代数学 I, II 講義ノート

2023 年 1 月 5 日

http://www.math.u-ryukyu.ac.jp/~suga/algebra/lecturenote.pdf

序

以下は, 2015 年度において, 琉球大学理学部数理科学科 3 年次対象の科目「代数学 I, II」の講義ノートを加筆したものである. Galois 理論を述べるのが目標で, 授業時間の都合上, Galois 理論と関係する内容が中心的な題材である.

2 年次対象の代数学序論 I, II, 代数学序論 I, II で講義されているであろう内容の証明で簡単なものは, 多くを省くか演習問題としてある.

注意

この文書は, まだ作成途中です. 間違っている内容が, 多数含まれている可能性があります. ダウンロードする際には, タイトル下の日付欄を見て下さい. 日付が以前のものと変わっていたら, 修正 (間違いの訂正) が行われています. 以下の更新履歴も常に確かめてください.

更新履歴

2016 年 4 月 14 日: 不完全なまま最初の公開.
2016 年 5 月 16 日: 加筆訂正をしたものの未だ不完全.
2016 年 6 月 2 日: 幾つかの訂正をした. 対称多項式の部分 (付録) を削除.
2016 年 6 月 30 日: 幾つかの訂正をした. 対称多項式の部分 (付録) を復活.
2016 年 10 月 6 日: 幾つかの訂正をした.
2016 年 10 月 20 日: 幾つかの加筆 (特に命題 4.4.2 の後の解説) をした.
以下単純なミスの訂正の更新履歴は書かないことにする.
2017 年 11 月 2 日: B 節を追加.
2018 年 2 月 1 日: H 節を追加.
2021 年 1 月 5 日: 注意 4.13.1 を追加.
2021 年 3 月: J 節を追加.
2021 年 9 月: 4.15 節が雑すぎたので, 加筆.
2922 年 12 月: 定理 4.10.1 の証明が間違っていたので訂正. ついでに系 4.9.1 を追加と注意 4.13.1 を加筆.

記号と言葉遣い

以下で用いる記号をまとめておく.

1. $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ はそれぞれ, 自然数, 整数, 有理数, 実数, 複素数全体のなす集合とする. 自然数には, 0 を含めないとする.
2. 集合 A に対して, $|A|$ を A の濃度 (有限集合の場合は, 個数) とする. 集合の濃度については, 有限が無限かは問題にするが, 無限集合の濃度を問題にすることはない.
3. 共通部分を持たない和集合 (disjoint union) を記号 $\sqcup$ を用いて表す. すなわち, $A = B \sqcup C$ は, $A = B \cup C$ かつ $B \cap C = \emptyset$ の意味で用いる.
4. 集合 A から A への恒等写像を id_A と書く. すなわち, $\mathrm{id}_A : A \to A$, $\mathrm{id}(a) = a$, $a \in A$ である.
5. 集合 A, B と写像 $f : A \to B$ に対して, $f(A) = \mathrm{Im}(f) = \{f(x) \mid x \in A\} \subset B$ を f の像という. また, B の部分集合 C に対して, C の原像を $f^{-1}(C) = \{x \in A \,|f(x) \in C\}$ とする. 特に C が 1 点集合 $\{y\}$ のときには, $f^{-1}(\{y\}) = f^{-1}(y)$ と略記する. 同様に, 1 点集合の場合, 集合と元を区別しないで書くことは多くある.
6. A, B を集合とし, $f : A \to B$ を写像とする. $\mathrm{Im}(f) = B$ であるとき, f を全射, あるいは上への写像 (surjection) という. f が 1 対 1 の写像であるとき, f は単射であるとか, 中への写像 (injection) という. 特に, $A \subset B$ であるとき, A の元を B の元であると見る自然な単射がある. この写像は, 埋め込み (embedding) あるいは包含写像 (inclusion) という. 逆に, $f : A \to B$ が単射であるとき, $f(A) \subset B$ を A と同一視して, B の部分集合であると見ることもある. このときにも, f を埋め込みという. f が全射かつ単射であるとき, f は全単射 (bijection) であるという.
7. A, B を集合, $f : A \to B$ を写像とする. $C \subset A$ に対して f の C への制限で決まる写像を, $f_{|C} : C \to B$ と書く.
8. A を集合とし, $\sim$ を A で定義された同値関係とする. $a \in A$ に対して, a と同値な元の集合を

   $$\overline{a} = \{x \in A \,|\, x \sim a\}$$

   で表すことにする. a を $\overline{a}$ の代表元 (representative) という. $\pi : A \to A/\!\sim$, $\pi(a) = \overline{a}$ を同値関係から決まる自然な射影 (projection) という. $A/\!\sim = \{\overline{a}_i\}$ であるとき, $\{a_i\}$ を $A/\!\sim$ の完全代表系という. 同値類を扱う際によく現れる「well–defined」という言葉づかいの意味は, 理解していると想定する.
9. 整数 a, b に対して, $a \mid b$ は, a は b の約数 (b は a の倍数) を意味する. そうでないときは, $a \nmid b$ と書く. 0 はすべての整数の倍数であり, 0 でないどの整数の約数でもない. (a, b) は, a, b の最大公約数とする.
10. (漢字圏以外の) 外国人の姓は基本的にアルファベット表記とした.

目次

1　代数学について

代数学は,「方程式を解く」ことを動機として形成され, 発展してきた. 中学, 高校時代に学習した,「消去法で連立 1 次方程式を解く」,「平方完成を用いて 2 次方程式の根の公式を求める」というのは, 代数学における最も根本的な考え方である.

この講義では, 現在の代数学の発展の動機となった, 高次方程式の根についての性質を記述する Galois(ガロア[*1]) 理論の解説を目標とする. Galois 理論を講義するのは多くの予備知識を必要とするため, 前期 (代数学 I) は, Galois 理論を述べるために必要な群論と可換環論の基礎を講義し, Galois 理論とその応用 (代数的可解性の判定や, 作図問題) は後期 (代数学 II) で講義する.

1.1　3 次方程式を解いてみる

ここでは導入として, 3 次方程式の代数的な解法を述べる. まず,「代数的に解く」という言葉の意味をはっきりさせておく必要がある.

この講義全般で考える方程式は, 代数方程式と呼ばれるもので,

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \tag{1.1}$$

としたときに, $f(\theta) = 0$ となるような数 θ を見出すことを問題にする. すなわち, 多項式 $f(x)$ の零点を求めよ, という問題である. このとき θ は, 方程式 $f(x) = 0$, あるいは多項式 $f(x)$ の根 (root) という. 中学・高校では解という用語が使われているが, 根の方がより正しい言葉である. $a_n \neq 0$ のとき, (1.1) は n 次方程式と呼ばれるのは, よく知られていることである.

さて, これを「代数的に解く」とは, 次のように定義される.

> n 次方程式の代数的な解法とは, 係数の加減乗除の 4 則演算とベキ乗根をとるという操作を有限回用いる事で, その根を求める事である.

2 次方程式の根の公式は, 確かに上の条件を満たしている. 2 次方程式の解法は, 古代バビロニアにまでさかのぼることができるものらしい. しかし, 3 次方程式の代数的な解法は, Cardano(カルダノ) の著書 Ars magna de Rebus Algebraicis(1545 年, 偉大なる代数の技法という意味のラテン語) において初めて発表された (解法の本当の発見者は, Cardano ではないらしい) 比較的新しい数学である. 同じ頃に 4 次方程式の代数的な解法も発見されている. これらが発見された 16 世紀中頃においては, 現在のように文字式の記法は発明されておらず, Cardano の著書も, 図形的, 幾何的な記法を用いていた. 現在のような文字式の記法は, 16 世紀後半から 17 世紀にかけて, Viète(ヴィエト) が作ったとされている.

5 次以上の方程式については, その後いろいろな研究がされたが, 1826 年に Abel(アーベル) が, 5 次方程式は一般には代数的な解法がないことの証明を発表した. 同じ頃 Galois は, 代数的な解法があるような方程式を特徴付けることに成功した. それが, この講義の主題の Galois 理論である. その特徴付けは, 群論の言葉でなされており, 群論という数学の本格的な始まりでもあった. なお, Galois の研究は Galois の生存中には発表されておらず, 死後 (Galois は 21 歳のときに決闘で負った傷により亡くなった) に遺稿を Liouville(リウビル) や Dedekind(デデキント) がその内容を分析した (1850 年頃).

[*1] 本来はガロワと表記すべきだが, ガロアと表記されることの方が多い

まず素朴な疑問として, 代数方程式に根はあるのかという問題がある. これについては, 結局のところ, 数の体系をどう捉えるかという問題になる. この方向での最初の結果は, Gauss による次の結果である.

定理 1.1.1（Gauss, 1799, 代数学の基本定理, あるいは方程式論の基本定理） $f(x)$ を複素数係数の多項式とするとき, $f(\alpha)=0$ となる $\alpha\in\mathbb{C}$ が必ず存在する.

上の定理は, 実際には「実数の連続性」に基づくもので, 代数学というよりむしろ解析学や位相の問題である. Gauss の時代には, 実数の連続性が正確に把握されていなかったため, Gauss の証明自身, その部分にはごまかしがある. 何通りかの証明が可能であるが,「複素関数論」を用いる証明が, もっとも簡明なようである. 後期の講義において, 時間があれば, 実数の連続性を用いる以外は「代数的」な証明を与える (D 節).

n 次方程式の根は, もしすべて見つかれば, 重複を込めると n 個であることに注意する. 実際, θ を $f(x)$ の根とすると, 因数定理より, $f(x)=(x-\theta)g(x)$ と $f(x)$ は因数分解され, $g(x)$ は $n-1$ 次式なので, 帰納法により証明される. また, 多項式の「素因数分解の一意性」から, 根の集合や重複度は, 方程式から一意的に定まることにも注意しておく.

次に,「根と係数の関係」も次数に関係なく一般的に成立する. すなわち, (1.1) の n 個の根を, (重複も込めて) $\theta_1,\dots,\theta_n$ とすると,

$$f(x)=a_n(x-\theta_1)(x-\theta_2)\cdots(x-\theta_n)$$

と $f(x)$ は因数分解される. 右辺を展開して, x の各次数の係数を比較することにより, 次を得る ($a_n\neq 0$ とする. 下の式の第 i 行目は, 上の式の x^{n-i} の両辺の係数を比較して得られる.)[*2].

$$\begin{cases} -\dfrac{a_{n-1}}{a_n}=\displaystyle\sum_{i=1}^{n}\theta_i \\ \dfrac{a_{n-2}}{a_n}=\displaystyle\sum_{1\leqq i<j\leqq n}\theta_i\theta_j \\ -\dfrac{a_{n-3}}{a_n}=\displaystyle\sum_{1\leqq i<j<k\leqq n}\theta_i\theta_j\theta_k \\ \quad\vdots \\ (-1)^n\dfrac{a_0}{a_n}=\theta_1\cdots\theta_n \end{cases} \tag{1.2}$$

これらの式の右辺は, $\theta_1,\dots,\theta_n$ の**基本対称式**と呼ばれるものである.

さて, 表題にあげた, 3 次方程式の代数的解法を述べる. ここで述べるのは, 本質的には Cardano が発表したものと同じであるが, 少しは Galois 理論を意識した解法である. 考える方程式は,

$$x^3+ax^2+bx+c=0$$

とし, 最高次の係数は 1 として良いことは簡単にわかる (両辺を最高次の係数で割り算した結果を, 改めて方程式とすれば良い). さらに, 2 次方程式と同様に「立方完成」を考えてみると,

$$x^3+ax^2+bx+c=\left(x+\frac{a}{3}\right)^3+\left(b-\frac{a^2}{3}\right)\left(x+\frac{a}{3}\right)+c-\frac{ab}{3}+\frac{2a^3}{27}=0$$

[*2] 現行の高校の教科書には, 根の公式を利用した 2 次方程式の根と係数の関係式が書かれている. 実際には, 根と係数の関係式は, 因数分解を利用すれば一般的に求まるものであり, 根の公式は不要である.

と元の方程式は変形される．ここで, $x+\dfrac{a}{3}$ を改めて x とおき, $p=b-\dfrac{a^2}{3}$, $q=c-\dfrac{ab}{3}+\dfrac{2a^3}{27}$ とおくと, 元の方程式は,

$$x^3+px+q=0$$

という形までは, 簡易化できる．この方程式の根を $\theta_1,\theta_2,\theta_3$ とすると, 根と係数の関係は, 次になる．

$$\begin{cases}\theta_1+\theta_2+\theta_3=0\\ \theta_1\theta_2+\theta_2\theta_3+\theta_3\theta_1=p\\ \theta_1\theta_2\theta_3=-q\end{cases}$$

ここで, 1 の複素 3 乗根 ω を導入する．$x^3-1=(x-1)(x^2+x+1)$ なので, ω は $\omega^2+\omega+1=0$ を満たす．2 次方程式の根の公式より, $\omega=\dfrac{-1\pm\sqrt{-3}}{2}$ となるが, $\pm$ はどちらを選んでも結論は同じことが, 後にわかる．注意すべきは, 一方を ω とすると, もうひとつは ω^2 となることである．また, $\omega+\omega^2=-1$ であることにも注意する．ω と上の 3 次方程式の根 $\theta_1,\theta_2,\theta_3$ から決まる次の数を考える (Lagrange(ラグランジュ) の分解式)．

$$\alpha=\theta_1+\omega\theta_2+\omega^2\theta_3$$
$$\beta=\theta_1+\omega^2\theta_2+\omega\theta_3$$

このとき, $\alpha\beta$ および, $\alpha^3+\beta^3$ は, 上の根と係数の関係式を用いて p,q の式で表されることがわかる．実際,

$$\begin{aligned}\alpha\beta&=(\theta_1+\omega\theta_2+\omega^2\theta_3)(\theta_1+\omega^2\theta_2+\omega\theta_3)=\theta_1^2+\theta_2^2+\theta_3^2+(\omega+\omega^2)(\theta_1\theta_2+\theta_2\theta_3+\theta_3\theta_1)\\&=(\theta_1+\theta_2+\theta_3)^2-3(\theta_1\theta_2+\theta_2\theta_3+\theta_3\theta_1)=-3p\end{aligned}$$

は直ちにわかる．さらに,

$$\begin{aligned}\alpha^3&=(\theta_1+\omega\theta_2+\omega^2\theta_3)(\theta_1+\omega\theta_2+\omega^2\theta_3)(\theta_1+\omega\theta_2+\omega^2\theta_3)\\&=\theta_1^3+\theta_2^3+\theta_3^3+3\omega\theta_1^2\theta_2+3\omega^2\theta_1\theta_2^2+3\omega\theta_2^2\theta_3+3\omega^2\theta_2\theta_3^2+3\omega^2\theta_1^2\theta_3+3\omega\theta_1\theta_3^2+6\theta_1\theta_2\theta_3\\\beta^3&=\theta_1^3+\theta_2^3+\theta_3^3+3\omega\theta_1^2\theta_3+3\omega^2\theta_1\theta_3^2+3\omega\theta_3^2\theta_2+3\omega^2\theta_3\theta_2^2+3\omega^2\theta_1^2\theta_2+3\omega\theta_1\theta_2^2+6\theta_1\theta_2\theta_3\end{aligned}$$

となる．上の計算では, β は α で, θ_2,θ_3 を入れ替えた式であることを利用している．ここで,

$$\omega^2+\omega=-1 \tag{1.3}$$
$$\theta_1^3+\theta_2^3+\theta_3^3-3\theta_1\theta_2\theta_3=(\theta_1+\theta_2+\theta_3)(\theta_1^2+\theta_2^2+\theta_3^2-\theta_1\theta_2-\theta_2\theta_3-\theta_3\theta_1)=0 \tag{1.4}$$

を利用すると,

$$\begin{aligned}\alpha^3+\beta^3&=-3(\theta_1^2\theta_2+\theta_1\theta_2^2+\theta_2^2\theta_3+\theta_2\theta_3^2+\theta_3\theta_1^2+\theta_1\theta_3^2)+18\theta_1\theta_2\theta_3\\&=-3\{(\theta_1+\theta_2+\theta_3)(\theta_1\theta_2+\theta_2\theta_3+\theta_3\theta_1)-3\theta_1\theta_2\theta_3\}+18\theta_1\theta_2\theta_3\\&=27\theta_1\theta_2\theta_3=-27q\end{aligned}$$

を得る．従って, $\alpha^3\beta^3=-27p^3$, $\alpha^3+\beta^3=-27q$ が成立するから, α^3, β^3 は, X の 2 次方程式,

$$X^2+27qX-27p^3=0$$

の根である．よって例えば,

$$\alpha^3=\frac{-27q+\sqrt{(27q)^2+4\cdot27p^3}}{2}=-3^3\left(\frac{q}{2}-\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}\right)$$
$$\beta^3=-3^3\left(\frac{q}{2}+\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}\right)$$

とできる. もともと,

$$\begin{cases} \theta_1+\theta_2+\theta_3=0 \\ \theta_1+\omega\theta_2+\omega^2\theta_3=\alpha \\ \theta_1+\omega^2\theta_2+\omega\theta_3=\beta \end{cases}$$

という関係式であったので, これを逆に解いて,

$$\begin{cases} \theta_1=\frac{1}{3}(\alpha+\beta) \\ \theta_2=\frac{1}{3}(\omega^2\alpha+\omega\beta) \\ \theta_3=\frac{1}{3}(\omega\alpha+\omega^2\beta) \end{cases}$$

を得る. 従って, 求める根は次である.

$$\theta_1=\left(-\frac{q}{2}+\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}\right)^{\frac{1}{3}}+\left(-\frac{q}{2}-\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}\right)^{\frac{1}{3}}$$

$$\theta_2=\omega^2\left(-\frac{q}{2}+\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}\right)^{\frac{1}{3}}+\omega\left(-\frac{q}{2}-\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}\right)^{\frac{1}{3}}$$

$$\theta_3=\omega\left(-\frac{q}{2}+\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}\right)^{\frac{1}{3}}+\omega^2\left(-\frac{q}{2}-\sqrt{\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3}\right)^{\frac{1}{3}}$$

上で, ω, α, β の選び方を変えることもできるが, それは, 根の公式において, θ_2,θ_3 の入れ替えに対応する. また, 3 乗根も 3 通りの選び方が常にある. $\sqrt[3]{a}$ を a の 3 乗根の 1 つとすると, $\sqrt[3]{a}\omega$, $\sqrt[3]{a}\omega^2$ も a の 3 乗根となる. しかし, このように 3 乗根の取り方を変えたとしても, 根 $\theta_1,\theta_2,\theta_3$ の置換が生じるだけであることが容易に分かる ($\alpha\beta=-3p$ という関係式があることに注意する). 従って, 途中の方程式の根の取り方によらず, 上の式は, 元の 3 次方程式の根の集合を一意的に与えることがわかる.

上のような解法が可能な理由は何か? あるいは, 5 次以上の方程式で, 何がダメになるのかを解説するのが,「代数学 I, II」の目標である. また, このような現象の背景に, 根の置換 (上で述べたことでいうと, 解法の途中で出てきた方程式の根 ω, α, β や, 3 乗根の選び方) に対する群論的 (不変式論的) な現象を見抜いたのが, Galois である.

> 上の解法が上手くいく理由を, 根の置換を用いて簡単に解説しておく. 3 次の対称群 S_3 により, 根 $\theta_1,\theta_2,\theta_3$ を置換することを考える. このとき, 互換 $(1,2)$(θ_1 と θ_2 の入れ替え) によって, $\alpha\mapsto\omega\beta$, $\beta\mapsto\omega^2\alpha$ となることがわかる. また, 巡回置換 $(1,2,3)$ を使うと, $\alpha\mapsto\omega\alpha$, $\beta\mapsto\omega^2\beta$ となることがわかる. S_3 は, $(1,2)$, $(1,2,3)$ から生成されるから, $\alpha\beta$, $\alpha^3+\beta^3$ は根の任意の置換によって不変であることがわかる. これら 2 つの数が, 元の 3 次方程式の係数で書くことができたのは, この「不変性」が理由である. 実際次の定理が成立する (E, 定理 E.1).
>
> **定理 1.1.2** $f(x_1,\dots,x_n)$ を n 変数の多項式とし, 任意の変数の置換で不変であるとする. すなわち, 任意の置換 σ に対して, $f(x_{\sigma(1)},\dots,x_{\sigma(n)})=f(x_1,\dots,x_n)$. このとき, f は基本対称式の多項式となる.
>
> 上の定理と,「根と係数の関係式」より, $\alpha^3+\beta^3$, $\alpha\beta$ が元の 3 次方程式の係数の多項式となったのである.

1.2 基本的な代数系の定義

群・環・体という言葉を, 代数学序論等で 1 度は聞いたことがあると仮定している. ここでも, 改めてその定義を書くが, それは, この講義で一般的に用いる記号や, 言葉遣いを与えることも兼ねている.

定義 1.2.1（群） 集合 G が群であるとは, つぎの性質を持つ 2 項演算 (積) $G \times G \to G$, $(x, y) \mapsto xy$ が定義されていることをいう.

1. $(xy)z = x(yz),\ x, y, z \in G$ (結合律)
2. $e \in G$ が存在して, $ex = xe = x$ が全ての $x \in G$ について成立する (単位元の存在).
3. 任意の $x \in G$ に対して, $x^{-1} \in G$ が存在して, $xx^{-1} = x^{-1}x = e$ が成立する (逆元の存在).

公理の 1. の結合律から, 3 個以上の積の結果は計算の順序によらない. よって, 群 G の元 $x_1, \ldots, x_n$ に対して, これらを順に積を取った結果は, 特別な場合を除いて, 括弧を使わずに $x_1 \cdots x_n$ と書く.

任意の $x, y \in G$ に対して, $xy = yx$ が成立するとき, G を可換群あるいは Abel 群という. あるいは, G は可換であるとか Abelian であるともいう. 可換群に対しては, 演算を $+$, 単位元を 0, x の逆元を $-x$ と書き, 加法群あるいは加群ということもある. これらの使い分けは前後の文脈による. また, 数や行列などの集合がもともと定義されている積で群をなすとき, 単位元は, その文脈に応じて 1 と書いたり, E(単位行列) と書いたりもする.

例 1.2.1

1. 単位元のみからなる集合 $\{e\}$ は群になる. この群を**単位群**あるいは**自明な群**という.
2. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/n\mathbb{Z}$ $(n \in \mathbb{N})$ を群と見るときは, 加法を演算とした群である.
3. $\mathbb{Q}^\times, \mathbb{R}^\times, \mathbb{C}^\times$ は, それぞれの集合の 0 以外の元全体を表し, 乗法に関して可換群になる. 可換な群であるが, これらの群の演算を加法記号で書くことはない. 正の実数全体からなる集合 $\mathbb{R}_+^\times$, 正の有理数全体の集合 $\mathbb{Q}_+^\times$ も乗法に関して群をなす.
4. $[n] = \{1, 2, \ldots, n\}$ として, $S_n = \{\sigma : [n] \to [n] \mid \sigma\text{は全単射 }\}$ とおく. S_n に写像の合成で積を導入すると, 群になる. 単位元は恒等写像で, 逆元は逆写像である. S_n を n 次の対称群という. S_n は, $[n]$ の置換全体と自然に同一視される. $\sigma \in S_n$ を, $\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$ のように 2 行で書くことが多い. S_n の元 σ に対して, σ の符号を $\mathrm{sgn}(\sigma)$ で表すことにする.
   より一般に, X を集合とするとき, $S(X) = \{\sigma : X \to X \mid \sigma\text{は全単射 }\}$ は, 写像の合成で群になる. これを X の置換群という.
5. $A_n = \{\sigma \in S_n \mid \mathrm{sgn}(\sigma) = 1\}$, すなわち, 偶置換全体のなす集合は, S_n の中の演算で閉じている. これを n 次交代群という.

他の分野の数学と同様, 代数学においても, さまざまな集合での演算の定義を比較することによって, その構造を調べていく. 代数系においては, その演算を保つような写像が重要になる.

定義 1.2.2 G, G' を群とし, $f : G \to G'$ を写像とする. f が準同型写像とは, $f(gh) = f(g)f(h)$ が, すべての $g, h \in G$ について成立することを言う. さらに f が全単射であるとき, f は同型写像という. 同型写像 $f : G \to G'$ が存在するとき, G と G' は同型であるといい, $G \cong G'$ と書く. 同型は同値関係になる.

例 1.2.2　1. n 次対称群の (置換の) 符号 sgn は, 群の準同型写像 $\mathrm{sgn} : S_n \to \{\pm 1\}$ を定める. ここで $\{\pm 1\}$ は, 通常の積で演算を入れた 2 個の元からなる群である.

2. 0 でない複素数の乗法群に対して, 絶対値を取る写像, $\mathbb{C}^\times \to \mathbb{R}_+^\times,\ z \mapsto |z|$ は群の準同型写像である.
3. 指数関数 $\exp : \mathbb{R} \to \mathbb{R}_+^\times,\ x \mapsto \exp(x) = e^x$ は, 加法群 $\mathbb{R}$ から, 正の実数全体のなす乗法群 $\mathbb{R}_+^\times$ への同型写像である.
4. G を群とし, $a \in G$ とする. $I_a : G \to G$ を $I_a(x) = axa^{-1}$ とおくと, I_a は G の同型写像になる. I_a の形の同型写像 $G \to G$ を内部自己同型写像という. G に対して, $\mathrm{Aut}(G) = \{f : G \to G \mid f \text{ は同型写像 }\}$ とおく. $\mathrm{Aut}(G)$ の元を G の自己同型写像という. $\mathrm{Aut}(G)$ は写像の合成を積と定義すると群になり (例 1.2.1, 3. の $S(G)$ の部分群), G の自己同型群という.

問 1.2.1　1. $f : G \to G'$ を群の準同型写像とするとき, $f(e) = e$, $f(x^{-1}) = f(x)^{-1}$ を示せ.

2. 上の例の I_a が G の同型写像になることを示せ.

(有限) 群 G に対して, $|G|$ を G の位数 (order) という. $|\mathbb{Z}/n\mathbb{Z}| = n$, $|S_n| = n!$, $|A_n| = \dfrac{n!}{2}$ である. $|G|$ が有限であるとき有限群, そうでないとき無限群という. この講義では, 無限群の濃度を問題にすることはない.

次に環の定義を与えるが, 代数学の分野で通常現れる, 乗法の単位元の存在を仮定したものとする.

定義 1.2.3 (環)　集合 R が (単位元を持つ) 環であるとは, R に加法 $R \times R \to R,\ (a, b) \mapsto a + b$ と乗法 $R \times R \to R,\ (a, b) \mapsto ab$ が定義されており, 次を満たすことを言う.

1. R は加法において, 可換群をなす. 加法に関する単位元は 0 と記す.
2. $(ab)c = a(bc),\ a, b, c \in R.$ すなわち, R の乗法は結合律を満たす.
3. $1 \in R$ が存在して, $a1 = 1a = a,\ \forall a \in R.$ すなわち, 乗法における単位元が存在する.
4. $a(b + c) = ab + ac,\ (a + b)c = ac + bc,\ \forall a, b, c \in R$ (分配律).

R の乗法が可換であるとき, R を可換環という.

注意 1.2.1　環に対して, 単位元の存在を仮定しないこともある (解析学系で出てくる) が, 下の例 1.2.3 以外は, この講義では扱わない.

