められた順序によつて順序集合である.

定義 33.2. 順序集合 A において, 任意の 2 つの元 a, $b \in A$ に対して $a \leqq b$ または $b \leqq a$ が成り立つとき, A は全順序集合 であるといはれる.

定義 33.3. 極大元極小元最大元最小元

定義 33.4. 上界下界上に有界帰納的

定理 33.5. Zorn の補題

定義 33.6. 整列集合

例 33.7. $\mathbb{N}$, $(2\mathbb{N}+1) \cup (2\mathbb{N})$, $\{-\infty, 0\} \cup \mathbb{N}$

§ 34. 群の作用

定義 34.1. 群 G と集合 X, および写像 $X \times G \to X$, $(\alpha, a) \mapsto \alpha^a$ が与へられてゐて, 任意の a, $b \in G$, $\alpha \in X$ について
A1. $\alpha^1 = \alpha$,
A2. $\alpha^{ab} = (\alpha^b)^a$
の 2 つが共に成り立つとき, G は X に 作用 するといふ. さらに, 任意の $\alpha, \beta \in X$ に対し $\alpha^a = \beta$ となる元 $a \in G$ が存在するとき, G は X に 可移的 または 推移的 に作用するといふ.

例 34.2. 作用の例とさうでない例を記す.
(1) 加法を演算とする群 $G = \mathbb{Z}$ と $X = \mathbb{Z}$ について
$$\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (m, n) \mapsto m + n$$
は作用である. これは可移的である.
(2) 乗法を演算とする群 $G = \mathbb{Q}^\times$ と $X = \mathbb{Q}$ について
$$\mathbb{Q} \times \mathbb{Q}^\times \to \mathbb{Q}, \quad (x, y) \mapsto x + y$$
は作用ではない.
(3) Galois 拡大 L/K とその Galois 群 $\mathrm{Gal}(L/K)$ について,
$$L \times \mathrm{Gal}(L/K) \to L, \quad (\alpha, \sigma) \mapsto \alpha^\sigma$$
は作用である. これは可移的ではない.
(4) K を体とし, これの代数的閉包 $\overline{K}$ を 1 つ固定する. α の $\overline{K}$ 内の K 上の共役元のすべてからなる集合を $S = \{\alpha_1, \cdots, \alpha_n\}$ とし, $L = K(\alpha_1, \cdots, \alpha_n)$ とせよ. このとき
$$S \times \mathrm{Gal}(L/K) \to S, \quad (\alpha_i, \sigma) \mapsto {\alpha_i}^\sigma$$
は作用である. これは可移的である.

作用を利用すると, 新しく群を見出すこともできる. 例へば p 元体 $\mathbb{F}_p$ を $\mathbb{F}_p$ 自身の上の 1 次元 vector 空間として, vector $a \in \mathbb{F}_p$ による “a 移動”
$$\mathbb{F}_p \ \to \ \mathbb{F}_p, \quad v \mapsto v + a$$
および $b \in {\mathbb{F}_p}^\times$ による “b 倍”
$$\mathbb{F}_p \ \to \ \mathbb{F}_p, \quad v \mapsto bv$$
を考へると, これら写像の全体とそれらの合成は $\mathbb{F}_p$ と ${\mathbb{F}_p}^\times$ の元の組からなるある群を成してゐて, それが $\mathbb{F}_p$ に作用してゐると見做せる. 例へば $p = 5$ とすれば ${\mathbb{F}_5}^\times$ の原始根として 2 がとれる. いま 5 元集合 $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$ に関する対称群 S_5 を使へば, 元 (0 1 2 3 4) と (2 4 3 1) がそれぞれ “1 移動” と “2 倍” を表してゐて,
$$(0\ 1\ 2\ 3\ 4) \colon \mathbb{F}_p \ \to \ \mathbb{F}_p, \quad v \mapsto v + 1$$
$$(2\ 4\ 3\ 1) \colon \mathbb{F}_p \ \to \ \mathbb{F}_p, \quad v \mapsto 2v$$
であり, これらの生成する群 $H < S_5$ が見付かつた.

問 34.3. 上の群 H の元を全て書き上げよ. 位数はいくつか. また, H が 28.20 の $\mathrm{Gal}(K/\mathbb{Q})$ と同型であることを示せ.

§ 35. 整拡大

A が環 B の部分環であるとき, B は A の 拡大環 と呼ばれる.

定義 35.1. B を環 A の拡大環とし, $b \in B$ とする. b が A に係数を持つ monic 多項式の根であるとき, 即ち $f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \in A[x]$ が存在して $f(b) = 0$ となるとき, b は A 上整であるといはれる. もし B のあらゆる元が A 上整であれば, 環 B は環 A 上整であるといはれる.

定義 35.2. 整閉整域

例題 35.3. UFD は整閉整域であることを示せ.

解答 A を UFD とし, $K = \mathrm{frac}(A)$ とする. 任意の $a \in K$ をとる. a はある 1 次式 $px + q \in A[x]$ の根である. つまり $pa = -q$. A は UFD だから $p|q$ でなければならない. $q = -pc$, $c \in A$ と書けば, $a = c$ であつて a は $x - c$ の根である. □

命題 35.4. A を整閉整域, K を A の商体とし, $f(x) \in A[x]$ を monic な多項式とする. $f(x) \in K[x]$ とみて, $f(x)$ が $K[x]$ で既約であることと, $f(x)$ が $A[x]$ で既約であることは同値である.

□

索 引