例 1.2.3 (乗法の単位元の存在以外は, 可換環の公理を満たす代数系の例)

$$C_0(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{C} \mid f \text{ は連続かつ } \mathrm{supp}(f) \text{ はコンパクト }\}$$

とおく. ここで $\mathbb{R}$ 上の関数 f に対して, $\mathrm{supp}(f) = \overline{\{x \in \mathbb{R} \mid f(x) \neq 0\}}$ (上付きのバーは, 閉包の意味) で, f の台 (support) と呼ばれる集合である. $C_0(\mathbb{R})$ は通常の関数の和と積で積の単位元の存在以外の可換環の公理を満たす. 積の単位元は, 存在するなら 1 という定数関数であるが, この関数の台はコンパクトではない.

$C_0(\mathbb{R})$ には, 合成績 (convolution) と呼ばれる積が入り, その積を用いても, 単位元のない可換環になる (単位元を無理に入れようとすると, Dirac(ディラック) の δ 関数と呼ばれる「超関数」が必要になる). 合成績 (合成積の演算記号は $*$ が通常用いられる) は, 次で定義される.

$$(f * g)(x) = \int_{-\infty}^{\infty} f(x - y)g(y)dy$$

例 1.2.4　1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/n\mathbb{Z}\,(n \in \mathbb{N})$ は通常の積と和によって可換環となる.

2. $\{0\}$ は $(1 = 0$ と見て$)$ 環とみなすことができる. これを零環という. これ以外の環では, $0 \neq 1$ となる.

3. R を環とするとき, $R[X] = \left\{ \sum_{i=0}^{n} a_i X^i \mid a_i \in R \right\}$ R 上の 1 変数多項式環という. 積は, $X^i X^j = X^{i+j}$, $aX = Xa$, $(a \in R)$ という規則で入れる. R が可換環なら, $R[X]$ も可換環である. X は不定元 (indeterminate) という.

4. R を環, $X_1, \ldots, X_l$ を l 個の不定元とするとき, n 変数多項式環 $R[X_1, \ldots, X_l]$ が同様に定義される. $R[X_1, \ldots, X_{l-1}][X_l] = R[X_1, \ldots, X_l]$ と, l について帰納的に定義しても良い.

5. R を可換環とするとき, $M_n(R) = \{$ 成分が R の元である $n \times n$ 行列 $\}$ とおく. 通常の行列の積と和で環になる. $n \geqq 2$ であるとき, これは非可換な環になる.

問 1.2.2　1. 環において, $a0 = 0a = 0$, $(-1)a = -a$, $(-1)(-1) = 1$ を証明せよ.

2. 零環以外では, $0 \neq 1$ が成立することを示せ.

3. 例 1.2.3 で, 合成積が定義できること, すなわち, $f, g \in C_0(\mathbb{R})$ なら, $f * g \in C_0(\mathbb{R})$ となること, および, これが可換な演算であることを示せ.

R を環とするとき, 積に関して可逆な元全体の集合を,

$$R^\times = \{x \in R \mid y \in R \text{ が存在して, } xy = yx = 1\}$$

とおく, $R^\times$ の元を単元あるいは可逆元という. $R^\times$ は積に対して群をなすが, これを R の単元群 (unit group) という. 下にあるように, これはさまざまな群の例を与える.

例 1.2.5　1. $\mathbb{Z}^\times = \{\pm 1\}$

2. $n \in \mathbb{N}$ とする. $(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \mid (a, n) = 1\}$ である. ここで, 整数 a, b に対して, (a, b) は, a, b の最大公約数を意味している. $|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$ を Euler(オイラー) の関数という. n の素因数分解を $n = p_1^{r_1} \cdots p_k^{r_k}$ $(r_i \geqq 1$ かつ, $i \neq j$ なら $p_i \neq p_j)$ とすると, 次が成立する.

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)$$

3. R を可換環としたとき, $M_n(R)^\times = \{A \in M_n(R) \mid \det A \in R^\times\}$ である. この集合を $GL_n(R)$ と書き, R 上の一般線形群 (general linear group) という.

問 1.2.3　1. $(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \mid (a, n) = 1\}$ を示せ. (問 2.1.2, 2. も見よ.)

2. 上の例の 2. の $\varphi(n)$ の公式を n と互いに素な数を「数え上げること」により証明せよ. (Chinese Remainder Theorem を用いた証明もある. 例 3.3.1)

3. 上の例の 3. の $M_n(R)^\times = \{A \in M_n(R) \mid \det A \in R^\times\}$ を証明せよ.

環の準同型写像についても, 群と同様に定義される. ただし, 群のときと違い, 環の場合 $f(1) = 1$ という性質は,「演算を保つ」ということから導くことができない. したがって, この性質を定義に加えておく.

定義 1.2.4　R, R' を環とし, $f : R \to R'$ を写像とする. 次の性質を持つとき, f は環の準同型写像という.

1. $f(a+b) = f(a) + f(b), \qquad a, b \in R$
2. $f(ab) = f(a)f(b), \qquad a, b \in R$
3. $f(1) = 1$

さらに f が全単射であるとき, f は同型写像という. 同型写像 $f : R \to R'$ が存在するとき, R と R' は同型であるといい, $R \cong R'$ と書く.

注意 1.2.2　上の定義では, 零写像, すなわち $f(x) = 0$, $\forall x \in R$ は, $R' = \{0\}$ のときだけ準同型写像になる.

問 1.2.4　R, R' を (単位元を持つ) 環とする. $f : R \to R'$, $(f \neq 0)$ で, 上の定義の 1., 2. を満たすが, 3. を満たさない写像の例を作れ.

定義 1.2.5**（体）**　集合 K が体であるとは, K は環であって $K^\times = K \setminus \{0\}$ が成立すること, すなわち, 0 以外の元はすべて単元であるこという.

体の定義においても, 積の可換性をここでは仮定していない. 通常は, 可換体を単に体と言い, 非可換な体は, 斜体 (skew field, 略して sfield) という.

例 1.2.6　1. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ は通常の演算で体になる.
2. p を素数とするとき, $\mathbb{Z}/p\mathbb{Z}$ は体になる (p 個の元からなる体).
3. $\mathbb{H} = \{a + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k} \mid a, b, c, d \in \mathbb{R}\}$ として, $\boldsymbol{i}^2 = \boldsymbol{j}^2 = \boldsymbol{k}^2 = -1$, $\boldsymbol{ij} = -\boldsymbol{ji} = \boldsymbol{k}$, $\boldsymbol{jk} = -\boldsymbol{kj} = \boldsymbol{i}$, $\boldsymbol{ki} = -\boldsymbol{ik} = \boldsymbol{j}$ と定義して, 結合律を満たすようにすると, これは非可換な体になる. これを Hamilton の 4 元数体という.

問 1.2.5　$\mathbb{H}$ が斜体になること, すなわち, 0 以外の元は積において単元であることを示せ.

体は環であるので, 体の準同型写像の定義は, 環のものと同じである.

以下では, 環は常に単位元を持つものとし, 特に断らなければ非可換であることを許容する. 可換な環に話を限るときには,「可換環」という言葉を用いる. 体に関しては, 何も断らなければ可換体を意味し, 非可換な体は「斜体」ということにする.

以上が, この講義で扱う代数系である. これ以外にも, Lie(リー) 代数や Jordan 代数 (数学の人はジョルダン代数といい, 物理の人はヨルダン代数という) などの重要な代数系はある. (Lie 代数については, 日本語でも幾つかの良い参考書があるが, Jordan 代数については, 日本語の参考書はないと思われる.)

1.3　Zorn の補題

この後の議論で, 証明において Zorn(ツォルン) の補題が何度か必要となるので, それについて述べておく. これは, 選択公理, 整列可能性定理と同値な命題であることが知られており, 現代の数学では,「公理」として仮定されるのが普通である.

空でない順序集合 A は, その空でない全順序部分集合が常に上界を持つとき, 帰納的順序集合という.

定理 1.3.1**（Zorn の補題）**　帰納的順序集合には極大元が存在する.

2 (有限) 群論

ここでは, 有限群の性質を中心に述べる. 代数学序論 I, II, 代数学序論演習 I, II で学習したであろう内容の多くを問にしてあるが, 復習の意味で解いて欲しい. Galois 理論では, 代数方程式が代数的に解けるか否かは, その方程式の Galois 群の性質に帰着される.

2.1 部分群と剰余類

G を群とし, A, B を G の部分集合とするとき, G の部分集合 A^{-1}, AB を

$$A^{-1} = \{a^{-1} \mid a \in A\} \subset G$$
$$AB = \{ab \mid a \in A,\ b \in B\} \subset G$$

で定義する. また, 下段の記述において, 例えば A が 1 元集合 $\{a\}$ であるとき, $\{a\}B = aB$ と略記する. B についても同様である. 3 つ以上の集合の積で書かれる部分集合も同様に定義され, 1 元集合に対する略記法も同様とする.

定義 2.1.1 群 G の部分集合 H が, G の演算 (積と逆元をとる) で閉じているとき, H を G の部分群という. 上の記号を用いると, $HH = H$, $H^{-1} = H$ が成立する集合のことである.

例 2.1.1

1. G 自身および $\{e\}$ を自明な部分群という.
2. n 次交代群, A_n は n 次対称群 S_n の部分群である.
3. H を $\mathbb{Z}$ の加法群の部分群とする. このとき, $m \in \mathbb{N} \cup \{0\}$ が存在して, $H = m\mathbb{Z} = \{\, ma \mid a \in \mathbb{Z}\}$ となる (命題 2.1.1, 1.).
4. R を可換環とする. $SL_n(R) = \{A \in GL_n(R) \mid \det A = 1\}$ とすると, $\det AB = \det A \det B$ より, $GL_n(R)$ の部分群となる. これを R 上の特殊線形群 (special linear group) という.
5. G を群とするとき, $Z(G) = \{x \in G \mid xy = yx,\ \forall y \in G\}$ とおく, $Z(G)$ は G の部分群になることは容易に分かる. $Z(G)$ を G の中心という.

問 2.1.1

1. 上の 3., 5. を証明せよ.
2. $G \supset H, K$ を G の 2 つの部分群とすると, $H \cap K$ も G の部分群になることを示せ.
3. 群 G の部分集合 H が部分群になるための必要十分条件は, 任意の $x,\ y \in H$ に対して, $xy^{-1} \in H$ が成立することであることを示せ.

$S \subset G$ の部分集合とする.

$$< S >= \bigcap_{\substack{H \text{ は } G \text{ の部分群,} \\ S \subset H}} H$$

とおく. 部分群の共通部分は部分群だから (問 2.1.1, 2), 定義より, $< S >$ は集合 S を含む最小の部分群になる. これを S から生成された部分群という. より具体的に書くと,

$$< S >= \{\, a_1^{k_1} \cdots a_l^{k_l} \mid a_i \in S,\ k_i \in \mathbb{Z}\}$$

となる. 特に, $< S >= G$ となる時, S は G を生成すると言い, S を G の生成元の集合, あるいは G の生成系

という. S が有限集合 $\{a_1, \ldots, a_n\}$ であるとき, $< S >=< a_1, \ldots, a_n >$ と略記する.

ただ 1 つの元から生成される群を, 巡回群という. 次の命題は, 代数学序論で学習していると思う.

命題 2.1.1　1. 巡回群の部分群は巡回群である.

2. C を巡回群とする. $|C| = \infty$ なら C は $\mathbb{Z}$ と同型になり, $|C| = n < \infty$ なら, C は $\mathbb{Z}/n\mathbb{Z}$ と同型である.

問 2.1.2　1. 上の命題を証明せよ

2. $m, n \in \mathbb{N}$ とし, $d = (m, n)$(m, n の最大公約数) とするとき, 上の命題を利用して,

$$\{ma + nb \mid a, b \in \mathbb{Z}\} = d\mathbb{Z}$$

となることを示せ. 特に, $ma + nb = d$ となる $a, b \in \mathbb{Z}$ が存在する.

上の命題の 2 より, $\mathbb{Z}$ を無限巡回群, $\mathbb{Z}/n\mathbb{Z}$ を, 位数 n の巡回群を意味する記号として用いることが多い.

$a \in G$ とし $| < a > | = n$ であるとき, n を a の位数といい, $o(a)$ で表すことにする.

2.2 剰余類と商集合

H を G の部分群とする. $x, y \in G$ に対して,

$$x \sim_L y \Longleftrightarrow x^{-1}y \in H$$

によって, $\sim_L$ を定義すると, これは同値関係になる. 実際, $x^{-1}x = e \in H$ だから, 反射律が成立し, $x^{-1}y \in H$ とすると, $(x^{-1}y)^{-1} = y^{-1}x \in H$ となるので, 対称律が成立し, $x \sim_L y$, $y \sim_L z$ とすると, $x^{-1}y \in H$ かつ $y^{-1}z \in H$ となるが, このとき, $x^{-1}z = (x^{-1}y)(y^{-1}z) \in H$ となるので, 推移律が成立する. この同値関係による商集合 $G/\sim_L$ を G/H と書き, G の H による左剰余類の集合という. $a \in G$ とすると, a と $\sim_L$ で同値な元の集合 a の H に関する左剰余類という. これを $\overline{a}_L$ と表すと,

$$\overline{a}_L = \{x \in G \mid a \sim_L x\} = aH = \{ah \mid h \in H\}$$

が成立する. 実際, $ah \in aH$, $h \in H$ なら, $a^{-1}ah = h \in H$ で, $ah \sim_L a$ であり, 逆に, $a \sim_L x$ なら $a^{-1}x = h$ となる $h \in H$ が存在するから, $x = ah \in aH$ である.

左剰余類と同様に,

$$x \sim_R y \Longleftrightarrow xy^{-1} \in H$$

で, $\sim_R$ を定義すると, やはり同値関係になる. この同値関係による商集合 $G/\sim_R$ を $H\backslash G$ と書き, H による右剰余類の集合という. $a \in G$ に対し, a と $\sim_R$ で同値な元の集合を $\overline{a}_R$ と表すと,

$$\overline{a}_R = \{x \in G \mid x \sim_R a\} = Ha = \{ha \mid h \in H\}$$

となる. $i : G \to G$ を $i(x) = x^{-1}$ とすると, これは, 全単射な写像を与える. $\{a_j\}_{j \in I} \subset G$ を G/H の代表元の集合を取り, i から誘導される写像,

$$\overline{i} : G/H \to H\backslash G, \qquad \overline{i}(a_jH) = Ha_j^{-1}$$

を考えると, これは well–defined で, 全単射を与えることが容易に分かる. 従って, $|G/H| = |H\backslash G|$ が成立する. この濃度を H の G に対する指数といい, $[G : H]$ で表す.

問 2.2.1　$\bar{i}$ が well-defined で, 全単射であることを示せ.

定理 2.2.1（Lagrange）　G を有限群, H をその部分群とする.

1. $|G| = [G : H]|H|$, 特に部分群の位数は G の位数の約数である.
2. $a \in G$ に対して, $o(a)$ は $|G|$ の約数である.

証明. 1. $f : H \to aH$ を $f(h) = ah$ で定めると, H は部分群なので, 全単射になる. 実際, 全射性は aH の定義から従い, $ah = ah'$ なら両辺から a^{-1} を掛けることにより, $h = h'$ となり単射性が従う. よって, $\{a_i\}$ を G/H の代表系とすると, $G = \coprod a_i H$ で, $|a_i H| = |H|$ なので, $|G| = |\{a_i\}||H| = [G : H]|H|$. 特に, この式の右辺の因子はともに整数なので, $|H|$ は $|G|$ の約数である.
2. $o(a) = | < a > |$ と 1. から従う.

命題 2.2.1　G を有限群, H, K を G の部分群とし, $G \supset H \supset K$ とするとき,

$$[G : K] = [G : H][H : K]$$

が成立する.

証明. $g_1, \ldots, g_m \in G$ を G/H の完全代表系とし, $h_1, \ldots, h_n \in H$ を H/K の完全代表系とするとき, $\{g_i h_j\}$ が G/K の完全代表系であることを示せばよい. $g \in G$ をとると, ある i が存在して, $g \in g_i H$ であるので, $g = g_i h$, $h \in H$ と書くことができる. このとき, j が存在して, $h \in h_j K$ であるので, $g \in g_i h_j K$ となり, $G = \bigcup_{i,j} g_i h_j K$ である. これは, G の K による剰余類の和集合であるので, i, j が異なれば集合として相異なることを示せばよい. $g_{i'} h_{j'} K = g_i h_j K$ であるとする. このとき, $K \subset H$ かつ h_j, $h_{j'} \in H$ なので,

$$g_{i'} H \supset g_{i'} h_{j'} K = g_i h_j K \subset g_i H$$

となる. $g_1, \ldots, g_m$ の取り方から, $g_i \neq g_{i'}$ なら $g_i H \cap g_{i'} H = \emptyset$ なので, このようなことが起こるのは, $i = i'$ のときだけである. さらにこのとき, $h_{j'} K = h_j K$ となるので, $j = j'$ となる. よって, 対偶を取ると, $i \neq i'$ または $j \neq j'$ なら, $g_i h_j K \neq g_{i'} h_{j'} K$ となり, $G = \coprod_{i,j} g_i h_j K$ となる.

G を群, H, K を G の部分群とする. $x, y \in G$ に対して,

$$x \sim_T y \Longleftrightarrow h \in H \text{ と } k \in K \text{ が存在して, } y = hxk$$

で定義すると, $\sim_T$ は同値関係になる. これに関する同値類の集合を H, K に関する両側剰余類といい. $H\backslash G/K$ と書く. $x \in G$ のこの同値関係による同値類の集合は, HxK となる. $H\backslash G/K$ の個数については, 左右の剰余類のような易しい表示はない.

問 2.2.2　$\sim_T$ が G の同値関係を与えることを示せ.

2.3　正規部分群と準同型定理

定義 2.3.1　G を群, N を G の部分群とする. N が G の正規部分群であるとは, 任意の $g \in G$ に対して, $gNg^{-1} = N$ が成立することを言う. このとき, $G \rhd N$ あるいは, $N \lhd G$ と書く.

例 2.3.1　　1.　G および $\{e\}$ は, G の正規部分群である. これらを自明な正規部分群という.

2.　G が可換群なら, G の任意の部分群は正規部分群である.

3.　G の中心, $Z(G)$ は G の正規部分群である.

問 2.3.1　例 2.3.1 の 2., 3. を示せ.

G を群, N を G の正規部分群とする. 2 つの左剰余類 $G/N \ni aN, bN$ に対して, $aNbN = ab(b^{-1}Nb)N = abN$ が成立する (等号は, 全て集合としての一致を意味している). したがって, $aNbN = abN$ で G/N の積を定義すると, G/N は群をなす. 実際, 結合律は G の結合律から従い, 単位元は, $e \in G$ の剰余類である N で, gN $(g \in G)$ の逆元は, $g^{-1}N$ である. G/N のこの規則での群を G の正規部分群 N による商群 (または剰余群) という. この定義から, 商群への自然な射影

$$\pi : G \to G/N, \quad \pi(g) = gN$$

は群の全射準同型写像になる.

G が自明でない正規部分群を持てば, G の性質の多くは, 正規部分群 N と商群 G/N の性質に帰着することが, 原理的にはできる. したがって, 次のような定義がされる.

定義 2.3.2　群 G は, 非自明な正規部分群を持たないとき, 単純群であるという.

例 2.3.2　可換な有限単純群は, 素数 p に対する加法群 $\mathbb{Z}/p\mathbb{Z}$ に同型になる.
実際, 可換群では, 任意の部分群は正規部分群である. 群の位数が合成数であれば, その素因子を位数にもつ元の存在が容易に示せるので, それから生成される部分群を考えることにより, 単純群ではなくなる. 位数が素数 p であれば, 約数は 1 と p だけなので, 素数位数の群は常に単純群である. また G を位数 p を持つ群とすれば, 単位元と異なる任意の元 $a \in G$ の位数は p であり, $G =< a >$ となる. このとき $G \to \mathbb{Z}/p\mathbb{Z}$, $a \mapsto \overline{1}$ は群の同型写像になる.

5 次以上の交代群が非可換な単純群であることが, 5 次以上の方程式の根の公式が作れない理由である. 有限単純群は, その同型類が完全に分類されている. (有限) 群論に関しては, すぐれた日本語の専門書, [11, 12] がある.

G, G' を群とし, $f : G \to G'$ を準同型写像とする. このとき, f の像, $\mathrm{Im}(f) = f(G) = \{f(x) \mid x \in G\}$ は G' の部分群であり, f の核, $\mathrm{Ker}(f) = f^{-1}(e) = \{x \in G \mid f(x) = e\}$ は G の正規部分群になる.

問 2.3.2　　1.　上の $\mathrm{Im}(f)$ が G' の部分群で, $\mathrm{Ker}(f)$ が G の正規部分群であることを証明せよ.

2.　群の準同型写像 f が単射 $\iff$ $\mathrm{Ker}(f) = \{e\}$ を示せ.

定理 2.3.1 **(準同型定理)**　G, G' を群とし, $f : G \to G'$ を群の準同型写像とする. このとき, f から定まる自然な同型写像 $\overline{f} : G/\mathrm{Ker}(f) \xrightarrow{\simeq} f(G)$ が存在する.

証明.　$a \in G$ に対して, $\overline{f}(a\mathrm{Ker}(f)) = f(a)$ とすると, $\overline{f}$ は well-definend である. 実際, $a\mathrm{Ker}(f) = b\mathrm{Ker}(f)$ とすると, $a^{-1}b \in \mathrm{Ker}(f)$ となるので, $f(a^{-1}b) = e$ となり, f が準同型写像だから, $f(a) = f(b)$ となる. 上にあるように, $\mathrm{Ker}(f)$ は G の正規部分群だから, $G/\mathrm{Ker}(f)$ は群の構造を持ち, もともと f は準同型写像だから $\overline{f}$ も準同型写像である. $\mathrm{Im}(f)$ への全射であることは, 明らかである. $\overline{f}(a\mathrm{Ker}(f)) = e$ とすると, $a \in \mathrm{Ker}(f)$ となるので, $\mathrm{Ker}(\overline{f}) = \{\mathrm{Ker}(f)\} \in G/\mathrm{Ker}(f)$ となるので, $\overline{f}$ の核は単位元のみとなり, $\overline{f}$ は単射である.

例 2.3.3　1. $\mathrm{sgn} : S_n \to \{\pm 1\}$ は全射準同型写像で, $\mathrm{Ker}(\mathrm{sgn}) = A_n$ である. 従って, $S_n \rhd A_n$ であり, $S_n/A_n \cong \{\pm 1\}$ である.

2. R を可換環とする. 行列式を取る写像, $\det : GL_n(R) \to R^\times$ は全射準同型写像である (例 2.1.1 の 3. det の全射性の証明を与えよ). $\mathrm{Ker}(\det) = SL_n(R)$ なので, $GL_n(R) \rhd SL_n(R)$ で, 準同型定理より, $GL_n(R)/SL_n(R) \cong R^\times$ となる.

3. $S^1 = \mathbb{C}^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ とおく. これは, 通常の積により群となる (図形的には, 複素平面で原点を中心とした半径 1 の円周. S^1 の S は Sphere(球面) の頭文字の S で, 1 は 1 次元の意味). $e : \mathbb{R} \to S^1$ を $e(x) = e^{2\pi i x}$ で定義すると, これは群の全射準同型写像となる. $\mathrm{Ker}(e) = \mathbb{Z}$ なので, e は群の同型写像 $\overline{e} : \mathbb{R}/\mathbb{Z} \xrightarrow{\simeq} S^1$ を得る. 実際には, $\mathbb{R}/\mathbb{Z}$ に適切な位相を入れると, $\overline{e}$ は群の同型写像であるだけでなく, 位相同型写像にもなる ($\overline{e}$ が位相同型写像になるように, $\mathbb{R}/\mathbb{Z}$ に位相を入れると考えるべきかもしれない).

例 2.3.4　例 1.2.2 で定義した, $I_a \in \mathrm{Aut}(G)$ を考える. $I : G \to \mathrm{Aut}(G)$, $a \mapsto I_a$ は準同型写像になる (証明せよ). $\mathrm{Ker}(I) = Z(G)$ (G の中心) であり, 準同型定理より, $\mathrm{Im}(I) \cong G/Z(G)$ が成立する.

問 2.3.3　上で, $\mathrm{Im}(I) \lhd \mathrm{Aut}(G)$ が成立することを示せ. 商群 $\mathrm{Aut}(G)/\mathrm{Im}(I)$ を G の外部自己同型群という.

定理 2.3.2（第 1 同型定理）　H を G の部分群とし, N を G の正規部分群とするとき, HN は G の部分群であり, $HN/N \cong H/(H \cap N)$.

証明.　N が正規部分群だから, $h' \in H$, $n \in N$ に対して ${h'}^{-1} n h' \in N$ である. よって, h, $h' \in H$, n, $n' \in N$ に対して, $hnh'n' = (hh')(({h'}^{-1} n h')n') \in HN$ となり, HN は G の部分群である.

$\pi : G \to G/N$ を自然な射影とし, π の H への制限 $\pi_{|H}$ を考える. 定義から $\pi_{|H}$ は準同型写像で, $\mathrm{Im}(\pi_{|H}) = \pi_{|H}(H) = HN/N \subset G/N$ である $\mathrm{Ker}(\pi_{|H}) = H \cap N$ となるのも明らかなので, 準同型定理から, $\pi_{|H}$ は群の同型写像, $\overline{\pi}_{|H} : H/(H \cap N) \xrightarrow{\simeq} HN/N$ を与える.

定理 2.3.3（第 2 同型定理）　$G \rhd H$, $G \rhd N$ かつ $H \supset N$ とする. このとき,

$$G/H \cong (G/N)/(H/N)$$

証明.　$H \supset N$ だから, $f : G/N \longrightarrow G/H$ を $f(aN) = aH$ と定めると, これは, well–defined である. 商群の定義から, f は全射準同型写像となることも, 直ちにわかる. また, $\mathrm{Ker}(f) = H/N$ となることも, 定義からわかるので, 準同型定理を用いて, 定理を得る.

2.4　群の作用と置換表現

定義 2.4.1　G を群 X を集合とする. G の集合 X への左からの作用とは, 写像

$$G \times X \to X, \quad G \times X \ni (g, x) \mapsto g \cdot x \in X$$

で, 次を満たすものをいう. このとき, $G \curvearrowright X$ と書く.

1. $(gh) \cdot x = g \cdot (h \cdot x), \qquad g, h \in G,\ x \in X.$
2. $e \cdot x = x, \qquad x \in X.$

同様に, 右からの作用とは, 写像

$$X \times G \to X, \quad G \times X \ni (x, g) \mapsto x \cdot g \in X$$

で, 次を満たすものをいう. このとき, $X \curvearrowleft G$ と書く.

1. $x \cdot (gh) = (x \cdot g) \cdot h, \qquad g, h \in G,\ x \in X.$
2. $x \cdot e = x, \qquad x \in X.$

特に混乱の恐れがないときは, 作用を積のように $g \cdot x = gx$, $x \cdot g = xg$ と書く. G が X に作用しているとき, G を X の変換群ともいう.

例 2.4.1

1. $G = S_n$(n 次対称群), $X = [n] = \{1, 2, \ldots, n\}$ とする. $\sigma \in G$, $x \in X$ に対して, $\sigma \cdot x = \sigma(x)$ は, 対称群の集合 $[n]$ への作用を定める. より一般に X を集合として, $S(X)$ を X の全単射全体のなす群として, 同様の作用が定まる.
2. R を可換環とする. R^n を R の n 個の直積集合で, 各成分を縦に並べて, R を成分とする列ベクトルだと思う. $G = GL_n(R)$ は R^n に行列の積で左から作用する. R_n をやはり群 R の n 個の直積で, 各成分を横に並べて行ベクトルであると思うと, 行列の (右からの) 積で $GL_n(R)$ は R_n に右から作用する.
3. 群 G 自身の積 $G \times G \to G$, $(g, x) \mapsto gx$, $(x, g) \mapsto xg$ はそれぞれ, G の G 自身への左右からの作用となる. これらをそれぞれ, 左移動, 右移動という. $G \supset H$ を部分群とすると, それぞれの作用を H に制限することにより, H の G への右移動, 左移動が定義される.
4. (共役) G の G 自身への左からの作用 $G \times G \to G$ を, $g \cdot x = I_g(x) = gxg^{-1}$ で定めることができる. これを共役による作用という.

注意 2.4.1 左右の違いは, 群での積 gh のうちどちらが先に X に作用するかを決めているのである.

例えば上の例 2.4.1, 2. において, $g \in GL_n(R)$ と列ベクトル $x \in R^n$ に対して, $x \cdot g = {}^t gx$ と定義する. このとき, これは右からの作用になる. 実際, ${}^t(gh) = {}^t h {}^t g$ なので, $x \cdot (gh) = {}^t(gh)x = {}^t h {}^t g x = {}^t h (x \cdot g) = (x \cdot g) \cdot h$ が成立し, 右からの作用の公理を満たす.

G が可換群の場合は, 左右の区別をする必要は無くなる.

煩雑さを避けるため, 以下では, 主に左からの作用を考えるが, 右からの作用でも同様の結果は得られる.

G が集合 X に左から作用しているとき, $a \in G$ に対して,

$$t_a : X \to X, \quad t_a(x) = ax,\ x \in X$$

で写像 t_a を定める. $t_{a^{-1}} \circ t_a(x) = a^{-1}(ax) = (a^{-1}a)x = ex = x = \mathrm{id}_X(x)$ で, 同様に $t_a \circ t_{a^{-1}} = \mathrm{id}_X$ となるので, t_a は X の全単射である. すなわち, $t_a \in S(X)$ となる. さらに, 作用の定義から, $t_a \circ t_b = t_{ab},\ a, b \in G$ が成立するので,

$$t : G \to S(X), \quad a \mapsto t_a$$

は群の準同型写像となる. この準同型写像を, G の X 上の置換表現という. 逆に, 準同型写像 $t : G \to S(X),\ a \mapsto t_a$ が与えられると, $a \in G,\ x \in X$ に対して, $a \cdot x = t_a(x)$ と定義すると, G の X 上の作用が定義されることが容易にわかる. 準同型写像 $t : G \to S(X)$ が単射であるとき, これに対する G の X への作用を忠実 (faithful) な作用であるという.

G が集合 X に左から作用しているとする. X に $\sim_G$ を

$$x \sim_G y \iff \text{ある } g \in G \text{ が存在して, } y = gx$$

で定義すると, これは同値関係になる.

問 2.4.1　上が同値関係になることを示せ.

X のこの同値関係による商集合 $X/\sim_G$ を $G\backslash X$ と書くことにする. $x \in X$ の同値類は,

$$\overline{x} = G \cdot x = \{gx \mid g \in G\}$$

であり, x の G–軌道 (orbit) と呼ばれる. $G\backslash X$ が 1 点集合となるとき, X 全体が 1 つの G–軌道となり, この G の X への作用は推移的 (transitive) であるという.

例 2.4.2　$H \subset G$ を部分群とする. H は G に積で左から作用する. このとき, $x \in G$ の H 軌道は, 右剰余類 Hx である. 逆に, 積で右から作用させると, x の H–軌道は左剰余類 xH となる.

G が X に左から作用しているとし, $x \in X$ とする. このとき,

$$\mathrm{Stab}_G(x) = G_x = \{g \in G \mid gx = x\}$$

は G の部分群になることが容易にわかる. これを x の固定化部分群 (stabilizer), あるいは等方部分群 (isotropy subgroup) という.

問 2.4.2
1. 上の記号を用いる. $x \in X$ で $y = gx \in X$ とするとき, $G_y = gG_xg^{-1}$ が成立することを示せ. 特にこのとき, $G_x \cong G_y$(群の同型) である.
2. $\mathrm{GL}_n(\mathbb{R})$ の $\mathbb{R}^n$ への行列の積による左からの作用において, $\mathbb{R}^n$ の軌道は, $\{0\}$ と $\mathbb{R}^n \setminus \{0\}$ の 2 つになることを示せ. (0 は零ベクトルの意味.)

命題 2.4.1　G が X に左から作用しているとし, $x \in X$ とする. このとき, 自然な全単射

$$\varphi : G/G_x \to G \cdot x$$

が存在する. 特に G が有限群なら, $|G \cdot x| = \dfrac{|G|}{|G_x|}$ が成立する.

証明. $\overline{g} \in G/G_x$ に対して, $\varphi(\overline{g}) = gx$ とする. φ は, $\overline{g}$ の代表元によらず, well–defined である. 実際, $h \in \overline{g}$ とすると, $h = gk,\ k \in G_x$ となるが, $hx = gkx = gx$ である. G–軌道 $G \cdot x$ と φ の定義から, φ は全射である. $\varphi(\overline{g}) = \varphi(\overline{h})$ とすると, $gx = hx$ となるから, 両辺に左から g^{-1} を作用させると, $g^{-1}hx = x$ となり, $g^{-1}h \in G_x$ となる. このとき, $h \in gG_x$ となり, $\overline{g} = \overline{h}$ となるから, φ は単射である.

2.5　共役類

$x \in G$ に対して, 共役による作用の x の軌道を x の共役類といい, $C(x)$ で表すことにする. すなわち, $C(x)$ は次で与えられる G の部分集合である.

$$C(x) = \{axa^{-1} \mid a \in G\}$$

$x, y \in G$ が同じ共役類の集合に属するとき, すなわち, ある $a \in G$ が存在して, $y = axa^{-1}$ となるとき, 互いに共役であるという.

例 2.5.1（Jordan 標準形）　複素数体上の一般線形群 $GL_n(\mathbb{C})$ を考える. $A, P \in GL_n(\mathbb{C})$ に対して, PAP^{-1} は, A を $\mathbb{C}^n$ 上の線形変換と見たときの, 基底の取り換えに対する行列表示の変化を表している. 群論的には, これらが $GL_n(\mathbb{C})$ の同じ共役類に属することと解釈できる. Jordan 標準形は, 共役類の代表元として最もやさしい形を見出すことに, 他ならない.

共役による作用の, x の固定化群を $C_G(x)$ と書いて, G における x の中心化群という. 定義から,

$$C_G(x) = \{a \in G \mid ax = xa\}$$

となる.

問 2.5.1　$S \subset G$ を部分集合とするとき,

$$N_G(S) = \{a \in G \mid aSa^{-1} = S\}, \qquad C_G(S) = \{a \in G \mid as = sa,\ \forall s \in S\}$$

とする. これらは G の部分群になることを示せ. それぞれ, 集合 S の G における正規化群, 中心化群という.

$C(x) = \{x\}$(1 点集合) となるためには, 任意の $a \in G$ に対して, $axa^{-1} = x$, すなわち, $ax = xa$ が成立することであり, これは, $x \in Z(G)$ と同値になる.

G を有限群とし, $\{x_i\}$ を G の共役類の代表元の集合とする. G を共役類の和集合に分割すると, $G = \coprod_i C(x_i)$ となるが, $|C(x_i)| = 1$ であることと $x_i \in Z(G)$ が同値なので, G の位数に対して, 次の式が成立する.

$$|G| = |Z(G)| + \sum_{|C(x_i)|>1} |C(x_i)|$$

この式を, 類等式という. $|C(x_i)| = |G|/|C_G(x_i)|$ なので, $|C(x_i)|$ は $|G|$ の約数になる.

問 2.5.2　p を素数とする. 類等式を利用することにより, 位数 p^2 の群は可換群になることを示せ.

対称群の共役類

与えられた群に対して, 共役類を記述するのは, 群が複雑であれば大変な作業になる. ここでは, 共役類がわかりやすい記述を持つ群として, 対称群を取り上げる. 以下の計算では, 対称群の積は写像の合成で定義されていることに注意する.

S_n を n 次の対称群とする. $I = \{i_1, i_2, \ldots, i_r\} \subset \{1, \ldots, n\}$ とし, $c_I \in S_n$ を

$$\begin{cases} c_I(i_k) = i_{k+1},\ k = 1, \ldots, r-1 \\ c_I(i_r) = i_1 \\ c_I(j) = j,\ j \notin I \end{cases}$$

で定める. c_I を S_n の長さ r の巡回置換 (cycle) という. $c_I = (i_1, i_2, \ldots, i_r)$ と書く. $(i_1, i_2, \ldots, i_r) = (i_2, i_3, \ldots, i_r, i_1) = \cdots$ に注意する. ただ 1 つの元からなる巡回置換 (i) は, 単位元と同じものである.

補題 2.5.1　$\sigma \in S_n$ とする. このとき, 集合の分割 $\{1, 2, \ldots, n\} = I_1 \sqcup I_2 \sqcup \cdots \sqcup I_r$ が存在して, $\sigma = c_{I_1} \cdots c_{I_r}$ と書ける. $c_{I_1}, \cdots, c_{I_r}$ は互いに可換で, σ をこのような積に表す方法は, 積の順序を除けば一意的である.

証明.　$\sigma \in S_n$ に対して, $\sigma^s(1) = 1$ となる最小の自然数 s をとる. このとき, 1, $i_2 = \sigma(1)$, $i_3 = \sigma^2(1)$, ..., $\sigma^{s-1}(1) = i_s$ は, s の取り方からすべて異なる数である. $I_1 = \{1, i_2, \ldots, i_s\}$ とする. $I_1 = \{1, \ldots, n\}$ なら, $\sigma = c_{I_1}$ となり証明は終わる. そうでなければ, $k_1 \in \{1, \ldots, n\} \setminus I_1$ が存在する. 同様に, $\sigma^t(k_1) = k_1$ となる最小の自然数 t をとり, $k_2 = \sigma(k_1), \ldots, k_t = \sigma(k_{t-1})$ とすると, これらはすべて異なる数になる. $I_2 = \{k_1, \ldots, k_t\}$ とすれば, 作り方から, $I_1 \cap I_2 = \emptyset$ である. $I_1 \sqcup I_2 = \{1, \ldots, n\}$ なら, $\sigma = c_{I_1} c_{I_2}$ でやはり定理が成立することがわかる. そうでないなら, この操作を繰り返すことにより, 集合分割 $\{1, \ldots, n\} = I_1 \sqcup \cdots \sqcup I_r$

が得られ, $\sigma = c_{I_1} \cdots c_{I_r}$ が成立する. これらの巡回置換が互いに可換であることは, 作り方より明らかである. また, このような表示は積の順を除いて一意的である.

例 2.5.2

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 2 & 4 & 1 & 9 & 8 & 7 & 6 \end{pmatrix} = (1,3,2,5)(4)(6,9)(7,8)$$

系 2.5.1 1. S_n は互換の集合 $\{(i,\, j)\}$ から生成される.

2. S_n は $n-1$ 個の隣接互換 $(1,\, 2), (2,\, 3), \ldots, (n-1,\, n)$ から生成される.

証明. 1. 上の定理から, 巡回置換 $(i_1, i_2, \ldots, i_r)$ が互換の積で表されることを示せばよいが, 簡単な計算で,

$$(i_1, i_2, \ldots, i_r) = (i_1, i_2)(i_2, i_3) \cdots (i_{r-1}, i_r)$$

となることがわかる. 2. は問とする (1. に帰着させる).

問 2.5.3 上の 2. を証明せよ.

$\sigma \in S_n$ として, σ から補題 2.5.1 で定まる集合分割を, $\{1, \ldots, n\} = I_1 \sqcup \cdots \sqcup I_r$ とする. この集合分割において, $|I_k| = i$ となる集合, すなわち, i 個の元からなる集合の個数を m_i, $(i = 1, 2, \ldots, n)$ とする. このとき, σ はサイクルタイプ $(1^{m_1} 2^{m_2} \cdots n^{m_n})$ を持つという. ベキ乗と記号が紛らわしいが, 問 2.5.4 の結果が, この記号の起源ではないかと思われる.

例 2.5.3 例 2.5.2 のサイクルタイプは, $(1^1 2^2 3^0 4^1 5^0 6^0 7^0 8^0 9^0) = (1^1 2^2 4^1)$(0 の部分は省略する) である.

命題 2.5.1 $\sigma, \sigma' \in S_n$ が共役であるための必要十分条件は, そのサイクルタイプが一致することである

証明. 補題 2.5.1 で定まる σ の巡回置換への分解を,

$$\sigma = (i_1, \ldots, i_r)(j_1, \ldots, j_s) \cdots (k_1, \ldots, k_t)$$

とする. 簡単な計算で (例えば, $\tau\sigma\tau^{-1}(\tau(i_1)) = \tau(i_2)$),

$$\tau\sigma\tau^{-1} = (\tau(i_1), \ldots, \tau(i_r))(\tau(j_1), \ldots, \tau(j_s)) \cdots (\tau(k_1), \ldots, \tau(k_t))$$

を得るので, 共役によってサイクルタイプは変化しない. 逆に σ, σ' が同じサイクルタイプを持つとする. σ' を σ のサイクルタイプに合わせて,

$$\sigma' = (i'_1, \ldots, i'_r)(j'_1, \ldots, j'_s) \cdots (k'_1, \ldots, k'_t)$$

と書くと,

$$\tau = \begin{pmatrix} i_1 & \cdots & i_r & j_1 & \cdots & j_s & k_1 & \cdots & k_t \\ i'_1 & \cdots & i'_r & j'_1 & \cdots & j'_s & k'_1 & \cdots & k'_t \end{pmatrix}$$

とすれば, 上の計算から, $\tau\sigma\tau^{-1} = \sigma'$ となり, σ, σ' は互いに共役になる.

問 2.5.4 $\sigma \in S_n$ のサイクルタイプが $(1^{m_1} 2^{m_2} \cdots n^{m_n})$ であるとき,

$$|Z_{S_n}(\sigma)| = 1^{m_1} m_1! \cdot 2^{m_2} m_2! \cdots n^{m_n} m_n!$$

であり, σ と共役な元の個数は, $\dfrac{n!}{|Z_{S_n}(\sigma)|} = \dfrac{n!}{1^{m_1} m_1! \cdot 2^{m_2} m_2! \cdots n^{m_n} m_n!}$ となることを示せ.

自然数 n に対して, $n = \lambda_1 + \lambda_2 + \cdots + \lambda_r$, $\lambda_1 \geqq \lambda_2 \geqq \cdots \geqq \lambda_r > 0$ となるとき, $(\lambda_1, \lambda_2, \ldots, \lambda_r)$ を n の分割 (partition) という. n の分割の総数を $p(n)$ と書いて, n の分割数という ($p(0) = 1$ と約束する). $p(1) = 1$, $p(2) = 2$, $p(3) = 3$, $p(4) = 5$, $p(5) = 7, \ldots$ である.

$\sigma \in S_n$ に対して, 補題 2.5.1 から定まる集合分割 $\{1, \ldots, n\} = I_1 \sqcup \cdots \sqcup I_r$ を考え, $|I_1|, \ldots, |I_r|$ を大きい順に $\lambda_1 \geqq \lambda_2 \geqq \cdots \geqq \lambda_r > 0$ と並べると, これは n の分割を与える. 逆に, n の分割 $(\lambda_1, \ldots, \lambda_r)$ に対して, $I_1 = \{1, \ldots, \lambda_1\}$, $I_2 = \{\lambda_1 + 1, \ldots, \lambda_1 + \lambda_2\}, \ldots, I_r = \{\sum_{i=1}^{r-1} \lambda_i + 1, \ldots, n\}$ として, $\{1, \ldots, n\}$ の集合分割が得られる. 命題 2.5.1 より, これは, 1 つの対称群の共役類を与える. よって次を得る.

定理 2.5.1　n 次対称群 S_n は, $p(n)$ 個の共役類に分割される.

2.6　Sylow(シロー) の定理

群の作用の応用として, Sylow の定理について述べる. 有限群の性質を調べる上で, もっとも基本的な定理である.

p を素数とする. $|G| = p^n$, $(n \geqq 1)$ であるとき, G は p–群であるという. G を有限群とし, $|G| = p^n m$, $(p, m) = 1$ とする. G の部分群 P で, $|P| = p^n$ となる群を Sylow p–部分群という. 次の定理が, 名前の由来である.

定理 2.6.1 (Sylow)　上の記号の下で, 次が成立する.

1. $P' \subset G$ を G の部分群で p–群であるとすると, P' を含む Sylow p–部分群が存在する.
2. G の Sylow p–部分群は, すべて互いに共役である. すなわち P, Q を G の Sylow p–部分群とすると, $g \in G$ が存在して, $gPg^{-1} = Q$ となる.
3. G に含まれる異なる Sylow p–部分群の個数は, $kp + 1$, $k \in \mathbb{Z}$, $k \geqq 0$ の形をしている.

証明. 1.　まず, Sylow p–部分群が存在することを示す. 集合 X を次のように定義する.

$$X = \{S \subset G \mid S \text{ は } G \text{ の部分集合で}, |S| = p^n\}$$

X に, G の元 g を左移動で作用させる. すなわち,

$$X \ni S \mapsto gS = \{gs \mid s \in S\} \in X.$$

$|X|$ は $p^n m$ 個の元から p^n 個の元を選ぶ組み合わせの総数だから,

$$|X| = \binom{p^n m}{p^n} = \frac{p^n m}{p^n} \cdot \frac{p^n m - 1}{p^n - 1} \cdots \frac{p^n m - i}{p^n - i} \cdots \frac{p^n m - p^n + 1}{1}$$

である. この式で, $(p, m) = 1$ だから, $p^n m - i$ と $p^n - i$ を素因数分解した時の p のベキは同じになる. すなわち, 分母・分子ともに同じ p のベキで割り切れるので, 約分をしてしまうと, $(|X|, p) = 1$ である. 従って, $S \in X$ が存在して, X の G–軌道 $G \cdot S$ で, $(|G \cdot S|, p) = 1$ となるものが存在する. P を S の固定化群とする. $|G \cdot S| = \dfrac{|G|}{|P|}$, $|P| = \dfrac{|G|}{|G \cdot S|}$ なので, $|P|$ は p^n の倍数である. 一方, $s \in S$ に対して, $Ps \subset S$ で $|Ps| = |P|$, なので, $|P| \leqq |S| = p^n$ となる. 従って, $|P| = p^n$ となり, P は Sylow p–部分群となる.

P' を G の部分群で, p–群であるとする. P を (上で存在が保証されている) G の Sylow p–部分群とする.

$$G = Px_1P' \sqcup \cdots \sqcup Px_rP'$$

を 2.2 節の最後で述べた, G の P, P' に対する両側剰余類への分解とする. 各 Px_iP' は P の左移動で不変な集合で, この P の左移動に関する軌道分解を考える.

$$Px_iy_1 = Px_iy_2, \quad y_1, y_2 \in P' \iff x_iy_1y_2^{-1}x_i^{-1} \in P \iff y_1y_2^{-1} \in x_i^{-1}Px_i$$

なので,

$$(P' \cap x_i^{-1}Px_i)\backslash P' \ni (P' \cap x_i^{-1}Px_i)y \mapsto Px_iy \subset Px_iP' \quad (y \in P')$$

は, 右剰余類の集合 $(P' \cap x_i^{-1}Px_i)\backslash P'$ から, Px_iP' の P–軌道の集合への well–defined な全単射を与えることがわかる. P' が p–群なので, $|(P' \cap x_i^{-1}Px_i)\backslash P'|$ は, p^{e_i} の形をしている. 従って, 上の両側剰余類への分解を用いると, P の G への左移動の作用の軌道の個数は,

$$p^{e_1} + p^{e_2} + \cdots + p^{e_r}$$

となる. 一方, G の P の左移動の軌道は, G の P による右側剰余類に他ならないので, その軌道の数は, $|G|/|P| = m$ である. $(m, p) = 1$ なので, $m = p^{e_1} + p^{e_2} + \cdots + p^{e_r}$ となるためには, $e_i = 0$ となる i が存在する. この i に対して, $P' \cap x_i^{-1}Px_i = P'$ であり, $x_i^{-1}Px_i$ は P' を含む Sylow p–部分群である.

2. 1. の後半部分の証明において $P' = P$ と取れば良い.
3. $\mathcal{P}$ を G の Sylow p–群全体のなす集合とする. G は共役によって, $\mathcal{P}$ に作用する.

$$G \times \mathcal{P} \ni (g, P) \mapsto gPg^{-1} \in \mathcal{P}$$

2. より, この作用は推移的であり, $P \in \mathcal{P}$ の固定化群は, $N_G(P) = \{g \in G \mid gPg^{-1} = P\}$ である. $N_G(P) \supset P$ に注意する. 2. の証明と同様に, $N_G(P)$ と P に対する G の両側剰余類への分解を考える. この際に, 最初の部分集合は, G の単位元に対応する剰余類とする.

$$G = N_G(P)y_0P \sqcup N_G(P)y_1P \sqcup \cdots \sqcup N_G(P)y_sP, \quad (y_0 = e)$$

1. の証明の後半と同様に, 各 $N_G(P)y_jP$ における $N_G(P)$ 軌道の数は, $|(P \cap y_j^{-1}N_G(P)y_j)\backslash P| = p^{f_j}$ となる. $f_0 = 0$ であることに注意する. $j \neq 0$ に対して, $f_j = 0$ となるとする. このとき, $y_j^{-1}N_G(P)y_j \supset P$ となり, $N_G(P) \supset y_jPy_j^{-1}$ を得る. よって, P, $y_jPy_j^{-1}$ はともに $N_G(P)$ の Sylow p–部分群になるから, 2. より互いに $N_G(P)$ の中で共役である. 従って, $x \in N_G(P)$ が存在して, $P = xy_jPy_j^{-1}x^{-1}$ となる. このとき, $xy_j \in N_G(P)$ である. $x \in N_G(P)$ から $y_j \in N_G(P)$ となり, $N_G(P)y_jP = N_G(P)P$ となるので, $j \neq 0$ に矛盾する. よって, $j \neq 0$ なら $f_j > 0$ であり,

$$|N_G(P)\backslash G| = 1 + p^{f_1} + \cdots + p^{f_s} = 1 + (p^{f_1 - 1} + \cdots + p^{f_s - 1})p = 1 + kp$$

を得る. G の $\mathcal{P}$ への共役による作用は推移性と $P \in \mathcal{P}$ の固定化群が $N_G(P)$ であることから, 命題 2.4.1 を用いると, $|\mathcal{P}| = |G/N_G(P)| = |N_G(P)\backslash G| = 1 + kp$ となる.

2.7 群の直積

G, H を群とするとき, 直積集合 $G \times H$ には, 成分毎の積を考えることにより, 群の構造が入る. すなわち, (g_1, h_1), $(g_2, h_2) \in G \times H$ に対して, $(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2)$ と定義するのである. 積の結合律は, それぞれの群での結合律から従う. このとき, 単位元は, e_G, e_H をそれぞれ G, H の単位元としたとき,

(e_G, e_H) であり, $(g, h) \in G \times H$ の逆元は, (g^{-1}, h^{-1}) となる. このようにしてできる群を, G, H の直積群という. このとき, $\{(g, e_H) \in G \times H \mid g \in G\}$ は $G \times H$ の G と同型な部分群であるが, これを G と同一視する. また,

$$i_G : G \to G \times H, \quad i_G(g) = (g, e_H) \in G \times H$$

は, 中への同型写像であるが, これを自然な包含写像 (inclusion), あるいは埋め込み (immersion) という. H についても同様に, 包含写像 $i_H : H \to G \times H,\ h \mapsto (e_G, h)$ が定義される.

一般に, 有限個の群 $G_1, \ldots, G_r$ が与えられたとき, これらの群の直積群 $G_1 \times \cdots \times G_r$ も同様に定義される.

命題 2.7.1 H, K を群とし, $G = H \times K$ を H, K の直積で作られる群とする. H, K を上で述べたように G の部分群と見る. このとき, 次が成立する.

1. $G = HK$ で, 任意の $g \in G$ は, $g = hk$, $h \in H$, $k \in K$ と一意的に書ける.
2. H の元と K の元は G の中で互いに可換である.
3. $H \cap K = \{e\}$.
4. $H \lhd G$ かつ $K \lhd G$.

証明. 1. 2. 3. は定義から明らかである. 4. は 2. から直ちに従う.

上の命題は, 逆が成立する. すなわち, 次の 2 つの定理が成立する.

定理 2.7.1 G を群, H, K を G の部分群で, 命題 2.7.1 の 1, 2 を満たすとする. このとき, 群として $G \cong H \times K$ である.

証明.

$$f : H \times K \to G, \quad f(h, k) = hk$$

とおくと, 性質 1 からこれは全単射で, 性質 2 から準同型写像となる. すなわち, f は同型写像で, $G \cong H \times K$.

定理 2.7.2 G を群, H, K を G の部分群で, $G = HK$ かつ, 命題 2.7.1 の 3, 4 を満たすとする. このとき, 群として $G \cong H \times K$ である.

証明. 上の定理 2.7.1 の 1, 2 が成立することを示せばよい. $G = HK$ は仮定されている. $g = hk = h'k'$, $h, h' \in H$, $k, k' \in K$ とする. このとき, $h'^{-1}h = k'k^{-1}$ となる. 左辺は, H の元で右辺は K の元となるから, 両辺とも $H \cap K$ の元である. $H \cap K = \{e\}$ なので, $h'^{-1}h = k'k^{-1} = e$ となり, $h = h'$, $k = k'$ を得るので, $g = hk$ の書き方は一意的である. $h \in H$, $k \in K$ とする. $H \lhd G$ なので, $(khk^{-1})h^{-1} \in H$ である. 同様に, $K \lhd G$ なので, $k(hk^{-1}h^{-1}) \in K$ である. よって, $khk^{-1}h^{-1} \in H \cap K = \{e\}$ となり, $hkh^{-1}k^{-1} = e$ となって, $hk = kh$ が任意の $h \in H$, $k \in K$ について成立し, 定理 2.7.1 の 2 が成立する.

G を群, H を G の部分群とする. G の部分群 K が存在して, $G \cong H \times K$ となるとき, H を G の直積因子という. すべての群は, 自明な直積分解 $G = G \times \{e\}$ を持つ. G, $\{e\}$ を自明な直積因子という. 自明な直積因子以外の直積因子を持たない群を**直既約**という.

問 2.7.1 $\mathbb{Z}$ は直既約であることを示せ.

例 2.7.1（Sylow の定理の 1 つの応用）　p, q を素数とし, $p > q$ と仮定する. G を位数 pq の群とする. Sylow の定理 (定理 2.6.1) より, 位数 p の部分群 (Sylow p–部分群)$P \subset G$ が存在する. p が素数なので, $P \cong \mathbb{Z}/p\mathbb{Z}$ であることに注意する. $G \supset N_G(P) \supset P$ で, $[G : P] = q$ が素数であることから, $N_G(P) = G$ もしくは, $N_G(P) = P$ となる. 定理 2.6.1 3 より,

$$kp + 1 = |\{\text{Sylow } p - \text{部分群 }\}| = [G : N_G(P)] = q \text{ または } 1$$

となるが, $p > q$ より上の式で $k = 0$ となり, $[G : N_G(P)] = 1$ となって, $N_G(P) = G$ が成立するので, $P \lhd G$ である.

q に対しても Sylow の定理を適用すると, 位数 q の部分群 $Q \subset G$ が存在する. q が素数なので, $Q \cong \mathbb{Z}/q\mathbb{Z}$ である. $P \lhd G$ なので, PQ は G の部分群となる (第 1 同型定理, 定理 2.3.2 の証明を見よ). $|PQ| > p$ なのは明らかなので, G の部分群の位数は pq の約数であることを考えると, $PQ = G$ である. また, $P \cap Q = \{e\}$ であることも容易にわかる.

G が, 常に P と Q の直積になる条件を考える. 定理 2.7.1 の 1, 2 が常に成立する条件を考える. $G = PQ$ と $P \cap Q = \{e\}$ より, 定理 2.7.1 の 1 が成立することがわかる (定理 2.7.2 の証明を見よ). 調べることは, 定理 2.7.1 の 2 の可換性である. a, b をそれぞれ P, Q の生成元とする. $P \lhd G$ より, $bab^{-1} \in P$ である. 以下, 群の積は乗法的に書く. 従って, $bab^{-1} = a^r$ となる $r \in \mathbb{N}$ $((r, p) = 1)$ が存在する. この r が (p を法として) 1 以外に存在しない条件を考える. $a = eae^{-1} = b^q ab^{-q} = a^{r^q}$ だから, $r^q \equiv 1 \pmod{p}$ でなければならない. $q \nmid (p-1)$ なら, このような r は $r \equiv 1 (\mathrm{mod}\ p)$ 以外には存在しない (Fermat の小定理から, 乗法群 $(\mathbb{Z}/p\mathbb{Z})^\times$ の元の位数は, $p - 1$ の約数.). よって次の事実が証明された.

p, q を素数として, $p > q$ とする. $q \nmid (p-1)$ なら位数 pq の群は, 直積群 $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ と同型である.

問 2.7.2

1. 上の例の最後の部分で, $q \,|\, (p-1)$ なら, $r^q \equiv 1 \pmod{p}$ かつ $r \not\equiv 1 \pmod{p}$ となる r が存在することを示せ (Fermat の小定理を使う).
2. p を 3 以上の素数 (必然的に奇数となるため, 奇素数という) とする. 位数 $2p$ の非可換群は, 2 面体群 Dih_{2p} と同型になることを示せ. ここで 2 面体群 (dihedral group)Dih_{2n} とは, 正 n 角形の合同変換群で, 中心と各頂点を結ぶ直線に対する対称移動 (鏡映) s と $\dfrac{2\pi}{n}$ の回転 r を用いると, $Dih_{2n} = \{e, r, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}\}$ ($s^2 = r^n = e$, $srs = r^{-1}$を満たす群) で与えられる.

有限生成アーベル群の基本定理の紹介

G を有限個の元から生成される可換群とする. このとき, G が巡回群の直積になるというのが, 有限生成アーベル群の基本定理である. 証明は, 少し一般化した, 単項イデアル整域上の有限生成加群の性質を述べた「単因子論」を $\mathbb{Z}$ に適用する形で行うのが自然なので, A 節で述べる.

定理 2.7.3（有限生成アーベル群の基本定理. 証明は付録 A, 定理 A.2）　G を有限個の元から生成される可換群とする. このとき, 自然数 $d_1, \ldots, d_r$ と l が一意的に定まって, $d_{i-1} \,|\, d_i$, $(i = 2, \ldots, r)$ であり, G は次のような巡回群の直積群と同型である. ここで $\mathbb{Z}^l$ は, $\mathbb{Z}$ の l 個の直積を意味する.

$$G \cong \mathbb{Z}^l \times \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}$$

2.8 可解群

G を群とし, $x, y \in G$ とする. $[x, y] = xyx^{-1}y^{-1}$ を, x, y の交換子 (commutator) という. 定義から, x, y が互いに可換であることと, $[x, y] = e$ であることは同値である. G の交換子全体から生成される部分群, $[G, G] =< [x, y] \mid x, y \in G >$ を G の交換子群 (commutatar subgroup) という. G が可換群である必要十分条件は, $[G, G] = \{e\}$ が成立することである.

問 2.8.1 $[S_3, S_3] = A_3,\ [S_4, S_4] = A_4$ を示せ.

命題 2.8.1 1. $G \rhd [G, G]$ であり, $G/[G, G]$ は可換群である.

2. G を群とし, N を G の正規部分群とする. G/N が可換群になる必要十分条件は, $N \supset [G, G]$ である.

証明. 1. $g[x, y]g^{-1} = gxyx^{-1}y^{-1}g^{-1} = (gxg^{-1})(gyg^{-1})(gxg^{-1})^{-1}(gyg^{-1})^{-1} = [gxg^{-1}, gyg^{-1}]$ だから, 交換子全体の集合は G の共役による作用で不変である. よって, それらの積も G の共役による作用で不変となり, $G \rhd [G, G]$ である. $G/[G, G]$ での x を代表元とする同値類を $\overline{x}$ で表すことにする. $x, y \in G$ とすると, $[x, y] \in [G, G]$ より $[\overline{x}, \overline{y}] = [x, y][G, G] = [G, G] = \overline{e}$ となり, $G/[G, G]$ は可換群である.

2. G/N が可換群とすると, 任意の $g, h \in G$ に対して, $ghN = hgN$ が成立するから, $g^{-1}h^{-1}gh = [g^{-1}, h^{-1}] \in N$ となり, $N \supset [G, G]$ が従う. 逆に, $N \supset [G, G]$ とすると, 任意の $g, h \in G$ に対して, $[g^{-1}, h^{-1}] \in [G, G] \subset N$ となる. これより $g^{-1}h^{-1}ghN = N$ となり, $ghN = hgN$ が成立し, G/N は可換群になる.

定義 2.8.1**（正規列と組成列）** G を群とする. G の部分群の列

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\}$$

を考える. このとき,

1. 上の列において, 常に $G_i \rhd G_{i+1}$ が成立するとき, この列を正規列という.
2. さらに, すべての i に対して, $G_i \supsetneqq N \supsetneqq G_{i+1}$ となる正規部分群 N が存在しない ($\Leftrightarrow G_i/G_{i+1}$ は単純群) とき, 組成列という. このとき, 商群 G_i/G_{i+1} を G の組成因子という.

注意 2.8.1 1. 上の 1. において, $G \rhd G_i$ は仮定していない. また, $G \rhd N_1$ かつ $N_1 \rhd N_2$ から, $G \rhd N_2$ は導けない (下の問 2.8.2, 3).

2. 有限群 G を与えると, G の組成因子からなる群の集合は, 同型を除いて一意的に決まることが証明できる (Jordan–Hölder の定理). 時間の都合で, その証明は与えない.

定義 2.8.2**（導来列と可解群）** 1. G を群とするとき, 部分群の列 $\mathcal{D}^k(G)$ を, 帰納的に $\mathcal{D}^1(G) = [G, G]$, $\mathcal{D}^i(G) = [\mathcal{D}^{i-1}(G), \mathcal{D}^{i-1}(G)]$ で定義する. このようにしてできる部分群の列,

$$G \supset \mathcal{D}^1(G) \supset \mathcal{D}^2(G) \supset \cdots$$

を G の導来列という.

2. 自然数 n が存在して, $\mathcal{D}^n(G) = \{e\}$ となるとき, G を可解群という.

定義から, $\mathcal{D}^i(G) \rhd \mathcal{D}^{i+1}(G)$ が常に成立し, 導来列は正規列になる. 命題 2.8.1 より, $\mathcal{D}^i(G)/\mathcal{D}^{i+1}(G)$ は可

換群になる. 可解群という言葉は, 代数方程式から決まる Galois 群が可解群であることと, その方程式が代数的に解けることが同値であることに由来する. Abel 群は常に可解群である.

有限群 G が可解群でないとは, ある k が存在して, $\mathcal{D}^k(G) = \mathcal{D}^{k+1}(G) \neq \{e\}$ となることになる. 例えば, G が非可換な単純群であれば, 容易に分かるように $\mathcal{D}^1(G) = \mathcal{D}(G) = G$ が成立し, 可解群ではない. 奇数位数の有限群は常に可解であることが知られている (Feit – Thompson (ファイト–トンプソン) の定理. Thompson は有限単純群の分類理論で Fields 賞を受賞したが, その中でも最も有名な定理である).

問 2.8.2　1. S_3 の導来列は, $S_3 \rhd A_3 \rhd \{e\}$ になることを示せ.

2. $V_4 = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \subset S_4$ とする. S_4 の導来列は, $S_4 \rhd A_4 \rhd V_4 \rhd \{e\}$ になることを示せ.
3. $N = \{e, (1,2)(3,4)\} \subset V_4$ とするとき, $A_4 \supset V_4 \supset N \supset \{e\}$ は組成列であることを示せ. また, N は A_4 の正規部分群ではないことを示せ.

命題 2.8.2　1. G が可解群であるための必要十分条件は, G の正規列

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

で, G_i/G_{i+1} が全て可換群となるようなものが存在することである.

2. 可解群の部分群は可解群である.
3. G を群, N を G の正規部分群とするとき, G が可解群であるための必要十分条件は, N, G/N がともに可解群となることである.

証明. 1. G が可解群なら, G の導来列は正規列でありさらに命題 2.8.1 より, $\mathcal{D}^i(G)/\mathcal{D}^{i+1}(G)$ は可換群であるので, $\mathcal{D}^i(G) = G_i$ とすれば良い. 逆に, 正規列

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

に対して, G_i/G_{i+1} が全て可換群であるとする. 命題 2.8.1 より, $\mathcal{D}(G_i) \subset G_{i+1}$ である. 特に $\mathcal{D}^1(G) \subset G_1$ であり, これより, $\mathcal{D}^2(G) = \mathcal{D}(\mathcal{D}^1(G)) \subset \mathcal{D}(G_1) \subset G_2$ となる. この操作を繰り返すことにより, $\mathcal{D}^l(G) \subset G_l$ が得られるので, 特に, $\mathcal{D}^n(G) = \{e\}$ となり, G は可解群である.

2. $G \supset H$ を部分群とする. 定義から $\mathcal{D}^1(G) = [G,G] \supset [H,H] = \mathcal{D}^1(H)$ が成立する. これより, 帰納的に $\mathcal{D}^i(G) \supset \mathcal{D}^i(H)$, $(i = 1, 2, \ldots)$ が証明できるので, $\mathcal{D}^n(G) = \{e\}$ なら $\mathcal{D}^n(H) = \{e\}$ である.

3. $G \rhd N$ を G の正規部分群とし, $\pi : G \to G/N$ を自然な全射準同型写像とする. G が可解群なら, 2. より, N も可解群である. $g, h \in G$ に対して, $[gN, hN] = [g,h]N$ が成立するので, $[G/N, G/N] \subset [G,G]N$ が成立する. よって, $\mathcal{D}^n(G) = \{e\}$ なら, $D^n(G/N) = \{e\}$ となり, G/N も可解群である.

逆に, G/N, N がともに可解群であると仮定する. 一般に, $f : G \to H$ を群の準同型写像とすると, g, $h \in G$ に対して $f([g,h]) = [f(g), f(h)]$ なので, $f(\mathcal{D}(G)) = \mathcal{D}(f(G))$ が成立する. これを G の導来列と自然な射影 $\pi : G \to G/N$ に適用すると, $\mathcal{D}^l(G/N) = \pi(\mathcal{D}^l(G))$ となる. G/N は可解群なので, $n \in \mathbb{N}$ が存在して,

$$G/N = \mathcal{D}^0(G/N) \supset \mathcal{D}^1(G/N) \supset \cdots \supset \mathcal{D}^n(G/N) = N$$

となる. 特に, $\mathcal{D}^n(G) = N$ であることに注意する.N も可解群なので, N の導来列を

$$N = G_n \supset G_{n+1} \supset \cdots \supset G_{m+n} = \{e\}$$

とする．これらから G の導来列は

$$G = G_0 \supset \mathcal{D}^1(G) \supset \cdots \supset \mathcal{D}^n(G) = N \supset G_{n+1} \supset \cdots \supset G_{m+n} = \{e\}$$

となり, G は可解群である．

2.9 5 次以上の交代群の単純性

この節では, 5 次以上交代群が単純群であることを証明する．この定理と Galois 理論を用いると,「5 次以上の方程式では, 一般的な代数的解法が存在しない」という, 有名な Abel と Galois による定理が示される．

定理 2.9.1 $n \geqq 5$ とすると, n 次交代群 A_n は単純群である．

系 2.9.1 $n \geqq 5$ なら S_n は可解群ではない．

系の証明. 上の定理より, $n \geqq 5$ のとき, $[S_n, S_n] = A_n$ が成立する．実際, $[S_n, S_n] \subset A_n$ は交換子群の定義から明らかである．$n \geqq 3$ のとき S_n は非可換だから, $[S_n, S_n] \neq \{e\}$ である．また $[S_n, S_n] \lhd S_n$ より, $[S_n, S_n] \lhd A_n$ となる．A_n が単純群なら, 非自明な正規部分群を持たないので, $[S_n, S_n] = A_n$ となる．

$n \geqq 4$ なら A_n は非可換群だから, $[A_n, A_n]$ は A_n の単位群と異なる正規部分群となる．A_n が単純群なら, $[A_n, A_n] = A_n$ となる．よって, $n \geqq 5$ なら, $[A_n, A_n] = A_n$ となり, S_n は可解群ではない．

注意 2.9.1 G が非可換単純群なら, 上の証明にあるように $[G, G] = G$ であるが, 逆は成立しない．例えば, $p \geqq 5$ となる素数に対して, $[SL_2(\mathbb{Z}/p\mathbb{Z}), SL_2(\mathbb{Z}/p\mathbb{Z})] = SL_2(\mathbb{Z}/p\mathbb{Z})$ である (これを素朴に証明するのは, 少し面倒)．$p \geqq 3$ のとき, $Z(SL_2(\mathbb{Z}/p\mathbb{Z})) = \{\pm E\}$ となるので, $SL_2(\mathbb{Z}/p\mathbb{Z})$ は単純群ではない．$(SL_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3.)$

定理 2.9.1 の証明のために, いくつか補題を用意する．

補題 2.9.1 $n \geqq 3$ とすると, A_n は長さ 3 の巡回置換の集合から生成される．

証明. A_n は偶置換全体だから, $(i, j)(k, l)$ の形の元が長さ 3 の巡回置換の積に書けることを示せばよい．

$\{i, j\} = \{k, l\}$ のとき, $(i, j)(k, l) = e$ であるので, 明らかである．

$|\{i, j\} \cap \{k, l\}| = 1$ のとき, $(i, j)(k, l)$ は長さ 3 の巡回置換になる．

$\{i, j\} \cap \{k, l\} = \emptyset$ のとき, $(i, j)(k, l) = (i, j)(j, k)(j, k)(k, l) = (i, j, k)(j, k, l)$ となり, $(i, j)(k, l)$ は長さ 3 の巡回置換の積になる．

補題 2.9.2 $n \geqq 5$ とすると, 長さ 3 の巡回置換のなす集合は, A_n の中で 1 つの共役類をなす．

証明. n に関する帰納法を用いる．$n = 5$ とする．$\sigma = (1, 2, 3) \in A_5$ とする．

$$\begin{aligned} C_{A_5}(\sigma) &= \{\tau \in A_5 \mid \tau(1, 2, 3)\tau^{-1} = (1, 2, 3)\} \\ &= \{\tau \in A_5 \mid (\tau(1), \tau(2), \tau(3)) = (1, 2, 3)\} =< (1, 2, 3) > \end{aligned}$$

となるので, $|C_{A_5}(\sigma)| = 3$ となり, σ を含む共役類は, $\dfrac{60}{3} = 20$ 個の元からなる．一方, S_5 の中で, 長さ 3 の巡回置換の取り方は, ${}_5C_3 \times 2 = 20$ となるので, 長さ 3 の巡回置換の集合は, A_5 の 1 つの共役類をなす．

$n \geqq 6$ とし, $(i, j, k) \in A_n$ とする．$1 \leqq i, j, k \leqq n - 1$ とすると, 帰納法の仮定から, これは, $(1, 2, 3)$ と共役になる．$(i, j, k) \in A_n$ で, i, j, k のうち 1 つは n に一致するとする．$(i, j, k) = (j, k, i) = (k, i, j)$ なので,

$k = n$ として良い. $n \geqq 6$ なので, i, j, n とは一致しない異なる 2 つの数 p, q を取ることができる. このとき,

$$(p,q,n)(i,j,n)(p,q,n)^{-1} = (i,j,p), \quad (p,q,n) \in A_n$$

となり, p の取り方から $p < n$ である. 帰納法の仮定から, この (i,j,p) は $(1,2,3)$ と共役となるので, 結局 (i,j,n) は $(1,2,3)$ と共役になる.

問 2.9.1　4 次の交代群 A_4 では, 長さ 3 の巡回置換は 2 つの共役類に分かれることを示せ.

定理 2.9.1 の証明　n に関する帰納法を用いる. $\{e\} \neq N \lhd A_n$ として, $N = A_n$ を証明する.

$n = 5$ のとする. N が長さ 3 の巡回置換を含めば, N が正規部分群であることと, 補題 2.9.1, 2.9.2 より, $N = A_5$ である. 5 次の偶置換で, 長さ 3 の巡回置換でないものは, 2 つの異なる互換の積か, 長さ 5 の巡回置換である.

$\sigma = (i_1, i_2)(i_3, i_4) \in N$ とする (i_1, i_2, i_3, i_4 はすべて異なる). i_5 を i_1, i_2, i_3, i_4 とは違う数として, $\tau = (i_1, i_2)(i_4, i_5) \in A_5$ とすると, N が正規部分群であることより,

$$N \ni (\tau\sigma\tau^{-1})\sigma = (i_1,i_2)(i_4,i_5)(i_1,i_2)(i_3,i_4)(i_1,i_2)(i_4,i_5)(i_1,i_2)(i_3,i_4) = (i_3,i_4,i_5)$$

となり, N は長さ 3 の巡回置換を含む. 同様に, i_1, i_2, i_3, i_4, i_5 をすべて異なるとして, $\sigma = (i_1, i_2, i_3, i_4, i_5) \in N$ とすると, $\tau = (i_1, i_2, i_3) \in A_5$ に対して, やはり N が正規部分群であることより,

$$N \ni (\tau\sigma\tau^{-1})\sigma^{-1} = (i_1,i_2,i_3)(i_1,i_2,i_3,i_4,i_5)(i_1,i_3,i_2)(i_1,i_5,i_4,i_3,i_2) = (i_1,i_2,i_4)$$

となり, N は長さ 3 の巡回置換を含む. 従って, $N \neq \{e\}$ なら, $N = A_5$ である.

$n \geqq 6$ として, $n-1$ までは主張が成立すると仮定する. $i = 1, \ldots, n$ に対して,

$$A_n^{(i)} = \{\sigma \in A_n \mid \sigma(i) = i\}$$

とおく. $A_n^{(i)}$ は $n-1$ 次の交代群 A_{n-1} と同型な部分群になり, 帰納法の仮定より単純群である. よって, $N_i = N \cap A_n^{(i)}$ とおくと, N_i は, $A_n^{(i)}$ の正規部分群なので, $N_i = A_n^{(i)}$ となるか, $N_i = \{e\}$ である.

$N_i = A_n^{(i)}$ となる i が存在すれば, N_i は長さ 3 の巡回置換を含むので, N も長さ 3 の巡回置換を含み, $N = A_n$ となり証明は終わる.

すべての i について, $N_i = \{e\}$ であると仮定する. $\sigma \in N$, $\sigma \neq e$ とすると, $\sigma \notin A_n^{(i)}$ $(i = 1, 2, \ldots, n)$ なので, すべての i について, $\sigma(i) \neq i$ とならなければならない. $n \geqq 6$ なので, σ は次のような形をしている. (ここで, $i_3 \in \{1, 2, \ldots n\} \setminus \{1, i_1, i_2\}$ と取る.)

$$\sigma = \begin{pmatrix} 1 & i_1 & i_3 & \cdots \\ i_1 & i_2 & i_4 & \cdots \end{pmatrix} \qquad (1 \neq i_1,\ i_1 \neq i_2,\ i_3 \notin \{1, i_1, i_2\} \text{ で, } \sigma\text{の取り方から, } i_4 \notin \{i_1, i_2, i_3\})$$

$\tau = (1, i_1, i_3) \in A_n$ とする, $n \geqq 6$ なので $j \notin \{1, i_1, i_2, i_3, i_4\}$ となる j をとることができる. このとき, N が正規部分群であることより, $(\tau\sigma\tau^{-1})\sigma^{-1} \in N$ であるが, j の取り方から, $(\tau\sigma\tau^{-1})\sigma^{-1}(j) = j$ となる. これは, $(\tau\sigma\tau^{-1})\sigma^{-1} \in N_j$ を意味し, 仮定より, $(\tau\sigma\tau^{-1})\sigma^{-1} = e$ となる. しかし,

$$(\tau\sigma\tau^{-1})\sigma^{-1}(i_4) = \tau\sigma\tau^{-1}(i_3) = \tau\sigma(i_1) = \tau(i_2) \in \{i_1, i_2\} \quad (i_2 = 1 \text{ なら} \tau(i_2) = i_1, \text{それ以外は}, \tau(i_2) = i_2)$$

となって, 矛盾する. よって, ある i について, $N_i = A_n^{(i)}$ となり, $N = A_n$ である.

問 2.9.2　$n \geqq 3$ とし $\sigma = (1, 2, 3) \in A_n$ とする. $|C_{A_n}(\sigma)|$ を求めよ.

3　環 (主に可換環について)

3.1　基本事項

以下, R は常に単位元を持つ環とする. 最後の節までは, 可換環を主に扱い, 述べてある内容は可換環の初歩的な内容が中心である (特に例は, ほぼ可換環について書いてある). 環の例は, 例 1.2.4 に挙げた以外にも, 下の例のような, $\mathbb{Z}$ に整数係数代数方程式の根を付け加えてできる環も考えることが多い.

例 3.1.1　1. $\mathbb{Z}[\sqrt{-1}] = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Z}\}$ (Gauss の整数環, $\sqrt{-1}$ は $x^2 + 1 = 0$ の根)
2. $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$
3. $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$

整数環や 1 変数多項式環で成り立つ性質が, 一般の (可換) 環でどの程度類似のことが成立するか? という問題意識が, 環の性質を調べる第一歩である.

問 3.1.1　1. $\mathbb{Z}[\sqrt{-1}]^\times = \{\pm 1, \pm\sqrt{-1}\}$ を示せ.
2. $1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]^\times$ を示し, これを利用して, $\left|\mathbb{Z}[\sqrt{2}]^\times\right| = \infty$ を示せ.

定義 3.1.1　R を可換環とし $R \ni a \neq 0$ とする. $0 \neq b \in R$ が存在し, $ab = 0$ となるとき, a, b を R の零因子 (zero divisor) という. 可換環 R は, 零因子を持たないとき, R を整域 (integral domain) という.

R を可換環とし $a, b \in R$ とする. R が整域なら, $ab = 0$ から $a = 0$ または $b = 0$ が従う. このノートでは, 整域という言葉は, 常に可換環に対して用いることにする.

問 3.1.2　1. 例 3.1.1 に挙げた環は, すべて整域になることを示せ.
2. $\mathbb{Z}/n\mathbb{Z}$ が整域である必要十分条件は, n が素数であることである.
3. R を環 a, b, $c \in R$ とする. R が整域かつ $a \neq 0$ なら, $ab = ac \Rightarrow b = c$ が成立する事を示せ.
4. 有限個の元からなる整域は体になることを示せ. (特に $\mathbb{Z}/n\mathbb{Z}$ は整域なら体である.)
5. R を可換環, $R[X]$ を R 上の 1 変数多項式環とするとき, $R[X]$ が整域である条件は, R が整域であることを示せ.
6. R, R' を環, $f : R \to R'$ を写像とし, $f \neq 0$ とする. R' が整域なら, $f(ab) = f(a)f(b)$ から $f(1) = 1$ が従うことを示せ.

定義 3.1.2　R を環, $S \subset R$ とする. S が R の部分環であるとは, 次が成立することを言う.

1. $a, b \in S \Longrightarrow a \pm b \in S,\ ab \in S$
2. $1 \in S$

注意 3.1.1　群とは異なり, 単に演算で閉じているだけでは, 部分環とは言わない. 例えば, 偶数の集合 $2\mathbb{Z}$ は, 和 (差) と積の演算で閉じているが, 1 を含まないので, $\mathbb{Z}$ の部分環とは言わない.

例 3.1.2　$R[X]$ で, R を定数多項式 (次数 0 の多項式) の全体と同一視すると, R は $R[X]$ の部分環である.

定義 3.1.3 (環の直和 (非可換な環でも, 直和は同じ定義))　$R_1, \ldots, R_n$ を可換環とするとき, これらの加法

群としての直積を, $R_1 \oplus \cdots \oplus R_n$ と書く.

$$R_1 \oplus \cdots \oplus R_n = \{(a_1, \ldots, a_n) \mid a_i \in R_i\}$$

和を, 加法群としての直積群の演算で定義し, 積も成分ごとの積として定義する.

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$$
$$(a_1, \ldots, a_n)(b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n)$$

この演算で, $R_1 \oplus \cdots \oplus R_n$ は単位元 $(1, \ldots, 1)$ を持つ可換環になる. これを, $R_1, \ldots, R_n$ の直和という.

注意 3.1.2　上で, 各成分 R_i は $R_1 \oplus \cdots \oplus R_n$ の部分環ではない. 積の単位元が異なるからである. R_i の単位元 1_{R_i} を $R_1 \oplus \cdots \oplus R_n$ の元 $e_i = (0, \ldots, 0, 1_{R_i}, 0, \ldots, 0)$ と同一視すると. これは, 直和の単位元ではないが, $e_i^2 = e_i$ を満たす. このように, 2 乗しても変化しない環の元を, **ベキ等元**という.

問 3.1.3　R_1, R_2 を可換環とするとき, 単元群について, $(R_1 \oplus R_2)^\times \cong R_1^\times \times R_2^\times$ が成立することを示せ. ここで, 右辺は群の直積である.

3.2　イデアルと可換環の準同型定理

環の準同型写像や, 環の同型については, 定義 1.2.4 で定義してあるので, 改めて述べない.

定義 3.2.1　可換環 R の部分集合 I が次の条件を満たすとき, I を R のイデアルであるという.

1. I は R の加法群の部分群である.
2. 任意の $r \in R$, $a \in I$ に対して, $ra \in I$

注意 3.2.1　可換環を考えているので, イデアルに左右の区別はないが, 非可換環では, 「右イデアル」「左イデアル」「両側イデアル」の 3 通りが考えられる. (非可換環では, 上の定義は, 左イデアルの定義になる.) 下の剰余環や準同型定理は, イデアルを「両側イデアル」に置き換えれば, 非可換環でもそのまま成立する.

環論ではイデアルを調べることが, 環の性質の解明につながることが知られているので, 以下, イデアルについての様々な性質を順に述べていく. もともとイデアルは整数環 $\mathbb{Z}$ の素数の役割を担う対象物として, Kummer(クンマー) によって導入された.

例 3.2.1
1. R 及び $\{0\}$ はイデアルである. これらを自明なイデアルという. イデアル I に対して, $I = R$ であるための必要十分条件は, $I \ni 1$ であることに注意する.
2. $\mathbb{Z}$ のイデアルは, $m\mathbb{Z}$, $m \in \mathbb{Z}$ の形をしている.

I を可換環 R のイデアルとする. 加法群としての商群 R/I に積を,

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

で定義する. これは, 代表元の取り方によらず, well–defined である. 実際, $a - a' \in I$, $b - b' \in I$ とすると,

$$ab - a'b' = a(b - b') + (a - a')b' \in I$$

が得られる. この積において, $1 + I$ が積の単位元の性質を持つことは, 明らかである. また, 積の結合律, 交換

律, 分配律は, もとの R のそれから従う. このように, R/I に環の構造を入れたものを, R の I による剰余環という.

定理 3.2.1（可換環の準同型定理） R, R' を可換環とし, $f : R \to R'$ を準同型写像とする. このとき, 次が成立する.

1. $f(R) = \mathrm{Im}(f)$ は R' の部分環である.
2. $f^{-1}(0) = \mathrm{Ker}(f)$ は R のイデアルである.
3. 自然な可換環の同型写像 $\overline{f} : R/\mathrm{Ker}(f) \xrightarrow{\simeq} \mathrm{Im}(f)$ が存在する

証明. 1. $f(1) = 1$ より, $1 \in \mathrm{Im}(f)$ である. $a', b' \in \mathrm{Im}(f)$, $a' = f(a)$, $b' = f(b)$ とすると, $a' + b' = f(a+b) \in \mathrm{Im}(f)$, $a'b' = f(ab) \in \mathrm{Im}(f)$ より, $\mathrm{Im}(f)$ は部分環になる.

2. f は加法群としての準同型写像なので, $\mathrm{Ker}(f)$ は R の加法群の部分群になる. $a \in \mathrm{Ker}(f)$, $r \in R$ に対して, $f(ra) = f(r)f(a) = 0$ なので, $ra \in \mathrm{Ker}(f)$ となり, $\mathrm{Ker}(f)$ は R のイデアルである.

3. 群の準同型定理から, 加法群として自然な同型写像 $\overline{f} : R/\mathrm{Ker}(f) \xrightarrow{\simeq} \mathrm{Im}(f)$ が存在する. これが環の準同型であることは, 剰余環の積の定義から明らかである.

3.3 イデアルの演算と孫子の剰余定理

R を可換環, $S \subset R$ を部分集合とする.

$$RS = (S) = \left\{ \sum_{\text{有限和}} r_i s_i \mid r_i \in R,\, s_i \in S \right\} = \bigcap_{\substack{S \subset I \\ I \text{ はイデアル}}} I$$

とおく. すなわち, (S) は集合 S を含む最小のイデアルである. これを S から生成されたイデアルという.

S が一点集合 $\{a\}$ であるとき, (S) を (a) と書く. このようにただ 1 つの元から生成されるイデアルを, **単項イデアル**, あるいは主イデアル (対応する英語 principal ideal の日本語訳) という.

I, J を可換環 R のイデアルとする. このとき, $I \cap J$ はイデアルになる. また,

$$I + J = \{a + b \mid a \in I,\, b \in J\}$$

もイデアルになる. これを, イデアル I, J の和という.

イデアル I, J に対して, I, J の積を I の元と J の元の積から生成されるイデアルと定義する. 実際には, 次の集合に一致することは, 容易にわかる.

$$IJ = \left\{ \sum a_i b_i \mid a_i \in I,\, b_i \in J \right\}$$

また, $IJ \subset I \cap J$ であることも, 容易にわかる.

問 3.3.1 1. $\mathbb{Z}$ のイデアル I, J で $I \cup J$ がイデアルとなる例, ならない例を挙げよ.

2. $a, b \in \mathbb{Z}$ として, 単項イデアル $(a), (b)$ について, $(a) + (b)$, $(a)(b)$ を求めよ (共に単項イデアルとなるので, その生成元を求めよ).
3. $\mathbb{Z}$ において, $(a)(b) \subsetneqq (a) \cap (b)$ となる例を与えよ.
4. I を可換環 R のイデアルとするとき,

$$\sqrt{I} = \mathrm{rad}(I) = \{x \in R \mid \text{ある自然数 } n \text{ が存在して}, x^n \in I\}$$

も R のイデアルになることを示せ. このように定まる $\sqrt{I}$ をイデアル I の根基 (radical) という. 自明なイデアル $\{0\}$ の根基, $\sqrt{0}$ をべき零根基 (nilradical) という.

可換環 R の非自明なイデアル I, J は $I + J = R$ が成立するとき, **互いに素である**という.

問 3.3.2　1. $\mathbb{Z}$ のイデアル $m\mathbb{Z}$ と $n\mathbb{Z}$ が互いに素であることと, m, n が互いに素 (最大公約数が 1) な整数であることは, 同値であることを示せ.

2. 可換環 R のイデアル I, J が互いに素なら, $IJ = I \cap J$ が成立することを示せ.

互いに素なイデアルに対しては, 次の定理が成立する. これは, 孫子算経という 5 世紀頃の中国の算術書に由来する.

定理 3.3.1 (Chinese Remainder Theorem (中国式剰余定理, あるいは孫子の剰余定理))　R を可換環とし, $I_1, \ldots, I_n$ を R の互いに素なイデアルとする. すなわち, $i \neq j$ なら, $I_i + I_j = R$ がすべての i, j について成立しているとする. このとき, 次が成立する.

1. $I_i + \bigcap_{j \neq i} I_j = R$
2. 任意の $a_1, \ldots, a_n \in R$ に対して, $a \in R$ が存在して, $a - a_i \in I_i$ がすべての i について成立する.
3. $I = \bigcap_{i}^{n} I_i$ とすると, $R/I \cong R/I_1 \oplus \cdots \oplus R/I_n$.

証明. 1. i を固定する. すべての j $(\neq i)$ に対して, $I_i + I_j = R$ なので, j ごとに $u_j + v_j = 1$, $u_j \in I_i, v_j \in I_j$ となる u_j, v_j が取れる. このとき,

$$\begin{aligned} 1 &= (u_1 + v_1)(u_2 + v_2)\cdots(u_{i-1} + v_{i-1})(u_{i+1} + v_{i+1})\cdots(u_n + v_n) \\ &= u_1u_2\cdots u_n + u_1\cdots u_{n-1}v_n + \cdots + v_1v_2\cdots v_{n-1}u_n + v_1v_2\cdots v_n \\ &= x_i + y_i \end{aligned}$$

となる. 上では, 最後の項 (u_k を因子に含まない項) を y_i とし, それ以外の項 (u_k を因子に含む項) の和を x_i とおいた. すなわち,

$$\begin{aligned} x_i &= u_1u_2\cdots u_n + u_1\cdots u_{n-1}v_n + \cdots + v_1v_2\cdots v_{n-1}u_n \\ y_i &= v_1v_2\cdots v_n \end{aligned}$$

上の和において, y_i は $v_j \in I_j$ より, $y_i \in \bigcap_{j \neq i} I_j$ であり, x_i は $u_j \in I_i$ より, $x_i \in I_i$ となる. 従って, $1 = x_i + y_i$, $x_i \in I_i$, $y_i \in \bigcap_{j \neq i} I_j$ となる x_i, y_i が取れる. $r \in R$ を任意の元とすると, この式の両辺に r を掛けることにより, $r = rx_i + ry_i$, $rx_i \in I_i$, $ry_i \in \bigcap_{j \neq i} I_j$ となり, $R = I_i + \bigcap_{i \neq j} I_j$ である.

2. 1 の証明で定めた $y_i \in \bigcap_{j \neq i} I_j$, $i = 1, \ldots, n$ を考える. $a_1, \ldots, a_n \in R$ に対し, $a = a_1y_1 + \cdots + a_ny_n \in R$ とおく. このとき,

$$\begin{aligned} a - a_i &= a_1y_1 + \cdots + a_{i-1}y_{i-1} + a_i(y_i - 1) + a_{i+1}y_{i+1} + \cdots a_ny_n \\ &= a_1y_1 + \cdots + a_{i-1}y_{i-1} - a_ix_i + a_{i+1}y_{i+1} + \cdots a_ny_n \end{aligned}$$

となる．$x_i \in I_i$ なので，$-a_i x_i \in I_i$ である．また，$j \neq i$ に対して，$y_j \in \bigcap_{k \neq j} I_k \subset I_i$ なので，$a_j y_j \in I_i$ となる．よって，$a - a_i \in I_i$ がすべての i について成立する．

3. $f_i : R \to R/I_i$ を自然な射影とし，

$$f : R \to R/I_1 \oplus \cdots \oplus R/I_n, \quad f(a) = (f_1(a), \ldots, f_n(a))$$

とする．f が環の準同型写像になることは，明らかである．2 より，f は全射になる．実際，$(\overline{a_1}, \ldots, \overline{a_n})$ に対して，$a_1, \ldots a_n$ をそれぞれの R での代表元とすると，2 で定まる a を取れば，$f(a) = (\overline{a_1}, \ldots, \overline{a_n})$ である．

$$\mathrm{Ker}(f) = \{a \in R \mid f_i(a) = \overline{0},\ \forall i = 1, \ldots, n\} = \{a \in R \mid a \in I_i,\ \forall i = 1, \ldots, n\} = \bigcap_{i=1}^{n} I_i = I$$

なので，準同型定理より，証明を得る．

例 3.3.1（Euler の関数）　孫子の剰余定理より，$I_1, \ldots, I_m$ が全て互いに素であるなら，単元群に対して，次の群の直積分解が成立する (問 3.1.3)．

$$(R/(I_1 \cap \cdots \cap I_m))^\times \cong (R/I_1)^\times \times \cdots \times (R/I_m)^\times$$

$R = \mathbb{Z}$ に対して，これを適用する．$n \in N$ とし，n の素因数分解を $n = p_1^{r_1} \cdots p_m^{r_m}$ とする．$I_i = p_i^{r_i}\mathbb{Z}$ とすると，$I_1, \ldots, I_m$ は互いに素なイデアルになる (問 3.3.2)．また，$I_1 \cap \cdots \cap I_m = n\mathbb{Z}$ である．よって，群としての直積分解

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{r_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_m^{r_m}\mathbb{Z})^\times$$

を得る．数 $1, 2, \ldots, p_k^{r_k}$ の中で，p_k の倍数は，$p_k, 2p_k, \ldots, p_k^{r_k-1} \cdot p_k$ であるので，その個数は $p_k^{r_k-1}$ 個ある．これら以外が，$\mathbb{Z}/p_k^{r_k}\mathbb{Z}$ の単元の代表元のすべてなので，$|(\mathbb{Z}/p_k^{r_k}\mathbb{Z})^\times| = p_k^{r_k} - p_k^{r_k-1}$ となる．従って，

$$\begin{aligned}\varphi(n) &= |(\mathbb{Z}/n\mathbb{Z})^\times| = |(\mathbb{Z}/p_1^{r_1}\mathbb{Z})^\times| \cdots |(\mathbb{Z}/p_m^{r_m}\mathbb{Z})^\times| = (p_1^{r_1} - p_1^{r_1-1}) \cdots (p_n^{r_n} - p_m^{r_m-1}) \\ &= p_1^{r_1}\left(1 - \frac{1}{p_1}\right) \cdots p_m^{r_m}\left(1 - \frac{1}{p_m}\right) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_m}\right)\end{aligned}$$

を得る (例 1.2.5. の 2)．

3.4　極大イデアルと素イデアル

可換環 R のイデアル $\mathfrak{m}$ が極大イデアル (maximal ideal) であるとは，$\mathfrak{m}$ を真に含むイデアルは，R となることを言う．ここで，R 自身は極大イデアルとは言わないことに注意する．

定理 3.4.1　可換環 R のイデアル $\mathfrak{m}$ に対して，次の条件は同値である．

1. $\mathfrak{m}$ は極大イデアルである．
2. 剰余環 $R/\mathfrak{m}$ が体になる．

証明.　$1 \Rightarrow 2$. $a \in R$ として，$R/\mathfrak{m}$ で $\overline{a} \neq 0$ とする．これは，$a \notin \mathfrak{m}$ と同値である．$\mathfrak{m}$ は，極大イデアルであるので，$a, \mathfrak{m}$ から生成されるイデアル $(a, \mathfrak{m})$ は R と一致する．よって，$r \in R$ と $m \in \mathfrak{m}$ が存在して，$ra + m = 1$ となる．このとき，$R/\mathfrak{m}$ で $\overline{ra} = 1$ なので，$\overline{a}$ は可逆になり，$R/\mathfrak{m}$ は体である．

$2 \Rightarrow 1$. $I \supsetneqq \mathfrak{m}$ をイデアルとする. $a \in I \setminus \mathfrak{m}$ をとると, $R/\mathfrak{m} \ni \overline{a} \neq 0$ である. $R/\mathfrak{m}$ は体なので, $r \in R$ が存在して, $\overline{ra} = 1$ となる. このとき, $ar - 1 = m$, $m \in \mathfrak{m}$ となり, $ar + m = 1$ である. $a \in I$, $m \in \mathfrak{m} \subset I$ なので, $ar + m \in I$ となり, $1 \in I$ となる. このとき, $I = R$ となるから, $\mathfrak{m}$ を真に含むイデアルは R と一致し, $\mathfrak{m}$ は極大イデアルになる.

定理 3.4.2　R を可換環, I を R の自明でないイデアルとすると, I を含む極大イデアルが存在する.

証明.

$$\mathcal{I} = \{ J \subsetneqq R \mid J \text{ は } I \text{ を含むイデアル} \}$$

とおく. 集合の包含関係で順序を入れると, $\mathcal{I}$ は帰納的順序集合になることを示す.

全順序部分集合 $\mathcal{I}' \subset \mathcal{I}$ に対して,

$$J' = \bigcup_{J \in \mathcal{I}'} J$$

とおくと, J' は, $\mathcal{I}'$ の上界になる.

実際, $J' \supset I$ は明らかである. また, 任意の $\mathcal{I}'$ の元 J に対して, $1 \notin J$ なので, $1 \notin J'$ である. よって, $J' \neq R$ である. また, $a, b \in J'$ とすると, $a \in J_1$, $b \in J_2$ となる $J_1, J_2 \in \mathcal{I}'$ が存在する. J_1, J_2 のうち, 順序の大きい方を J'' とすると, $a, b \in J''$ で, J'' はイデアルだから, $a + b \in J'' \subset J'$ である. この状況のもとで, $r \in R$ に対して, $ra \in J_1 \subset J'$ でもある. よって, J' は R の真のイデアルであり, $\mathcal{I}'$ の上界である.

ここで, Zorn の補題 (定理 1.3.1) を用いると, $\mathcal{I}$ には極大元 $\mathfrak{m}$ が存在する. $\mathfrak{m} \in \mathcal{I}$ なので, $\mathfrak{m}$ は R の真のイデアルである. $\mathfrak{m} \subset J$ となる真のイデアル J が存在すると, $I \subset J$ となるので, $J \in \mathcal{I}$ となり, $\mathcal{I}$ での $\mathfrak{m}$ の極大性から $\mathfrak{m} = J$ となり, $\mathfrak{m}$ は R の極大イデアルである.

定義 3.4.1　可換環 R のイデアル $\mathfrak{p}$ が素イデアル (prime ideal) であるとは, $\mathfrak{p} \neq R$ かつ $a, b \in R$ に対して,

$$ab \in \mathfrak{p} \Longrightarrow a \in \mathfrak{p} \text{ または } b \in \mathfrak{p}$$

が成立することを言う.

素イデアルは, 整数での素数 p の持つ性質のひとつ,

$$a, b \in \mathbb{Z},\ ab \text{ が } p \text{ の倍数} \Longrightarrow a \text{ が } p \text{ の倍数, または } b \text{ が } p \text{ の倍数.}$$

のイデアルへの一般化である.

命題 3.4.1　R を可換環とする.

1. $\mathfrak{p}$ が R の素イデアルであるための必要十分条件は, $a, b \in R$ に対して,

   $$a \notin \mathfrak{p} \text{ かつ } b \notin \mathfrak{p} \Longrightarrow ab \notin \mathfrak{p}$$

   が成立することである.
2. $\mathfrak{p}$ が R の素イデアルであるこの必要十分条件は, 剰余環 $R/\mathfrak{p}$ が整域であることである.

証明. 1. これは定義 3.4.1 の条件の対偶を述べたものである.

2. 1. より, $\mathfrak{p}$ が素イデアルなら, $a, b \in R \setminus \mathfrak{p}$ とすると, $ab \notin \mathfrak{p}$ となる. これは, $\overline{a}, \overline{b} \in R/\mathfrak{p}$ に対して, $\overline{a} \neq 0$ かつ $\overline{b} \neq 0$ なら $\overline{a}\overline{b} \neq 0$ が成立することであるから, $R/\mathfrak{p}$ は整域である. 逆に, $R/\mathfrak{p}$ が整域なら, この議論を逆にたどれば, $a \notin \mathfrak{p}$ かつ $b \notin \mathfrak{p}$ なら $ab \notin \mathfrak{p}$ が成立する.

上の命題 3.4.1, 2. より特に次が成立する.

命題 3.4.2　極大イデアルは素イデアルである.

上の命題の逆は成立しない.

例 3.4.1　$\mathbb{C}$ 上の 2 変数多項式環 $\mathbb{C}[X, Y]$ と 1 変数多項式環 $\mathbb{C}[X]$ を考える. $\varphi : \mathbb{C}[X, Y] \to \mathbb{C}[X]$ を, $(\varphi(f))(X) = f(X, 0)$, $f \in \mathbb{C}[X, Y]$ で定義すると, φ は環の全射準同型写像である. 環の準同型定理より, $\mathbb{C}[X] \cong \mathbb{C}[X, Y]/\mathrm{Ker}(\varphi)$ であるが, $\mathbb{C}[X]$ は整域であるので, $\mathrm{Ker}(\varphi)$ は素イデアルである. しかし $\mathbb{C}[X]$ は体ではないので, $\mathrm{Ker}(\varphi)$ は極大イデアルではない.

定理 3.4.3　$f : R \to R'$ を可換環の準同型写像とする. $R' \supset \mathfrak{p}$ を素イデアルとすると $f^{-1}(\mathfrak{p})$ は R の素イデアルになる.

証明.　$f^{-1}(\mathfrak{p})$ は R のイデアルになる. 実際, $a, b \in f^{-1}(\mathfrak{p})$ なら, $f(a + b) = f(a) + f(b) \in \mathfrak{p}$ より $a + b \in f^{-1}(\mathfrak{p})$ であり, $r \in R$ に対して, $f(ra) = f(r)f(a) \in \mathfrak{p}$ となり, $ra \in f^{-1}(\mathfrak{p})$ である.

$a, b \in R$, $ab \in f^{-1}(\mathfrak{p})$ とすると, $f(a)f(b) = f(ab) \in \mathfrak{p}$ となる. $\mathfrak{p}$ は素イデアルなので, $f(a) \in \mathfrak{p}$ または $f(b) \in \mathfrak{p}$ である. よって, $a \in f^{-1}(\mathfrak{p})$ または $b \in f^{-1}(\mathfrak{p})$ となり, $f^{-1}(\mathfrak{p})$ は素イデアルである.

3.5　Euclid(ユークリッド) 整域, 単項イデアル整域

$\mathbb{Z}$ や, 体上の 1 変数多項式環においては,「素因数分解の一意性」が成立する. これを証明する際に利用する性質を公理化したものが, Euclid 整域である. すなわち, 可換環において, 何らかの形の「大きさ」が定義され, 割り算で「割る数より小さい余りが決まる」という性質が,「素因数分解の一意性」の根拠となっている.

イデアルも 3.2 節で可換環の準同型写像の核 (kernel) と捉えたが, もともとは,「素因数分解」を環に一般化するために導入された. 例えば, $\mathbb{Z}[\sqrt{-5}]$ においては,

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

と 2 通りの積に書けるが, ここに現れる因子, 2, 3, $1 \pm \sqrt{-5}$ は $\mathbb{Z}[\sqrt{-5}]$ において単元以外の約数を持たない (例えば, $ab = 2$, $a, b \in \mathbb{Z}[\sqrt{-5}]$ とすると, a または b が ± 1 になる). すなわち, $\mathbb{Z}[\sqrt{-5}]$ は, 素朴な意味での「一意的」な積への分解ができないのである.

この節と次の節では,「素因数分解」を問題にする. この節では, 環 R は可換環で常に整域 (零因子を持たない) であるとする.

定義 3.5.1　R を整域とし, N を整列集合 (全順序集合で, 任意の空でない部分集合が最小元を持つ集合, 例えば, 自然数全体) とする. R から N への写像 $\varphi : R \to N$ で, 次の性質を満たすものが存在するとき, R をユークリッド整域であるという. ($>$ は N に入っている順序関係とする.)

1. $x \neq 0 \Longrightarrow \varphi(x) > \varphi(0)$
2. $b \in R$, $b \neq 0$ なら任意の $a \in R$ に対して, $a = bq + r$, $\varphi(r) < \varphi(b)$ となる q, $r \in R$ が存在する.

例 3.5.1　1. $\mathbb{Z}$ は, $N = \mathbb{N} \cup \{0\}$, $\varphi(x) = |x|$ としてユークリッド整域である.

2. K を体とし, $K[X]$ を K 上の 1 変数多項式環とする. $N = \{-\infty, 0\} \cup \mathbb{N}$ とする ($-\infty < 0 < 1 < \cdots$ で N には順序を入れる). $f \in K[X]$ に対して, $\varphi(f) = \deg f$ と定義する. ただし, $\deg 0 = -\infty$ とする. 1 変数多項式環の割り算の計算より, $K[X]$ はユークリッド整域になる.

問 3.5.1　Gauss の整数環 $\mathbb{Z}[\sqrt{-1}] = \{x + y\sqrt{-1} \mid x, y \in \mathbb{Z}\}$ を考える. $\varphi(x + y\sqrt{-1}) = x^2 + y^2$ とすると, これはユークリッド整域になることを示せ. ($a, b \in \mathbb{Z}[\sqrt{-1}]$ に対して, a/b を複素数として計算して, これにもっとも近い点 $q \in \mathbb{Z}[\sqrt{-1}]$ をとり, $r = a - bq$ とおけば, 定義の条件を満たす.)

定義 3.5.2（単項イデアル整域, PID）　R を整域とする. R の任意のイデアルが単項イデアルであるとき, すなわち I を R のイデアルとすると, $a \in R$ が存在して $I = (a)$ となるとき, R を単項イデアル整域 (英語で Principal ideal domain, 略して PID) という.

Principal ideal は直訳すると主イデアルなので, 単項イデアル整域は主イデアル整域ともいう.

命題 3.5.1　ユークリッド整域は単項イデアル整域である.

証明.　R をユークリッド整域, N を全順序集合で, $\varphi : R \to N$ を定義 3.5.1 にある写像とする. R の自明なイデアルは, それぞれ, (0), (1) と書けるので, 単項イデアルである. I を R の非自明なイデアルとする. N は整列集合だから, $\varphi(I) \setminus \{\varphi(0)\} \subset N$ には最小元 n が存在する. $a \in I$ を $\varphi(a) = n$ となる元とする. 定義 3.5.1, 1. より, $a \neq 0$ となることに注意する. このとき, $I = (a)$ が成立する.

実際, $a \in I$ だから $(a) \subset I$ が従う. 逆に $b \in I$ とする. 定義 3.5.1, 2. から, $q, r \in R$ が存在して, $b = aq + r$, $\varphi(r) < \varphi(a)$ となる. このとき, $r = b - aq \in I$ となるが, $\varphi(a)$ の最小性から, $\varphi(r) = \varphi(0)$ となり, 定義 3.5.1, 1. より $r = 0$ となる. よって, $b = aq \in (a)$ となり. $I \subset (a)$ を得る.

注意 3.5.1　上の命題の逆は成立しない. 例えば, $\mathbb{Z}\left[\dfrac{1+\sqrt{-19}}{2}\right]$ は PID だがユークリッド整域ではない (B 節を参照). 情報科学演習で $e^{\sqrt{163}\pi}$ が整数値にとても近いという話をしたが (http://www.math.u-ryukyu.ac.jp/~suga/joho/2016/12/node5.html), これは $\mathbb{Z}\left[\dfrac{1+\sqrt{-163}}{2}\right]$ が PID であることと関係している. ちなみに $\mathbb{Z}\left[\dfrac{1+\sqrt{-163}}{2}\right]$ もユークリッド整域ではない. (このように, 一見無関係に見える, ある種の環の性質と指数関数の特殊値が結びついてしまうところが, 数学の面白いところである.)

また, ある環が PID であることを証明するのも, それほど易しいことではない. ユークリッド整域になることは十分条件だが必要条件ではないので, 上の例のような場合には, 別の手段で PID であることを示さなければならない.

3.6　素元分解整域

この節でも, R は可換環で整域であるとする. 一般の整域においても約数・倍数の関係は同様に定義される. 次の定義の, 素元・既約元の言葉遣いは, 多項式環を例として考えた方が, わかりやすいと思う.

定義 3.6.1　R を整域とする.

1. $a = bc$, b, $c \in R$ となるとき, b, c は a の約数, a は b, c の倍数という. このとき, $b|a$, $c|a$ と書く.
2. $a|b$ かつ $b|a$ であるとき, a と b は同伴であるという. このとき, $a \approx b$ と書く.
3. $a = bc$, $b, c \in R$ と a を積に分解したとき, b, c のどちらかが常に単元になるとき, すなわち, 単元以外に約数を持たないとき, a を既約元という.
4. $p \in R$ が素元であるとは, $p \neq 0$ かつ $p \notin R^\times$ で,

$$p|ab \Longrightarrow p|a \text{ または } p|b$$

が成立することを言う.

問 3.6.1　0 は任意の元の倍数, 単元は任意の元の約数であることを述べよ.

命題 3.6.1　R を整域とする.

1. 0 でない元 a, $b \in R$ が同伴であるなら, ある単元 $\varepsilon \in R^\times$ が存在して, $b = \varepsilon a$ となる. 特に, 同伴であるという条件は, 同値関係である.
2. 素元は既約元である.

証明. 1. 条件より, $a|b$ なので, $b = ac$, $c \in R$ と書ける. 同様に $b|a$ なので, $a = bc'$, $c' \in R$ と書ける. よって $b = bcc'$ となり, $b(1 - cc') = 0$ である. R は整域なので, $1 - cc' = 0$ となり, $c \in R^\times$ となり, 前半の証明を得る. 同伴が同値関係であることは, このことと, $R^\times$ が積に関して群であることから従う.

2. $p \in R$ が素元であるとする. $p = ab$, a, $b \in R$ とする. $p|p$ かつ p は素元なので, $p|a$ または, $p|b$ が成立する. $p|a$ と仮定すると, ある c が存在して, $a = pc$ となる. このとき, $p = ab = pbc$ となり, $p(1 - bc) = 0$ を得る. R は整域で $p \neq 0$ なので, $bc = 1$ となって, b は単元になる. $p|b$ のときも同様に考えると a が単元になる. よって, p は既約元である.

上の命題の 2. の逆は成立しない.

問 3.6.2　1. 既約元と同伴な元は既約元であり, 素元と同伴な元は素元であることを示せ.

2. 2, 3, $1 \pm \sqrt{-5}$ は $\mathbb{Z}[\sqrt{-5}]$ において既約元であることを示せ.
3. $\mathbb{Z}[\sqrt{-5}]$ において, $2 \not| (1 + \sqrt{-5})$ かつ $2 \not| (1 - \sqrt{-5})$ を示せ. $(2|6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ なので, このことから, 2 は $\mathbb{Z}[\sqrt{-5}]$ で素元ではない.)

命題 3.6.2　R を整域とし, $p \in R$ とする. p が素元である必要十分条件は, p から生成される単項イデアル (p) が素イデアルであることである.

証明. $x \in (p)$ であることと, $p|x$ は同値であることに注意する. よって, p が素元と仮定すると, $ab \in (p)$ なら $a \in (p)$ または $b \in (p)$ が成立するので, (p) は素イデアルである. 逆に (p) が素イデアルであるとする. $p|ab$ とすると, $ab \in (p)$ である. (p) は素イデアルであるから, $a \in (p)$ または $b \in (p)$ となり, $p|a$ または $p|b$ が成立する.

これまでに, $\mathbb{Z}[\sqrt{-5}]$ で何度か例示したことは, 上の言葉遣いをすると, 「一般の整域において既約元による因数分解は一意性が成り立たない.」ということになる. しかし, 素元を用いれば, もし素因数分解ができれば

一意的であることが証明できる. $\mathbb{Z}[\sqrt{-5}]$ は, 残念ながら, 素朴な意味での素因数分解はできない[*3].

補題 3.6.1　R を整域とし, $p, q \in R$ を素元とする. このとき, $q \in (p)$ ならば, $p \approx q$ で, 特に $(p) = (q)$ が成立する.

証明.　$q \in (p)$ だから, $r \in R$ が存在して, $q = pr$ となる. q は素元なので, 命題 3.6.1, 2. より, 既約元である. (p) は素イデアルなので, p は単元ではない. よって, q の既約性より, $r \in R^\times$ となり, $p \approx q$ である. このとき, $(p) = (q)$ であることは, 容易に分かる.

定理 3.6.1（整域における素元分解の一意性）　R を整域とし, $a \in R$ が素元の積に分解できたとすると, その分解は本質的に一意的である. すなわち, $p_1, \ldots, p_r$, $q_1, \ldots, q_s$ を R の素元とし,

$$a = p_1 \cdots p_r = q_1 \cdots q_s$$

であるとすると, $r = s$ であり, 積の順を入れかえると $p_1 \approx q_1, \ldots, p_r \approx q_r$ が成立する.

証明.　$r \leqq s$ と仮定して良い. $q_1 \cdots q_s = p_1 \cdots p_r$ より, $p_1 | q_1 \cdots q_s$ である. p_1 は素元なので, ある j が存在して, $p_1 | q_j$ である. 積の順を入れかえることにより, $j = 1$ として良い. p_1, q_1 は素元なので, 上の補題から, $p_1 \approx q_1$ となり, $q_1 = \varepsilon_1 p_1$ を得る. よって, $p_1 \cdots p_r = \varepsilon_1 p_1 q_2 \cdots q_s$ となる. R は整域なので ($ab = ac, a \neq 0 \Rightarrow b = c$ が成立するので), $p_2 \cdots p_r = \varepsilon_1 q_2 \cdots q_s$ となる. p_2 に対して, 上と同じことを実行すると, $q_2 = \varepsilon_2 p_2$, $\varepsilon_2 \in R^\times$ を得る. この操作を p_r まで実行すると, $q_i = \varepsilon_i p_i$, $\varepsilon_i \in R^\times$, $i = 1, \ldots, r$ となる. このとき, $1 = \varepsilon_1 \cdots \varepsilon_r q_{r+1} \cdots q_s$ となり, $q_{r+1}, \ldots, q_s \in R^\times$ であり, これらは素元ではありえない. よって, $r = s$ かつ $p_i \approx q_i$, $i = 1, \ldots, r$ である.

定義 3.6.2（素元分解整域, 一意分解整域, UFD）　R を整域とする. 任意の $a \in R \setminus \{0\}$ が素元の積に分解できるとき, R を素元分解整域, あるいは一意分解整域 (Unique factorization domain, 略して UFD) という.

上の定理 3.6.1 より, UFD での素元分解は常に一意的である. また, UFD では, 既約元と素元の概念が一致する. 再三例示してきた $\mathbb{Z}[\sqrt{-5}]$ は, UFD ではなく, 既約元が素元にならない.

命題 3.6.3　UFD では, 既約元は素元である.

証明.　R を UFD とし, $a \in R$, $(a \neq 0)$ を既約元とする. R は UFD なので, $a = p_1 \cdots p_r$ と素元の積に分解できる. a は既約元なので, このような分解があると, ある 1 つの p_i 以外は単元である. 従って, ある素元 p を用いて, $a = \varepsilon p$, $\varepsilon \in R^\times$ となり, a は素元である.

UFD なら素元分解の一意性があるが, そのような環の重要な例として, PID と, UFD 上の多項式環がある. 後者の証明は, 少し準備が必要なので次節で与え, ここでは前者だけを証明する.

定理 3.6.2　PID は UFD である.

証明.　R を PID とし, $a \in R (a \neq 0)$ とする. a が素元なら素元分解はすでに終わっているので, 素元ではないとする. 定理 3.4.2 より, R の中で, イデアル (a) を含む極大イデアル $\mathfrak{m}_1$ が存在する. R は PID なので, $p_1 \in R$ が存在して, $\mathfrak{m}_1 = (p_1)$ である. $R/\mathfrak{m}_1$ は整域 (実際には体) なので, p_1 は素元である (命題 3.6.2).

[*3] $\mathbb{Z}[\sqrt{-5}]$ において, 任意のイデアルは素イデアルの積で一意的に書ける」という定理は証明できる. 歴史的には, イデアル, 素イデアルは, この形の定理のために導入された.

$a \in (a) \subset (p_1)$ なので, $a_1 \in R$ が存在して, $a = a_1 p_1$ である. a_1 が素元なら, これが a の素元の積への分解を与える. そうでなければ, a_1 に対して同じ操作をすると, 素元 p_2 と $a_2 \in R$ が存在して, $a = a_2 p_1 p_2$ となる. 以下, この操作を繰り返したとき, それが有限回で終わることを示す.

この操作で現れる R の元の列, $a_1, a_2, \ldots,$ から作られる単項イデアルの列を考えると. $a = a_1 p_1$, $a_1 = a_2 p_2$, $a_2 = a_3 p_3, \ldots$ なので, $(a_1) \subset (a_2) \subset (a_3) \subset \cdots$ が成立する. ここで, $I = \bigcup_{i=1}^{\infty} (a_i)$ を考えると, これは R のイデアルになることが, 簡単に確かめられる. R は PID なので, ある $b \in R$ が存在して, $I = (b)$ となる. $b \in I$ で, I の作り方から, ある n が存在して, $b \in (a_n)$ である. このとき, $(b) \subset (a_n)$ となり, $I = (a_n)$ となる. よって, $(a_n) = (a_{n+1}) = \cdots$ を得る. これは, 上の操作法に従うと, (a_n) を真に含む極大イデアルが存在しないことになる. よって, (a_n) は極大イデアルで, a_n は素元であり, $a_n = a_{n+1} = \cdots$ を得る. すなわち, 上の操作は有限回で終了する.

注意 3.6.1　定理 3.4.2 では, 極大イデアルの存在に Zorn の補題を用いているが, PID に関しては, 上の証明の後半と同じ考え方で, Zorn の補題を用いずとも極大イデアルの存在が証明できる.

これまでの結果から,

ユークリッド整域 $\Longrightarrow$ PID $\Longrightarrow$ UFD

が示された. 従って, よく知られているように, $\mathbb{Z}$ や体 K 上の 1 変数多項式環 $K[X]$ は PID であり, UFD である. また, Gauss の整数環 $\mathbb{Z}[\sqrt{-1}]$ もユークリッド整域なので, PID であり, さらに UFD でもある.

注意 3.6.2　ここで, 言葉遣いを少し整理しておく. 自然数 p が素数であることの通常の定義は, これまでに述べた環での言葉では, p が整数環 $\mathbb{Z}$ の既約元であるという定義になる. これが $\mathbb{Z}$ の素元になることは, $\mathbb{Z}$ が UFD であることと上の命題から従う. すなわち, 整数環において, 素数 ($\mathbb{Z}$ の既約元) が素元であることは自明ではなく, 証明を要することなのである.

なおこれまでの証明では, PID という概念を用いて $\mathbb{Z}$ において素数が素元であることを示しているが, (PID を使わない) 直接的な証明も可能である.

定理 3.6.2 の逆は成立しない. 例えば, 体 K 上の 2 変数多項式環 $K[X, Y]$ は, 次節で示すように UFD である. しかし, 次の説明で見るように, 一般的に, これは PID ではない.

例 3.6.1 ($\mathbb{C}[X, Y]$ が PID ではないことの説明.)　$\mathbb{C}[X, Y]$ のイデアル I に対して, $\mathcal{V}(I) = \{(x, y) \in \mathbb{C}^2 \mid g(x, y) = 0,\ \forall g \in I\}$ とおく. すなわち, 方程式 $g(x, y) = 0$ が定める曲線の集合を, g をイデアルの元を全て動かしたときの共通部分である. これをイデアル I に対する代数的集合という. I が $f(X, Y) \in \mathbb{C}[X, Y]$ から生成される単項イデアル $I = (f)$ であるとすると, 容易に分かるように, これから定まる代数的集合は, $\mathcal{V}((f)) = \{(x, y) \in \mathbb{C}^2 \mid f(x, y) = 0\}$ となる. すなわち, 1 つの方程式 $f(x, y) = 0$ で定まる曲線に一致する. 一方, $\mathbb{C}[X, Y]$ の 2 つの単項式 X, Y から生成されるイデアル, $I = (X, Y)$ を考える. このとき, $\mathcal{V}((X, Y))$ は原点のみからなる 1 点集合 $\{(0, 0)\} \subset \mathbb{C}^2$ となる. しかし, $f \in \mathbb{C}[X, Y]$ に対して, $f(x, y) = 0$ が 1 点集合となることはありえない (無限集合になるか, 空集合 (f が 0 でない定数の場合) である. 定理 1.1.1 を考えよ) ので, (X, Y) は単項イデアルではない.

ここで, この節の内容から導かれる PID の性質についてまとめた命題を挙げておく. 代数方程式を考える際に, 体上の 1 変数多項式環でよく用いられる性質である.

命題 3.6.4（PID の性質のまとめ） R を PID とする.

1. R の素イデアルは, 既約元から生成される単項イデアルである.
2. R の素イデアルは, 極大イデアルである.

特に, R のひとつの既約元から生成される単項イデアルは, R の極大イデアルになる.

証明. 1. I を R の素イデアルとし, p を生成元とすると, 命題 3.6.2 より, p は素元であり, 特に既約元である. PID R は UFD なので既約元は素元であり, それから生成されるイデアルは, 素イデアルである.

2. $I=(p)$ を R の素イデアルとし, $J=(q)$ を I を含む R のイデアルとする. $p\in J$ なので, $r\in R$ が存在して, $p=qr$ となる. このとき, $p|qr$ であるが, p が素元であるので, $p|q$ または $p|r$ である. $p|q$ なら, p, q は互いに同伴となるので, $I=(p)=(q)=J$ となる. $p|r$ とすると, $r=ps,\ s\in R$ となるが, このとき, $p=pqs$ となり, R が整域であることより $qs=1$ を得る. よって, q は可逆元となり $J=R$ となる. これらのことから, I は極大イデアルである.

注意 3.6.3 上で, PID なら任意の素イデアルは極大イデアルであることを示したが, 逆は成立しない. 例えば, これまでの例に現れている $\mathbb{Z}[\sqrt{-5}]$ では, 任意の素イデアルは極大イデアルであることが示されるが, これが PID でないことは, 既に述べたとおりである.

3.7 局所化 (分数化) と商体

環の極大イデアルに対する剰余環は体になる. これとは別に, 環の元の分数を考えることによって体を作る方法がある. 整数環 $\mathbb{Z}$ から有理数体 $\mathbb{Q}$ を作る内容を公理化するのである. 分数の和と積を考えると, 分数の分母に現れる集合は, 「0 でない」という条件より少し弱くできて,「積で閉じている」でも分数計算が可能であることがわかる. すなわち, この分母の条件を少し弱くして分数を考えるのが, 局所化と呼ばれるもので, 「0 でない」のを全て分母に許容するのが, 商体と呼ばれるものである.

なお,「局所化」という日本語 (英語でも localization という) は, 「分数」とは無関係であるように見える.「局所化」という言葉遣いは, 下の例で, 素イデアル (の補集合) から定まる分数化に対して通常用いられる. なぜこのような言葉遣いをするのかは, 代数幾何学や代数的整数論を詳しく勉強しないとわからないので, 知りたい人は, 適当な参考書を参照していただきたい.

定義 3.7.1 R を可換環とする. R の部分集合 $R\supset S$ が積閉集合 (あるいは乗法的閉集合, multiplicatively closed set) であるとは, 次を満たすことを言う.

1. $a,b\in S\Longrightarrow ab\in S$
2. $1\in S,\quad 0\notin S$

例 3.7.1 R を可換環とするとき, 次は積閉集合である.

1. $x\in R$ とし, x が零因子でないとしたとき, $\{\ x^n\mid n=0,1,2,\dots\ \}$
2. $S=\{a\in R\mid a\neq 0,\ a$ は零因子でない $\}$. 特に R が整域であるとき, $S=R\setminus\{0\}$. (R が整域でなければ, $R\setminus\{0\}$ は, 定義の 2. の $0\notin S$ が問題となる).
3. $\mathfrak{p}$ を R の素イデアルとするとき, $R\setminus\mathfrak{p}$ (命題 3.4.1, 1.)

問 3.7.1　上の例の集合が積閉集合になることを確かめよ.

R を可換環, S を R の積閉集合であるとして, 直積集合 $R \times S$ に次で同値関係を入れる. 分数において「約分しても同じ分数」であることを環の場合に拡張したものであるが,「割り算」をするわけにはいかないので, 下のような定義になる.

$$(a_1, s_1) \sim (a_2, s_2) \Longleftrightarrow \text{ある } s \in S \text{ が存在して, } (a_1 s_2 - a_2 s_1)s = 0, \quad (a_i, s_i) \in R \times S, \ (i = 1, 2)$$

定義から, $s \in S$ に対して, $(s, s) \sim (1, 1)$ となることに注意する.

問 3.7.2　上で定めた $\sim$ が $R \times S$ の同値関係になることを示せ.

$R \times S/\sim$ を R_S あるいは $S^{-1}R$ と書く. $(a, s) \in R \times S$ とし (a, s) を代表元とする R_S の元を (a/s) と書くことにする. R_S に次の規則で和と積を定義する (分数の和と積の規則).

$$(a_1/s_1) + (a_2/s_2) = ((a_1 s_2 + a_2 s_1)/s_1 s_2)$$
$$(a_1/s_1)(a_2/s_2) = (a_1 a_2/s_1 s_2), \qquad (a_i/s_i) \in R_S, \ (i = 1, 2)$$

命題 3.7.1　上の和と積の規則は well–defined で, R_S は零元 $(0/1)$, 単位元 $(1/1)$ を持つ可換環になる.

証明. 和が well–defined であることだけを示す (残りは下の問). $(a_1/s_1) = (a_1'/s_1')$, $(a_2/s_2) = (a_2'/s_2')$ とする. このとき, $s,\ t \in S$ が存在して, $(a_1 s_1' - a_1' s_1)s = 0$, $(a_2 s_2' - a_2' s_2)t = 0$ となる. このとき,

$$\{(a_1 s_2 + a_2 s_1)s_1' s_2' - (a_1' s_2' + a_2' s_1')s_1 s_2\}\, st = (a_1 s_1' - a_1' s_1)s(s_2 s_2' t) + (a_2 s_2' - a_2' s_2)t(s_1 s_1' s) = 0$$

となるので, $(a_1/s_1) + (a_2/s_2) = (a_1'/s_1') + (a_2'/s_2')$ が成立する.

問 3.7.3　上の定理の証明の省略された部分を埋めよ.

上で定義された R_S を R の S による商環あるいは局所化という (商環と剰余環という 2 つの言葉が出てきているが, その違いに注意すること). $\mathfrak{p}$ を R の素イデアルとして, $S = R \setminus \mathfrak{p}$ であるときには, (記号に統一性が無いが) $R_{S \setminus \mathfrak{p}}$ とは書かずに, $R_{\mathfrak{p}}$ と書く.

例 3.7.2　$R = \mathbb{Z}$ とし, $p \in \mathbb{Z}$ を素数とする. (p) を p が生成する素イデアル, $S = \mathbb{Z} \setminus (p)$ とする. $\mathbb{Z}$ の S による局所化を $\mathbb{Z}_p$ と書き, p–進整数環という. 整数論では重要な環である.「p–進」という言葉遣いをする理由を解説するのは大変なので, 興味のある人は, 代数的整数論の専門書を参照していただきたい.

$$\mathbb{Z}_p = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, \ b \neq 0, \ (b, p) = 1 \right\}$$

R_S の積と和の定義, および零元と積の単位元の定義から, 写像

$$i : R \ni a \mapsto (a/1) \in R_S$$

は, 環の準同型写像になる. これによる S の像を考える. $s \in S$ に対して, $i(s) = (s/1)$ は, R_S の中で積に関する逆元 $(1/s)$ を持つ. すなわち, $i(S) \subset (R_S)^\times$ である. R_S は S の積に関する逆元を付け加えた環であるとも言える.

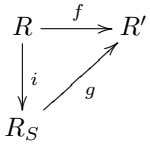
i の核を考えると, $R \times S$ で $(a, 1) \sim (0, 1)$ となる条件を書き下せば,

$$\mathrm{Ker}(i) = \{a \in R \mid s \in S \text{ が存在して, } as = 0\}$$

となる．よって, S が零因子を含まなければ, i は単射となり, R と $i(R)$ を同一視することにより, R は R_S の部分環であると思うことにする．

R の積閉集合 S に対して, S の積における逆元を付け加えて環を作るという操作において, R_S が最も一般的な環であることを, 次の定理は述べている．

定理 3.7.1（商環の普遍性 (universality)） R を可換環, $S \subset R$ を積閉集合とし, $i : R \to R_S$ を上で定めた自然な準同型写像とする．R' を別の可換環, $f : R \to R'$ を環の準同型写像で, $f(S) \subset (R')^\times$ となるものとする．このとき, 環の準同型写像 $g : R_S \to R'$ で, $f = g \circ i$ となるものが, 一意的に存在する．



証明. $(x/s) \in R_S,\ x \in R,\ s \in S$ に対して, $g((x/s)) = f(x)f(s)^{-1}$ で定義する ($f(S) \in (R')^\times$ だから, $f(s)$ は R' の単元であることに注意する). まず, これが well–defined であることに注意する．R_S において, $(x/s) = (x'/s')$ であるとすると, $t \in S$ が存在して, $(xs'-x's)t = 0$ となる．このとき, $(f(x)f(s')-f(x')f(s))f(t) = 0$ となるが, $f(t)$ は R' の単元だから $f(x)f(s') = f(x')f(s)$ となり, $f(x)f(s)^{-1} = f(x')f(s')^{-1}$ を得る．

g が環の準同型写像になることは, f が準同型写像であることから従い, $f = g \circ i$ となることは, 定義から明らかである．また, 上のような性質を持つ g が存在すれば, $g((x/s)) = g((x/1)(1/s)) = g((x/1)(s/1)^{-1}) = f(x)f(s)^{-1}$ でなければならないので, これから一意性が従う．

S として, R の非零因子全体の集合を取ったとき, $R_S = Q(R)$ と書いて, R の全商環という．R が整域なら, $S = R \setminus \{0\}$ となり, 全商環は体になる．これを整域 R の (全) 商体という．

例 3.7.3

1. $R = \mathbb{Z}$ ならその全商体は $\mathbb{Q}$ になる．
2. K を体として $R = K[X_1, \ldots, X_n]$ を K 上の n 変数多項式環とする．全商体の定義から, R の全商体は 0 でない元を分母にした元からなる体である．これを $K(X_1, \ldots, X_n)$ と書き, K の n 変数の有理関数体という．

$$K(X_1, \ldots, X_n) = \left\{ \frac{f(X_1, \ldots, X_n)}{g(X_1, \ldots, X_n)} \mid f, g \in K[X_1, \ldots, X_n],\ g \neq 0 \right\}$$

全商体を導入することにより, 次の定理が証明できるようになる．

定理 3.7.2 R を UFD とすると, R 上の多項式環 $R[X]$ も UFD である．

この定理を仮定すると, n に関する帰納法で次の系が証明できる．実際, $n = 1$ のときには, $K[X]$ はユークリッド整域なので UFD であり, $n \geqq 2$ のときは, $K[X_1, \ldots, X_n] = K[X_1, \ldots, X_{n-1}][X_n]$ を利用すれば良い．

系 3.7.1 K を体とすると K 上の n 変数多項式環 $K[X_1, \ldots, X_n]$ は UFD である．

定理 3.7.2 を証明するために, 少し準備をする．

以下では, R は UFD とする．よって, 任意の $a \in R$, $(a \neq 0)$ は素元の積に (単元倍を除いて) 一意的に書くことができる．また UFD では, 素元と既約元の概念が一致することも, 思い出しておく．今後, 素因数分解を考えるときには, 単元倍だけの差異は無視して考える．

素元の積への一意的な分解を利用すると, $a, b \in R$ に対して, a, b の最大公約数が (単元倍を除いて) 一意的に決まる. 通常の整数で考えることを, 素元の積への分解を利用して実行すれば良いのである.

K を R の全商体とする. R は整域なので, 上で述べたように, 自然に K の部分環であるとみなす ($r \in R$ は $(r/1) \in K$ と見る). $f(X) \in R[X]$ もこの埋め込みを利用して, $K[X]$ の元と見る.

$f(X) = a_n X^n + \cdots + a_1 X + a_0 \in R[X]$ は, $a_0, \ldots, a_n$ の最大公約数が 1 であるとき, すなわち, $a_0, \ldots, a_n$ の全てを割り切る素元が存在しないとき, $f(X)$ は原始的 (primitive) であるという.

補題 3.7.1 R を UFD, $R \subset K$ を R の全商体とする. $f(X) \in K[X]$ に対して, $c \in K$ と原始的な多項式 $f_0(X) \in R[X]$ が存在して, $f(X) = cf_0(X)$ と書ける. c は R の単元倍を除いて, $f(X)$ から一意的に定まる.

証明.

$$f(X) = c_n X^n + c_{n-1} X^{n-1} + \cdots + c_1 X + c_0 \in K[X]$$

とする. $c_i \in K$ だから, $c_i = \dfrac{a_i}{b_i}$, $a_i, b_i \in R$ と書ける. 各項の係数の分母をまとめると,

$$f(X) = \frac{1}{b_n \cdots b_0} \left\{ (a_n b_{n-1} \cdots b_0) X^n + (a_{n-1} b_n b_{n-2} \cdots a_0) X^{n-1} + \cdots + (a_1 b_n \cdots b_2 b_0) X + (a_0 b_n \cdots b_1) \right\}$$

となる. ここで, 左辺の括弧の中の多項式の係数に注目する.

$$a_n b_{n-1} \cdots b_0, \quad a_{n-1} b_n b_{n-2}, \ \ldots\ , a_1 b_n \cdots b_2 b_0, \quad a_0 b_n \cdots b_1$$

の最大公約数を a とおき, $b = b_n \cdots b_0 \in R$ とする. 括弧の中の X^i の係数から, $a_i b_n \cdots b_{i+1} b_{i-1} \cdots b_0 = a c_i'$ で, c_i' を定めると, a は左辺の約数であるから, $c_i' \in R$ である. $f_0(X) = c_n' X^n + c_{n-1}' X^{n-1} + \cdots + c_1' X + c_0'$, $c = \dfrac{a}{b}$ とおくと, $f(X) = cf_0(X)$ で, $f_0(X) \in R[X]$ は原始的である.

$f(X)$ が $R[X]$ の原始的な多項式 $h(X)$ と $c' \in K$ を用いて, $f(X) = c'h(X)$ と別の書き方ができたとする. $c' = \dfrac{a'}{b'}$, $a', b' \in R$ とする. 約分をすることにより, 上で定めた a, b および a', b' の最大公約数は 1 であるとして良い.

$$f(X) = \frac{a}{b} f_0(X) = \frac{a'}{b'} h(X)$$

となる. これより分母を払えば,

$$b' a f_0(X) = b a' h(X)$$

となる. よって, a は $ba'h(X)$ の係数の公約数になるが, a と b の最大公約数は 1 で, $h(X)$ は原始的なので, $a | a'$ となる. 逆のことを考えると, $a' | a$ となり, 命題 3.6.1, 1. より, $a \approx a'$ となる. b, b' についても同様の考察ができ, $b \approx b'$ となるので, c, c' は単元倍を除いて一致する.

定義 3.7.2 R を UFD, K を R の全商体とする. $f(X) \in K[X]$ に対して, 上の命題 3.7.1 で定まる c を f の内容 (content) といい, $I(f)$ で表す (I はドイツ語の Inhalt が由来).

補題 3.7.2 (Gauss の補題) 上の定義の仮定の元で, 次が成立する.

1. $f(X), g(X) \in R[X]$ が原始的であれば, $f(X)g(X)$ も原始的である.
2. $f(X), g(X) \in K[X]$ とすると, $I(f)I(g)$ と $I(fg)$ は R の単元倍を除いて一致する.

証明. 1.

$$f(X) = a_m X^m + a_{m-1} X^{m-1} + \cdots + a_0$$
$$g(X) = b_n X^n + b_{n-1} X^{n-1} + \cdots + b_0$$

とする. R は UFD だから, $f(X)g(X)$ のすべての係数を約数であるような素元が存在しないことを示せばよい. $p \in R$ を素元とする. $f(X)$, $g(X)$ は原始的だから, $a_m, \ldots, a_0$, $b_n, \ldots, b_0$ それぞれの中に, p が約数とならない元が存在する. $p \nmid a_i$ となる最小の i と $p \nmid b_j$ となる最小の j をとる. このとき, $f(X)g(X)$ の X^{i+j} の係数は,

$$(a_0 b_{i+j} + a_1 b_{i+j-1} + \cdots + a_{i-1} b_{j+1}) + a_i b_j + (a_{i+1} b_{j-1} + \cdots + a_{i+j} b_0)$$

となるが, $a_0, \ldots, a_{i-1}$ は p の倍数, $b_0, \ldots, b_{j-1}$ は p の倍数だから, 上の式の括弧で括られた部分は p の倍数である. しかし, a_i, b_j はともに p を約数に持たず, p が素元であることから, $a_i b_j$ も p を約数に持たない. よって上の式は, 全体として p を約数に持たない. p は任意の素元として取れるので, 結局 $f(X)g(X)$ の係数の公約数であるような素元は存在しない.

2. $f(X) = I(f) f_0(X)$, $g(X) = I(g) g_0(X)$ だから, 両辺の積を取ると $f(X)g(X) = I(f)I(g) f_0(X) g_0(X)$ である. 1. より, $f_0(X) g_0(X)$ も原始的であるから, 補題 3.7.1 より, $I(fg)$ と $I(f)I(g)$ は R の単元倍を除いて, 一致する.

命題 3.7.2 R を UFD とし, K を R の全商体とする. R は K の部分環なので, $f(X) \in R[X]$ は自然に (f の係数の元を K の元だと思って) $K[X]$ の元であると思える. このとき, $f(X)$ が $R[X]$ で既約なら, $K[X]$ でも既約である.

証明. f が $K[X]$ で, $f(X) = g(X)h(X)$, $g, h \in K[X]$ と分解されたとする. 両辺の内容を考えると, 補題 3.7.2, 2. より, $I(g)I(h) = \varepsilon I(f)$, $\varepsilon \in R^\times$ となる. 一方, I の定義から, $f \in R[X]$ なら $I(f) \in R$ であり, $R[X]$ の原始的な多項式, f_0, g_0, h_0 が存在して, $f(X) = I(f) f_0(X)$, $g(X) = I(g) g_0(X)$, $h(X) = I(h) h_0(X)$ となる. よって,

$$\begin{aligned} f(X) &= I(f) f_0(X) \\ &= g(X)h(X) = I(g)I(h) g_0(X) h_0(X) = \varepsilon I(f) g_0(X) h_0(X) \end{aligned}$$

となる. $I(f)$, $\varepsilon \in R$ だから, $\varepsilon I(f) g_0$, $h_0 \in R[X]$ となるが, これは, f の $R[X]$ での因数分解を与えている. f は $R[X]$ で既約であるので, g_0 か h_0 のいずれかは, 次数が 0 となり, これより, f の $K[X]$ での既約性が従う.

注意 3.7.1

1. R を UFD とし, $f(X) \in R[X]$ が $f(X) = g(X)h(X)$, $g(X), h(X) \in K[X]$ と $K[X]$ の元で因数分解できたとする. このとき, 上の証明から, $g(X)$, $h(X)$ の係数を定数倍して $g(X), h(X) \in R[X]$ と取れることが示されている.
2. $R = \mathbb{Z}$, $K = \mathbb{Q}$ のとき, 上の命題は高校の数学で, 暗に利用されている. 例えば, $f(X) = X^3 + 3X + 1$ が $\mathbb{Q}$ 上で既約であることを確かめるのに, $f(\pm 1) \neq 0$ だけを確かめている. しかし, 冷静に考えてみると, これは $\mathbb{Z}$ 上の既約性を確かめているだけに過ぎない. しかし, 上の命題から, $f(X)$ は $\mathbb{Q}$ 上の多項式と見ても既約であることが分かる.

補題 3.7.3　R を UFD とする.

1. $p \in R$ を素元とすると, p は $R[X]$ でも素元である.
2. $f(X) \in R[X]$ を既約な原始的多項式とすると, $f(X)$ は $R[X]$ の素元である.

証明.　1. $f(X), g(X) \in R[X]$ とし, $p \mid f(X)g(X)$ とする. 内容と原始的な多項式を用いて, $f(X) = I(f)f_0(X)$, $g(X) = I(g)g_0(X)$ と書く. このとき, $f(X)g(X) = I(f)I(g)f_0(X)g_0(X)$ で, $I(f), I(g) \in R$ となる. ガウスの補題 (補題 3.7.2) より, $f_0(X)g_0(X)$ は原始的である. よって, $p \mid I(f)I(g)$ を得る. p は R の素元なので, $p \mid I(f)$ または $p \mid I(g)$ となるが, これに応じて, $p \mid f(X)$ または $p \mid g(X)$ となり, p は $R[X]$ の素元である.

2. $f(X) \mid g(X)h(X)$, $g(X), h(X) \in R[X]$ とする. K を R の全商体として, この約数関係を $K[X]$ で考える. $f(X)$ の $K[X]$ で既約性 (命題 3.7.2) と $K[X]$ が UFD であることより, $f(X)$ は $K[X]$ で素元である (命題 3.6.3). よって, $K[X]$ で $f(X) \mid g(X)$ または $f(X) \mid h(X)$ が成立する. 例えば, $f(X) | g(X)$ であるとし, $g(X) = f(X)q(X)$, $q(X) \in K[X]$ とする. 両辺の内容を考えると, $I(g) = \varepsilon I(f)I(q)$, $\varepsilon \in R^\times$ となるが, f が原始的なので, $I(f) = 1$ であり, $g \in R[X]$ より, $I(g) \in R$ となる. よって, $I(q) \in R$ となるので $q(X) \in R[X]$ となり, $R[X]$ で $f(X) \mid g(X)$ となる. $f(X) \mid h(X)$ の場合も同様なので, 結局 $R[X]$ で $f(X) \mid g(X)$ または $f(X) \mid h(X)$ が成立し, f は素元である.

定理 3.7.2 の証明.　$f(X) \in R[X]$ が素元の積に書けることを示す. $f(X) = I(f)f_0(X)$ で, $f_0(X) \in R[X]$ は原始的である. R は UFD で $I(f) \in R$ だから, R の素元 $p_1, \ldots, p_r$ が存在して, $I(f) = p_1 \cdots p_r$ となる. K を R の全商体とするすると, $K[X]$ は UFD である. $f_0(X) \in K[X]$ と見て素元分解すると, $K[X]$ の既約な多項式 $q_1, \ldots, q_s$ が存在して, $f_0(X) = q_1(X) \cdots q_s(X)$ となる. 両辺の内容を考えると,

$$I(f_0) = 1 = I(q_1) \cdots I(q_s), \qquad I(q_i) \in K \ (i = 1, \ldots, s)$$

を得る. 内容の定義から, $\dfrac{q_i(X)}{I(q_i)} \in R[X]$ で, かつこの多項式は原始的でさらに既約である. すなわち, これらは $R[X]$ の素元である. 上の式から,

$$f(X) = I(f)f_0(X) = p_1 \cdots p_r \frac{q_1(X)}{I(q_1)} \cdots \frac{q_s(X)}{I(q_s)}$$

は $f(X)$ の $R[X]$ での素元分解を与える.

上の証明から, 次の系を得る.

系 3.7.2　R を UFD とすると, $R[X]$ の素元は R の素元 p もしくは, 既約かつ原始的な多項式の 2 種類に限られる.

3.8　環上の加群

M を加法群 (演算を加法として, 単位元を 0 で表す可換群) とし, R を (単位元を持つ) 環とする (一般的に非可換とする). 環が加法群 M に作用するという状況が, 数学において多く現れるので, その定義と性質の基本を, ここで述べておく.

定義 3.8.1　M が左 R–加群 (left R–module) であるとは, R の M への左からの作用が存在することを言う. ここで, R の左からの作用は次を満たす写像, $R \times M \to M,\ (r, m) \mapsto rm$ である.

1. $(rr')m = r(r'm),\ 1m = m, \quad r, r' \in R, \quad m \in M$
2. $(r + r')m = rm + r'm,\ r(m + m') = rm + rm', \quad r, r' \in R, \quad m, m' \in M$

右 R–加群も同様に定義される.

問 3.8.1　1. 右 R–加群の定義を書き下せ.

2. 左 R–加群の公理から, $0a = 0$, $(-1)a = -a$ $(\forall a \in M)$ を導け.

注意 3.8.1　R が可換環ならば, 左加群, 右加群の区別をする必要はない (積の可換性から, 右加群の公理と左加群の公理が同値になる) が, 非可換環なら異なる概念となる.

両側加群という概念もあり (その場合, 左からの作用と右からの作用が異なる環になることもある), 重要ではあるが, それについてはここでは述べない.

例 3.8.1　1. M を任意の加法群とする. $a \in M$, $n \in \mathbb{Z}$ に対して $na = \begin{cases} a + a + \cdots + a & (n \geqq 0) \\ -a - a - \cdots - a & (n < 0) \end{cases}$ ($|n|$ 項の和または差) と定義すると, M は $\mathbb{Z}$–加群になる. すなわち, 任意の加法群は $\mathbb{Z}$–加群である.

2. R 自身, 左右の積を作用だと思えば, 左右の R–加群である.
3. R を可換環とし, $M_n(R)$ を R 上の行列環とする. $R^n = \left\{ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \mid a_i \in R \right\}$ を R を成分とする n 項列ベクトルのなす加法群とすると, 通常の行列の積で R^n は左 $M_n(R)$–加群である. 同様に, $R_n = \{(a_1, \ldots, a_n) \mid a_i \in R\}$ を n 項の行ベクトル全体がなす加法群とすると, R_n は行列の積で, 右 $M_n(R)$–加群である.

以下では, 左 R–加群について述べるが, 右 R–加群についても同様のことが成立する.

定義 3.8.2　M を左 R–加群とし, $N \subset M$ とする. 次が成立するとき, N を部分 R–加群 (R–submodule, R の作用が明らかな場合は, 単に部分加群) という.

1. N は加法群として, M の部分群
2. $RN \subset N$

他の代数系の用語と同じように, $\{0\}$, M は, 自明な部分加群と呼ばれる. R が可換環であるとき, R 自身を R–加群と見たとき, その部分加群とはイデアルのことである.

$N \subset M$ を部分 R–加群とする. M が可換群なので, N は群として正規部分群である. よって, 商群 M/N を考えることができる. $a + N \in M/N$ と $r \in R$ に対して, $ra + N \in M/N$ は $a + N$ の代表元 a の取り方によらず, well–defined である. 実際, $a + N = a' + N$ とすると, $ra - ra' = r(a - a')$ で $a - a' \in N$ より $r(a - a') \in N$ となり, $ra + N = ra' + N$ である. この R の作用により, M/N は左 R–加群になる. これを, 商加群という. R を可換環とすると, R のイデアル I は部分加群である. R 自身も R–加群なので, 剰余環 R/I は商加群として R–加群である.

定義 3.8.3　M, N を左 R–加群とし, $f : M \to N$ を写像とする. f が R–加群の準同型写像 (略して, R–準同型写像あるいは, R–線形写像) であるとは, 次を満たすことを言う.

1. $f(a+b) = f(a) + f(b), \qquad a, b \in M$
2. $f(ra) = rf(a), \qquad r \in R,\ a \in M$

さらに f が全単射であるとき, f を R–同型写像であるという.

$f : M \to N$ を R–加群の準同型写像とすると,

$$\mathrm{Im}(f) = f(M) = \{f(a) \mid a \in M\} \subset N$$
$$\mathrm{Ker}(f) = f^{-1}(0) = \{a \in M \mid f(a) = 0\} \subset M$$

はそれぞれ, N, M の部分加群となる.

定理 3.8.1（**R–加群の準同型定理**）　M, N を左 R–加群とし, $f : M \to N$ を R–準同型写像とすると, f から誘導される自然な R–同型写像

$$\overline{f} : M/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$$

が存在する.

定理の証明は, 群や環の準同型定理の証明と同じである.

問 3.8.2　上の定理の証明を書け.

定義 3.8.4（**直積と直和**）　$\{M_i\}_{i \in I}$ を左 R–加群の族とする.

1. 直積

   $$\prod_{i \in I} M_i = \{(a_i)_{i \in I} \mid a_i \in M_i\}$$

   を集合としての直積とし, 和と R の作用は成分ごとに定義する. すなわち,

   $$(a_i)_{i \in I} + (b_i)_{i \in I} = (a_i + b_i)_{i \in I}, \qquad r(a_i)_{i \in I} = (ra_i)_{i \in I}$$

   これにより, 直積集合 $\prod_{i \in I} M_i$ は左 R-加群となる. これを R-加群 $\{M_i\}_{i \in I}$ の直積という.
2. 直和は直積の中の次の部分集合として定義される.

   $$\bigoplus_{i \in I} M_i = \{(a_i)_{i \in I} \in \prod_{i \in I} M_i \mid \text{有限個の } i \text{ を除いて } a_i = 0\}$$

   これが, $\prod_{i \in I} M_i$ の部分加群になることは容易に確かめられる.

上で, I が有限集合であれば, 直積と直和は同じものになるが, I が無限集合のときは, 一般に $\bigoplus_{i \in I} M_i \subsetneqq \prod_{i \in I} M_i$ である. $l \in \mathbb{N}$ に対して, R^l は, R 自身を R–加群と見たものの l 個の直和を表すことにする.

定義 3.8.5　M を左 R–加群とし $U \subset M$ を部分集合とする.

$$< U >= \left\{ \sum_{\text{有限和}} r_i u_i \mid r_i \in R,\ u_i \in U \right\}$$

は部分 R–加群となる. $< U >$ を U から生成された部分加群という.

定義 3.8.6　M を左 R–加群とし, $U \subset M$ を部分集合とする.

1. $u_1, \ldots, u_n$ が R 上 1 次独立 (あるいは線形独立) とは,

   $$r_1 u_1 + r_2 u_2 + \cdots + r_n u_n = 0 \Longrightarrow r_1 = \cdots = r_n = 0$$

   が成り立つことを言う.
2. U が M の基底であるとは, 次が成立することという.
   (a)　$< U >= M$
   (b)　U の任意の有限部分集合は, 1 次独立である.
3. M が基底を持つとき, 自由 R–加群 (free R–module) という.

注意 3.8.2　環上の加群においては, 基底を持たないことの方が通常である. 例えば, $n \in \mathbb{N}$ として, $\mathbb{Z}/n\mathbb{Z}$ を $\mathbb{Z}$–加群と見ると, これに基底は存在しない. $\{\overline{1}\}$ は生成元集合であるが, 1 次独立性が成り立たない ($n \cdot \overline{1} = \overline{0}$). もちろん, $\mathbb{Z}/n\mathbb{Z}$–加群と見る場合には, $\{\overline{1}\}$ は基底になる. よって, M だけでなくスカラーの集合 R の性質も重要になる.

例 3.8.2　R^l は自由 R–加群である. $e_i = (\delta_{ij})_j \in R^l$ (第 i 成分だけが 1 で残りの成分は 0) が基底になる. これを R^l の標準基底という.

定義 3.8.7**（ベクトル空間）**　K を体 (斜体でも良い) としたときに, K–加群の M のことを K 上のベクトル空間という. K が斜体であるなら, 左加群, 右加群に応じて, 左ベクトル空間, 右ベクトル空間という.

定理 3.8.2　ベクトル空間には, 基底が存在する. ベクトル空間の基底の濃度は, 取り方によらず一定である.

証明.　M を体 K 上のベクトル空間とし, M の次のような部分集合の族を考える.

$$\mathcal{B} = \{ B \subset M \mid B \text{ の任意の有限部分集合は, 1 次独立な元からなる } \}$$

$\mathcal{B}$ は, 集合の包含関係で順序を入れたときに, 帰納的順序集合となる. 実際, $\mathcal{B}' \subset \mathcal{B}$ を全順序部分集合とする. このとき,

$$B' = \bigcup_{B \in \mathcal{B}'} B$$

は $\mathcal{B}'$ の上界になる. なぜなら, B' の任意の有限部分集合 S をとると, $S \subset B$ となる $B \in \mathcal{B}'$ が取れるので, S の元は 1 次独立だからである.

Zorn の補題より, $\mathcal{B}$ には極大元 E が存在する. E は M の基底になる. 実際, $E \in \mathcal{B}$ だから, E の有限部分集合は, 1 次独立である. さらに, 任意の $x \notin E$, $x \neq 0$ に対して, $E \cup \{x\} \notin \mathcal{B}$ だから, ある有限集合 $S \subset E$ が存在して, $S \cup \{x\}$ は 1 次独立な集合ではない. よって

$$ax + \sum_{s \in S} a_s s = 0, \quad a,\ a_s \in K$$

となる非自明な線形関係が存在する．$a = 0$ とすると, S の元の 1 次独立性から $a_s = 0, \forall s \in S$ となって, 自明な線形関係になる．よって, $a \neq 0$ となり,

$$x = -\frac{1}{a} \sum_{s \in S} a_s s$$

となる．このことから, M の任意の元は, E の元の線形結合で表示できるのがわかる．

無限次元の場合の基底の濃度が一定であることは, この講義では必要ないので, 証明は省略する．有限次元の場合の基底の個数の一意性は, 線形代数学の教科書を参照すること．

定義 3.8.8　K を体, V を K 上のベクトル空間とするとき, 上で定まる V の基底の濃度を V の K 上の次元といい, $\dim_K V$ で表す．

4 体と Galois 理論

4.1 可換体の基本, 体の拡大

以下, K, L, M は特に断らない限り, 可換体を表すとする. 体という言葉は, 特に断らない限り, 可換体を意味する. K という文字を用いるのは, ドイツ語の Körper(身体という意味) に由来し, 体という日本語もそれに由来する.

$|K| = \infty$ のとき, K を無限体 (例: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$), $|K| < \infty$ のとき有限体 (例: $\mathbb{Z}/p\mathbb{Z}$) という. これら以外の例としては, $\mathbb{Q}$ に適当な方程式の根を付加した体, 例えば, 次のような体がある.

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

あるいは, 体上の有理関数体 ($K[X]$ の全商体)

$$K(X) = \left\{ \frac{f(X)}{g(X)} \mid f(X), g(X) \in K[X], g(X) \neq 0 \right\}$$

を念頭において読んでほしい.

問 4.1.1 $\mathbb{Q}(\sqrt{2})$ が体になることを示せ.

体は, 可換環の特別な場合であるので, “準同型写像”, “同型” などの言葉は, 可換環と同じ定義を用いる. 環ではなく体であるということから生じる差異として, 次がある.

- 体 K のイデアルは, 自明なイデアル, K と $\{0\}$ しかない. 従って, 体でイデアルを考えることはない.
- 上のことから, $f : K \to L$ を体の準同型写像とすると, $f \neq 0$ なら単射である. $f \neq 0$ のとき, $f(K)$ を K と同一視し f は埋め込みであると考えることが多い.
- 体には直和という概念がない. 環の直和を体に適用して作られるものは, 環ではあるが, 通常は体にはならない.

K を体とする. 環の準同型写像 $f : \mathbb{Z} \to K$ を $f(n) = n \cdot 1$ で定める. 右辺の意味は, $n \geqq 0$ なら, K の乗法の単位元 1 を n 個加えたもので, $n < 0$ なら -1 を $|n|$ 個加えたものとする. $f(\mathbb{Z})$ は, 体 K の中の部分環になるので整域である. 準同型定理から, $\mathrm{Ker}(f)$ は $\mathbb{Z}$ の素イデアルとなり, $\{0\}$ もしくは, 素数 p が存在して $p\mathbb{Z}$ のいずれかになる.

定義 4.1.1 体 K に対して, 上で決まるイデアルが $\{0\}$ のとき, K の標数は 0 であるという. $p\mathbb{Z}$ のとき, K の標数は p であるという. K の標数を $\mathrm{char}(K)$ と書く. 標数が 0 でない体のことを, 正標数の体ともいう.

例 4.1.1 $\mathrm{char}(\mathbb{Q}) = \mathrm{char}(\mathbb{R}) = \mathrm{char}(\mathbb{C}) = 0$, $\mathrm{char}(\mathbb{Z}/p\mathbb{Z}) = p$, ($p$ は素数)

問 4.1.2 $\mathrm{char}(K) = p > 0$ とすると, $a, b \in K$ に対して, $(a + b)^p = a^p + b^p$ が成立することを示せ. 特に, $a \mapsto a^p$ は K の自己準同型写像である.

K を体とする. $\mathrm{char}(K) = 0$ とすると, 上で定義した, f により, $\mathbb{Z}$ が K の部分環として埋め込まれている. 従って, $\mathbb{Z}$ の全商環 $\mathbb{Q}$ が K の部分環として埋め込まれてる (定理 3.7.1). 同様に $\mathrm{char}(K) = p > 0$ とすると, 上の f に対して, $f(\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$ が K の部分環として埋め込まれている. ここにあげた部分環は, 実際には体をなす. これを**素体**という. K に含まれる (包含関係で) 最小の部分体である.

K, L を体として $K \subset L$ であるとき, K を L の部分体, L を K の拡大体という. このとき, L/K という記号も用いる. K, M, L を体として, $K \subset M \subset L$ が成立するとき, M を拡大 L/K の中間体という. 体の拡大を, 集合の包含記号 $K \subset M \subset L$ ではなく, 下のように書くことも多い. この際には, 下にある体が上の体に含まれており, 線分は包含関係を表す.

$$\begin{array}{c} L \\ | \\ M \\ | \\ K \end{array}$$

L/K を体の拡大とする. $f(X) \in K[X]$ は自然に L 上の多項式であると思うことができる. 埋め込み写像 $\sigma : K \to L$ が明示されている場合, これを $\sigma(f(X))$ とも書く.

K が L の部分体であるとき, L は K の元の積をスカラー倍だと思う作用により, K 上のベクトル空間とみなすことができる. 特に, L には K 上のベクトル空間としての基底が存在する (定理 3.8.2).

定義 4.1.2 K が L の部分体であるとき, L を K 上のベクトル空間と見たときの次元, $\dim_K L$ を L の K に対する拡大次数といい. $[L : K]$ で表す. $[L : K] < \infty$ のとき有限次拡大, $[L : K] = \infty$ のとき, 無限次拡大という.

例 4.1.2 $[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{R} : \mathbb{Q}] = \infty$. $\mathbb{R}$ の $\mathbb{Q}$ 上の基底の集合は, Lebesgue 非可測集合の例として有名である.

命題 4.1.1 $K \subset M \subset L$ を体の拡大の列とする. このとき

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

証明. 有限次拡大のときに示すが, 無限次拡大でも同様である. $u_1, \ldots, u_m \in L$ を L の M 上の基底とし, $v_1, \ldots, v_n \in M$ を M の K 上の基底とするとき, $\{u_i v_j\}_{\substack{1 \leqq i \leqq m \\ 1 \leqq j \leqq n}}$ が L の K 上の基底になることを示せばよい. $a \in L$ とすると, $a_1, \ldots, a_m \in M$ が存在して, $a = \sum_{i=1}^{m} a_i u_i$ と書ける. $a_i \in M$ なので, $b_{ij} \in K$ が存在して, $a_i = \sum_{j=1}^{n} b_{ij} v_j$ となる. 従って, $a = \sum_{i,j} b_{ij} u_i v_j$ となるので, L の元は, $\{u_i v_j\}$ の K–線形結合になる. $c_{ij} \in K$ に対して, $\sum_{i,j} c_{ij} u_i v_j = 0$ が成立すると仮定する. $\sum_{i,j} c_{ij} u_i v_j = \sum_i (\sum_j c_{ij} v_j) u_i = 0$ となるが, 括弧の部分は M の元で, $\{u_i\}$ が L の M 上の基底であるので, $\sum_j c_{ij} v_j = 0,\ i = 1, \ldots, m$ となる. ここで, $\{v_j\}$ が M の K 上の基底であることを用いると, $c_{ij} = 0,\ (\forall i, j)$ を得るので, $\{u_i v_j\}$ は線形独立な元の集合である.

K を体とするとき,

$$\mathrm{Aut}(K) = \{ f : K \to K \mid f \text{ は同型写像 } \}$$

とし, 写像の合成で群と見る. これを K の自己同型群という. $L/K, L'/K$ が体の拡大であるとき, 体の同型写像 $f : L \to L'$ で, $f_{|K} = \mathrm{id}_K$ となるものを, K–同型写像という. さらに,

$$\mathrm{Aut}(L/K) = \{ f \in \mathrm{Aut}(L) \mid f_{|K} = \mathrm{id}_K \}$$

とおく. これは $\mathrm{Aut}(L)$ の部分群をなす. $\mathrm{Aut}(L/K)$ の元を, L の K–自己同型写像という.

例 4.1.3　$\mathbb{C}/\mathbb{R}$ において, $z \mapsto \overline{z}$ (複素共役) は $\mathrm{Aut}(\mathbb{C}/\mathbb{R})$ の元である.

L/K を体の拡大とする. 部分集合 $S \subset L$ に対して,

$$K(S) = \bigcap_{\substack{L \supset M \supset S \\ M \text{ は体}}} M$$

とおく, すなわち, $K(S)$ は集合 S を含む L の最小の部分体である. $K(S)$ を K 上 S から生成される体, あるいは, K に S の元を添加してできる体という. S が有限集合で, $S = \{\theta_1, \ldots, \theta_n\}$ であるとき, $K(S) = K(\theta_1, \ldots, \theta_n)$ とも書く. このとき, $K(S)$ は K 上有限生成な体という. $|S| = 1$, すなわち $S = \{\theta\}$ のとき, $K(\theta)$ を単拡大という.

例 4.1.4　$\mathbb{Q} \subset \mathbb{R}$ において, $S = \{\sqrt{2}\}$ とする. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ である.

定義から次は明らかである.

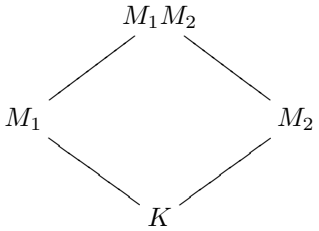
命題 4.1.2　L/K を体の拡大, $\theta_1, \ldots, \theta_n \in L$ とすると,

$$K(\theta_1, \ldots, \theta_n) = \left\{ \frac{f(\theta_1, \ldots, \theta_n)}{g(\theta_1, \ldots, \theta_n)} \mid f(x_1, \ldots, x_n),\, g(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n],\; g(\theta_1, \ldots, \theta_n) \neq 0 \right\}$$

L/K の 2 つの中間体, $L \supset M_1 \supset K$, $L \supset M_1 \supset K$ に対して,

$$M_1 M_2 = K(M_1 \cup M_2)$$

とおき, M_1, M_2 の合成体という. このとき, 拡大体 M_1M_2/M_1(resp. M_1M_2/M_2) を M_2/K(resp. M_1/K) の M_1 (resp. M_2) への持ち上げ (リフト) という.



4.2　単拡大

有限個の元による拡大, $K(\theta_1, \ldots, \theta_n)$ は, $K(\theta_1, \ldots, \theta_{n-1})(\theta_n)$ と帰納的に定義できるので, 単拡大 $K(\theta)$ の性質をまず調べる. L/K を体の拡大とし, $\theta \in L$ として, $M = K(\theta) \subset L$ とする.

$$\varphi : K[X] \longrightarrow M, \quad K[X] \ni f \mapsto f(\theta) \in M$$

とすると, φ は環準同型写像である. $K[X]$ は単項イデアル整域なので, $K[X]$ のイデアル $\mathrm{Ker}(\varphi)$ は, $\{0\}$ となるか, ある多項式 $f(X)$ が存在して, $\mathrm{Ker}(\varphi) = (f)$ となる.

$\mathrm{Ker}(\varphi) = \{0\}$ であるとき, θ は K 上超越的であるという. また, $K(\theta)$ は, K の超越拡大であるという. このとき, φ は $K[X]$ の商体 $K(X)$ に一意的に拡張され, 体の同型写像 $\varphi : K(X) \cong K(\theta)$ を与える (定理 3.7.1).

$\mathrm{Ker}(\varphi) \neq \{0\}$ であるとき, θ は K 上代数的であるという. $\mathrm{Ker}(\varphi)$ の生成元で, 最高次の係数が 1 であるもの[*4] を $\mathrm{Irr}(\theta, K : X)$ と書く. $K[X]$ は PID なので, これは一意的に定まる. このとき, φ から誘導される写

[*4] 最高次の係数が 1 の多項式をモニック (monic) な多項式という.

像を考える.

$$\overline{\varphi} : K[X]/(\mathrm{Irr}(\theta, K : X)) \longrightarrow M = K(\theta)$$

$M = K(\theta)$ から $\overline{\varphi}$ の全射性が従い, 環の同型写像になる. 従って, $K[X]/(\mathrm{Irr}(\theta, K : X))$ は体となり, イデアル $(\mathrm{Irr}(\theta, K : X))$ は極大イデアルになり, 特に素イデアルである. $K[X]$ の素イデアルは, K 上既約な多項式から生成されるから (命題 3.6.4), $\mathrm{Irr}(\theta, K : X)$ は K 上の既約多項式である. これを, θ の K 上の最小多項式といい, その次数を θ の K 上の次数という. すなわち, $\mathrm{Irr}(\theta, K : X)$ は, θ が満たす K 上の非自明な代数方程式の中で, 次数が最少かつ最高次の係数が 1 のものであると, 特徴付けられる.

上のことをまとめて, 次が示された.

定理 4.2.1　$K(\theta)$ を K の単拡大とするとき,

1. $f(\theta) = 0$ となる $f \in K[X]$ $(f \neq 0)$ が存在しないとき, $K(\theta) \cong K(X)$.
2. $f(\theta) = 0$ となる $f \in K[X]$ が存在するとき, このような 0 でない $K[X]$ の多項式で, 次数が最小かつ最高次の係数が 1 となるものが, ただ 1 つ存在する. それを $\mathrm{Irr}(\theta, K : X)$ とすると, $\mathrm{Irr}(\theta, K : X)$ は K 上既約な多項式で, $(\mathrm{Irr}(\theta, K : X))$ は $K[X]$ の極大イデアルとなり, $K(\theta) \cong K[X]/(\mathrm{Irr}(\theta, K : X))$.

命題 4.2.1　K を体, θ を K 上次数 n の代数的な元としたとき, $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ は $K(\theta)$ の K 上の基底になる. 特に,

$$[K(\theta) : K] = n$$

である.

証明.　θ の最小多項式を, $\mathrm{Irr}(\theta, K : X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 = q(X) \in K[X]$ とする. $1, \theta, \ldots, \theta^{n-1}$ が K 上 1 次従属であるとすると, 非自明な線形関係,

$$c_0 + c_1\theta + c_2\theta^2 + \cdots + c_{n-1}\theta^{n-1} = 0, \quad c_0, \ldots, c_{n-1} \in K$$

が存在する. これは, θ が n 次より小さい多項式 $c_0 + c_1X + c_2X^2 + \cdots + c_{n-1}X^{n-1}$ の根になることを示しているが, θ の次数の定義に矛盾する. よって, $1, \theta, \ldots, \theta^{n-1}$ は K 上 1 次独立である.

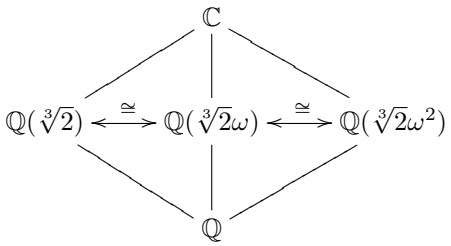
$\overline{\varphi} : K[X]/(q(X)) \to K(\theta)$ を定理 4.2.1 の証明で用いた同型写像とする. $g(X) \in K[X]$ とすると, $K[X]$ での割り算を利用して, $g(X) = f(X)q(X) + r(X)$, $\deg r < \deg f$ とできる. このとき, $\overline{\varphi}(g) = r(\theta)$ となるが, 右辺は, $1, \theta, \ldots, \theta^{n-1}$ の線形結合である. よって, $\overline{\varphi}$ の全射性より, $1, \theta, \ldots, \theta^{n-1}$ は線形空間として, K 上 $K(\theta)$ を生成する. よって, $\{1, \theta, \ldots, \theta^{n-1}\}$ は, $K(\theta)$ の K 上の基底である.

$f(X) \in K[X]$ を既約な多項式とする. $f(X) = 0$ の根 θ を K に付け加えた体 $K(\theta)$ を f **の根体**という.

命題 4.2.2　$f(X) \in K[X]$ を既約な多項式とする. このとき, $f(X)$ の根体は存在して, K–同型を除いて一意的である.

証明.　$f(X)$ は既約な多項式なので, f から生成されるイデアル $(f) \subset K[X]$ は極大イデアルである (命題 3.6.4). $K[X]/(f)$ は, K の拡大体で $f(X) = 0$ の根 $\overline{X} \in K[X]/(f)$ を含むので, f の根体である. また, 定理 4.2.1, 2. の証明と同様にして, f の根体は, $K[X]/(f)$ と同型になることがわかる.

例 4.2.1　$\mathbb{Q} \subset \mathbb{C}$ として, $f(X) = X^3 - 2 \in \mathbb{Q}[X]$ を考える ω を 1 の複素 3 乗根とするとき, $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$ が $\mathbb{C}$ における $X^3 - 2 = 0$ の根である. 体の同型 $\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}(\sqrt[3]{2}\omega) \cong \mathbb{Q}(\sqrt[3]{2}\omega^2)$ が存在する.



4.3　代数的拡大体

定義 4.3.1　L/K を体の拡大とする. 任意の $\theta \in L$ が K 上代数的であるとき, L/K を代数的拡大という.

定理 4.3.1　体の拡大 L/K に対して, 次は同値である.

1. $[L : K] < \infty$.
2. L は K 上有限個の代数的な元から生成される.

特に, 上の性質を持つとき, 体の拡大 L/K は代数的拡大である.

証明.　1. $\Longrightarrow$ 2.　$[L : K] = n < \infty$ とすると, L の K 上の基底で L は生成されているので, 有限生成である. また, $0 \neq \theta \in L$ に対して, $n + 1$ 個の元

$$1, \theta, \theta^2, \ldots, \theta^n$$

を考えると, これらは K 上 1 次独立ではありえない. 従って, $a_0, \ldots, a_n \in K$ が存在して, 非自明な線形関係 $a_0 + a_1\theta + \cdots + a_n\theta^n = 0$ があるので, θ は K 上代数的である.

2. $\Longrightarrow$ 1.　L の K 上の生成元を $\theta_1, \ldots, \theta_n$ とする. n に関する帰納法で証明する. $n = 1$ のときは, 命題 4.2.1 から従う. 一般の n の場合には, $M = K(\theta_1, \ldots, \theta_{n-1})$ とすると, $L = M(\theta_n)$ で, 帰納法の仮定から, $[M : K] < \infty$ である. θ_n は (K 上代数的なので)M 上代数的であり, $n = 1$ のときの証明から, $[L : M] < \infty$ である. よって, $[L : K] = [L : M][M : K] < \infty$ を得る.

系 4.3.1　L/K を体の拡大とし, $L \supset S$ とする. S の任意の元が K 上代数的なら, $K(S)$ は K 上代数的拡大体になる. すなわち, K 上代数的な元から生成される拡大体は, 代数的拡大体である.

証明.　$\theta \in K(S)$ が K 上代数的であることを示す. 拡大体の作り方から, $\theta_1, \ldots, \theta_n \in S$ が存在して, $\theta \in K(\theta_1, \ldots, \theta_n)$ となる. θ_i は K 上代数的だから, 上の定理より, θ は K 上代数的である.

系 4.3.2　L/K を体の拡大とし, $\alpha, \beta \in L$ が K 上代数的であるなら, $\alpha \pm \beta$, $\alpha\beta$, $\dfrac{\alpha}{\beta}$, $(\beta \neq 0)$ も K 上代数的である.

証明. 上の系において, $S = \{\alpha, \beta\}$ とすれば良い.

問 4.3.1　$\sqrt{2} + \sqrt{3}$ の $\mathbb{Q}$ 上の最小多項式を求めよ.

命題 4.3.1　$L \supset M \supset K$ を体の拡大とする. このとき

$$L/K \text{ が代数的} \iff L/M,\ M/K \text{ がともに代数的}$$

証明. $\Longrightarrow$ は明らかである.

$\Longleftarrow$ の証明: $\theta \in L$ をとる. θ は M 上代数的だから, (θ の M 上の次数を n とすると) $\alpha_0, \ldots, \alpha_{n-1} \in M$ が存在して, θ は

$$X^n + \alpha_{n-1}X^{n-1} + \cdots + \alpha_1 X + \alpha_0 = 0$$

の根となる. 従って, $M' = K(\alpha_0, \ldots, \alpha_{n-1})$ とおくと, θ は M' 上代数的である. M/K は代数的なので, $[M' : K] < \infty$ であり, $[M'(\theta) : K] = [M'(\theta) : M'][M' : K] < \infty$ を得る. $\theta \in M'(\theta)$ だから, θ は K 上代数的である.

上の命題の証明において, θ が K 上代数的な元からなる係数を持つ多項式の根ならば, θ は K 上代数的になることが示されていることに注意する.

系 4.3.3　L/K を体の拡大とし, M_1, M_2 を中間体とする. M_1, M_2 が K 上代数的なら, M_1M_2 も K 上代数的である.

証明. M_2 の元は K 上代数的なので, M_1 上も代数的である. よって, 系 4.3.1 より, M_1M_2/M_1 も代数的な拡大になる. M_1/K も代数的拡大だから, 上の命題より証明を得る.

4.4　代数的閉体

定義 4.4.1　L/K を体の拡大とする. $\overline{K}_L$ を次で定義する.

$$\overline{K}_L = \{\theta \in L \mid \theta \text{ は } K \text{ 上代数的 }\}$$

系 4.3.1, 系 4.3.2 より, これは K の代数的拡大体になる. $\overline{K}_L$ を K の L における代数的閉包 (algebraic closure) という.

$\overline{K}_L = K$ であるとき, K は L において代数的に閉じている (algebraically closed) という.

K の代数拡大が K 以外にないとき (すなわち, これ以上代数的に体を拡大できないとき), K を代数的に閉じている. あるいは, 代数的閉体であるという.

例 4.4.1　1.　$\mathbb{Q} \subset \mathbb{Q}(\pi) \subset \mathbb{R}$ を考える. π は $\mathbb{Q}$ 上超越的 ($\mathbb{Q}$ 上超越的な複素数を「超越数」という) であることが知られている (Lindemann(リンデマン), 1882 年). このとき, $\overline{\mathbb{Q}}_{\mathbb{Q}(\pi)} = \mathbb{Q}$ となり, $\mathbb{Q}$ は $\mathbb{Q}(\pi)$ において代数的に閉じている. 実際, π の超越性から, $\mathbb{Q}(\pi)$ の元は, $g(X) \in \mathbb{Q}(X)$ を用いて $g(\pi)$ と書かれる. $g(X) \notin \mathbb{Q}$(定数でない有理式) として, $f(X) \in Q[X]$ が存在して, $f(g(\pi)) = 0$ とすると, この π に対する分数式の分子を $h(\pi)$ とすると, $h(X) \in \mathbb{Q}[X]$ で, $h(\pi) = 0$ となるので, π の超越性に矛盾する. よって, 定数ではない有理式 $g \in \mathbb{Q}(X)$ に対して, $g(\pi)$ は $\mathbb{Q}$ 上代数的でない.

2. $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$ を考える．前節で述べたように, $\mathbb{Q}(\sqrt{2})$ は $\mathbb{Q}$ 上の代数的拡大になる．したがって, $\mathbb{Q}(\sqrt{2})$ の元は, すべて $\mathbb{Q}$ 上代数的である．すなわち, $\overline{\mathbb{Q}}_{\mathbb{Q}(\sqrt{2})} = \mathbb{Q}(\sqrt{2})$ であり, $\mathbb{Q}$ は $\mathbb{Q}(\sqrt{2})$ において, 代数的に閉じてはいない．

多項式に対する剰余定理, 因数定理から次の命題は明らかである．

命題 4.4.1　K を体とするとき, 次の 4 条件は互いに同値である．

1. K は代数的閉体である．
2. $K[X]$ の既約な多項式は 1 次式である．
3. $K[X]$ の定数でない多項式は, 1 次式の積に因数分解される．
4. $K[X]$ の定数でない多項式は, 必ず K に根をもつ．

系 4.4.1　L/K を体の拡大とする．L が代数的閉体であるなら, $\overline{K}_L$ も代数的閉体である．

証明.　$f(X) \in \overline{K}_L[X]$ を定数でない多項式とする．$f(X) \in L[X]$ と思うことができ, L は代数的閉体なので, $f(X) = 0$ の根 θ は, L の元である．一方, θ は $\overline{K}_L$ 上代数的であり, 体の拡大 $\overline{K}_L/K$ は代数的な拡大であるから, θ は K 上代数的である (命題 4.3.1 の証明を見よ)．よって, $\theta \in \overline{K}_L$ となり, 上の命題の 4. より, $\overline{K}_L$ は代数的閉体である．

例 4.4.2（代数的数体 (algebraic number field)）　定理 1.1.1(証明は D 節) より, $\mathbb{C}$ は代数的閉体である．$\overline{\mathbb{Q}} = \overline{\mathbb{Q}}_{\mathbb{C}}$ とする．すなわち, $\mathbb{Q}$ 係数の多項式の根全てからなる複素数の部分集合である．

$$\overline{\mathbb{Q}} = \{\theta \in \mathbb{C} \mid \exists f \in \mathbb{Q}[X],\ f(\theta) = 0\} \subsetneqq \mathbb{C}$$

上の系から, $\overline{\mathbb{Q}}$ は $\mathbb{C}$ の部分体になる．$\overline{\mathbb{Q}}$ を代数的数体と言い, その元を代数的数 (algebraic number) という．

定義 4.4.2（代数的閉包 (algebraic closure)）　K を体とする．K の拡大体 $\overline{K}$ が K の代数的閉包であるとは, 次の 2 条件を満たすことを言う．

1. 体の拡大 $\overline{K}/K$ は代数的である．
2. $\overline{K}$ は代数的閉体である．

定義から, 代数的閉包のある種の最小性が従う．実際 L, M を K の代数的閉包とし, $K \subset L \subset M$ とする．$a \in M$ とすると, a は K 上代数的かつ L が代数的に閉じていることから, $a \in L$ が従い, 結局 $L = M$ である．

例 4.4.3　$\overline{\mathbb{Q}}$ は $\mathbb{Q}$ の代数的閉包である．また, $\mathbb{R}$ の代数的閉包は, $\mathbb{C}$ である．

定理 4.4.1（Steiniz）　1.　K を体とするとき, K の代数的閉包 $\overline{K}$ が K 同型を除いて一意的に存在する．

2. L/K を代数的拡大体とし, Ω を代数的閉体であるとする．このとき, 体の埋め込み $\sigma : K \to \Omega$ は, 埋め込み $\tilde{\sigma} : L \to \Omega$, $\tilde{\sigma}_{|K} = \sigma$ に拡張することができる．

これの証明は, C に回す．証明の方針は, $f \in K[X]$ に対して, $f(X) = 0$ の根が K の中に無ければ, それを付け加えた体を考えると, f の根を持つ代数的拡大体ができる．これをありとあらゆる多項式に対して考えてやれば, 根を付け加えることができなくなり, 代数的閉体ができあがるわけである．Zorn の補題を用いてこのことを正当化する．

定理の 2. の埋め込みの拡張方法は, 複数ある. その個数は, 4.6 節で問題にする. 一般に, K を体, $K \subset L$ をその代数的拡大体とする. $K \subset \Omega$ を K の別の拡大体とするとき,

$$\mathrm{Emb}_K(L, \Omega) = \{\sigma : L \to \Omega \mid \sigma\text{は体の準同型}, \ \sigma_{|K} = \mathrm{id}_K\}$$

とおく. $\mathrm{Emb}_K(L, \Omega)$ の元を L の Ω への K–埋め込みという.

L/K を代数的拡大とする. このとき, L の代数的閉包 $\overline{L}$ は K の代数的閉包でもあることに注意する. 実際, $\overline{L}/L$ と L/K がともに代数的な拡大だから, $\overline{L}/K$ も代数的拡大になる. 同様に, K の代数的閉包 $\overline{K}$ が $\overline{K} \supset L$ を満たすなら, これは L の代数的閉包になる. 実際, 命題 4.3.1 の証明より, L 上代数的な元は K 上代数的なので, $\overline{K}$ の元となるからである.

例 4.4.4　定理の 2. において, $K = \mathbb{Q}, \Omega = \mathbb{C}$ とする. $\mathbb{C}$ は代数的閉体である. $f(X) = X^3 - 2$ として, $L = \mathbb{Q}[X]/(f)$ を考える (例 4.2.1). これは, $\mathbb{Q}$ の代数的拡大体である. 自然な埋め込み $\mathbb{Q} \to \mathbb{C}$ は $L \to \mathbb{C}$ に拡張されるが, L の元 $\overline{X}$ の像は 2 の 3 乗根である. $\overline{X}$ に対して, 3 つの 2 の 3 乗根の $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$ のどれを対応させるかによって, 埋め込みの拡張方法が異なる. すなわち, L の $\mathbb{C}$ への $\mathbb{Q}$–埋め込みは, 3 通りある.

次の命題は, 上の定理の 2. で $\Omega = \overline{K}$ としたものである.

命題 4.4.2　K を体, $\overline{K}$ を K の代数的閉包とする. 中間体 $K \subset L \subset \overline{K}$ を考える. このとき, K–埋め込み $i : L \to \overline{K}$ は, K–同型 $\sigma : \overline{K} \to \overline{K}$ に拡張される.

証明.　上の定理 4.4.1 の 2. において, Ω を $\overline{K}$ に置き換え, K を L に置き換え, L を $\overline{K}$ に置き換えると, i は K 埋め込み $\sigma : \overline{K} \to \overline{K}$ に拡張される. これが全射であることは, 上に述べた代数的閉包の最小性から従う[*5].

上の命題では, i が元々の包含写像であれば, 対応する $\overline{K}$ の K–同型写像は自明な写像となるが, $i(L) \neq L$ の場合の, 上の定理が重要である. 例えば, $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset \overline{\mathbb{Q}}$ であるが, $L = \mathbb{Q}(\sqrt[3]{2})$ としたとき, $L \to \mathbb{Q}(\sqrt[3]{2}\omega) \subset \overline{\mathbb{Q}}$, $\sqrt[3]{2} \mapsto \sqrt[3]{2}\omega$ という写像も, $\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}[X]/(X^3 - 2)$ の $\overline{\mathbb{Q}}$ への $\mathbb{Q}$–埋め込みである (中への体の同型写像). これに対して, この埋め込みを拡張した $\overline{\mathbb{Q}}$ の $\mathbb{Q}$–同型写像が存在することを述べている. この拡張で得られる $\mathbb{Q}$–同型写像を σ とすると, $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}\omega$ となる.

4.5　分解体と正規拡大体

定義 4.5.1　K を体, $f \in K[X]$ とする. K の拡大体 L において, $f(X)$ が 1 次式の積に分解するとき, すなわち, $\theta_1, \ldots, \theta_n \in L$ が存在して, $f(X) = c(X - \theta_1) \cdots (X - \theta_n)$ となるとき, L は f の分解体であるという.

さらに, $L = K(\theta_1, \ldots, \theta_n)$ であるとき, すなわち, f が 1 次式に分解する体の中で (集合の包含関係で) 最小のものであるとき, L を最小分解体という.

方程式の根を考えるためには, 最小分解体で十分なので, 文献によっては最小分解体を単に分解体と呼んでいるものも多い.

定理 4.5.1　上の記号と定義を用いる.

1. $f(X) \in K[X]$ の分解体は存在する.

[*5] $\overline{K}$ は無限集合になるので, 中への単射から全射は従わないことに注意する. ちなみに, 有限体 (有限個の元からなる体) は代数的閉体にはなり得ない. また, 無限集合の素朴な定義の 1 つとして「中への (全射ではない) 単射が存在する」がある.

2. L, L' を共に $f(X)$ の最小分解体とし, f のそれぞれの拡大体での素因数分解を,

$$f(X) = c(X-\alpha_1)\cdots(X-\alpha_n) \in L[X]$$
$$f(X) = c(X-\alpha'_1)\cdots(X-\alpha'_n) \in L'[X]$$

とすると, K–同型 $\sigma : L' \to L$ で, $\{\sigma(\alpha'_1), \ldots, \sigma(\alpha'_n)\} = \{\alpha_1, \ldots, \alpha_n\}$ となるものが存在する.

証明. 1. $\overline{K}$ を K の代数的閉包とすると, $f(X)$ は $\overline{K}$ において, $f(X) = c(X-\alpha_1)\cdots(X-\alpha_n)$ と因数分解されるから, $L = K(\alpha_1, \ldots, \alpha_n) \subset \overline{K}$ とおけば, L は f の (最小) 分解体になる.

2. L を 1. の証明で現れた $\overline{K}$ の中にある f の最小分解体とする. L' を別の最小分解体とすると, L' は K 上代数的である. 定理 4.4.1, 2. より, K–埋め込み $\sigma : L' \to \overline{K}$ が存在する. このとき σ は K–同型写像だから, $\sigma(f(X)) = f(X)$ である. 一方 L' は $f(X)$ の分解体だから, $f(X) = c(X-\alpha'_1)\cdots(X-\alpha'_n)$, $\alpha'_i \in L'$ であり, $\sigma(f(X)) = c(X-\sigma(\alpha'_1))\cdots(X-\sigma(\alpha'_n))$ となる. この式の右辺は $f(X)$ の $\overline{K}$ での因数分解であるから, $\{\alpha_1, \ldots, \alpha_n\} = \{\sigma(\alpha'_1), \ldots, \sigma(\alpha'_n)\}$ が成立する. $L = K(\alpha_1, \ldots, \alpha_n)$ なので $\mathrm{Im}(\sigma) = L$ が成立し, $\sigma : L' \to L$ は体の同型写像である.

例 4.5.1 $K = \mathbb{Q}$ とし, $f(X) = X^3 - 2$ とする. $\mathbb{Q}(\sqrt[3]{2})$ は f の分解体ではない. 実際

$$X^3 - 2 = (X - \sqrt[3]{2})(X^2 + \sqrt[3]{2}X + \sqrt[3]{4})$$

は, これ以上 $\mathbb{Q}(\sqrt[3]{2})$ では因数分解できない. ω を 1 の複素 3 乗根とするとき, $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2) = \mathbb{Q}(\sqrt[3]{2}, \omega) \subset \mathbb{C}$ が f の $\mathbb{Q}$ 上の最小分解体である.

命題 4.5.1 $\overline{K}$ を K の代数的閉包とする. $\alpha, \beta \in \overline{K}$ に対して, 次の 3 条件は同値である.

1. α, β の K 上の最小多項式は一致する.
2. K–同型写像 $\sigma : K(\alpha) \to K(\beta)$ で $\sigma(\alpha) = \beta$ となるものが存在する.
3. K–同型写像 $\sigma : \overline{K} \to \overline{K}$ で $\sigma(\alpha) = \beta$ となるものが存在する.

証明. 1.$\Longrightarrow$ 2. $f(X)$ を α, β の共通の最小多項式とする. このとき, $K(\alpha) \cong K[X]/(f(X)) \cong K(\beta)$ である. この同型写像は, 次で与えられる.

$$\varphi : K[X]/(f(X)) \to K(\alpha), \quad \overline{X} \mapsto \alpha$$
$$\psi : K[X]/(f(X)) \to K(\beta), \quad \overline{X} \mapsto \beta$$

よって, $\sigma = \psi \circ \varphi^{-1}$ とすれば良い.

2. $\Longrightarrow$ 3. $\overline{K}$ は $K(\alpha)$, $K(\beta)$ の代数的閉包でもあることに注意すると, 定理 4.4.1, 2. より, $\sigma : K(\alpha) \to K(\beta)$ は K–同型写像 $\sigma : \overline{K} \to \overline{K}$ に拡張されるので, それが求める写像である.

3. $\Longrightarrow$ 1. $f(X) \in K[X]$ を α の最小多項式とすると $\sigma(f) = f$ である. 一方, $0 = \sigma(f(\alpha)) = \sigma(f)(\sigma(\alpha)) = f(\beta)$ となるから, $f(X)$ は β の K 上の最小多項式で割り切れる. σ^{-1} に関して同じことを考えると, β の最小多項式は, f で割り切れる. すなわち, α の最小多項式と β の最小多項式は, (0 でない) 定数倍しか違わない. 最高次の係数がどちらも 1 であることより, α と β の最小多項式の一致が従う.

定義 4.5.2 上の命題を満たす $\alpha, \beta \in \overline{K}$ を K 上互いに共役であると言う.

例 4.5.2 複素数 $z \in \mathbb{C}$ に対して, その複素共役 $\bar{z}$ は, 上の定義の意味で $\mathbb{R}$ 上共役である. すなわち, 共役と言う言葉は, このことを一般の体に拡張したものである.

これまで何度も出てきている $\sqrt[3]{2},\ \sqrt[3]{2}\omega,\ \sqrt[3]{2}\omega^2 \in \overline{\mathbb{Q}}$ は, $\mathbb{Q}$ 上の最小多項式が X^3-2 であるから, $\mathbb{Q}$ 上共役な数である.

上では, 代数的な元の共役性について述べたが, 代数拡大体の共役性が同じように定義される. そのために, まず次の定理を証明する.

定理 4.5.2　L/K を代数的拡大体とし, $\overline{K}$ を K の代数的閉包とする. このとき, 次の 4 条件は同値である.

1. $L \subset M$ となる任意の拡大体 M と任意の $\sigma \in \mathrm{Aut}(M/K)$ に対して, $\sigma(L) = L$
2. $L \subset \overline{K}$ であるとき, 任意の $\sigma \in \mathrm{Aut}(\overline{K}/K)$ に対して, $\sigma(L) = L$
3. $\tau \in \mathrm{Emb}_K(L, \overline{K})$ に対して, $\mathrm{Im}(\tau) = \tau(L) \subset \overline{K}$ は, τ の取り方によらない.
4. $f(X) \in K[X]$ を既約多項式としたとき, $f(X)$ が L に根を持てば $f(X)$ は L で 1 次式の積に分解する.

証明.　1.$\Longrightarrow$ 2. $M = \overline{K}$ とすれば良い.

2. $\Longrightarrow$ 3. $\tau, \tau' \in \mathrm{Emb}_K(L, \overline{K})$ とする. $\tau : L \to \tau(L)$ は全単射だから, 体の K–同型写像 $\tau' \circ \tau^{-1} : \tau(L) \to \tau'(L)$ が得られる. ここで, 命題 4.4.2 を用いると, これは $\sigma \in \mathrm{Aut}(\overline{K}/K)$ に拡張される. 仮定より, $\sigma(\tau(L)) = \tau(L)$ だから, $\tau(L) = \sigma(\tau(L)) = \tau'(\tau^{-1}(\tau(L))) = \tau'(L)$.

3. $\Longrightarrow$ 4. $\tau(L)$ は $\tau \in \mathrm{Emb}_K(L, \overline{K})$ の取り方によらないので, これを改めて L とする. すなわち, $K \subset L \subset \overline{K}$ として良い. $f(X) \in K[X]$ を既約多項式とし, $\theta_1, \ldots, \theta_n$ を $f(X) = 0$ の $\overline{K}$ での根とする. $\theta_1 \in L$ と仮定して良い. $f(X)$ は K 上既約なので, 命題 4.5.1, 3. より, K–同型写像 $\sigma_i : \overline{K} \to \overline{K}$ で, $\sigma_i(\theta_1) = \theta_i$, $i = 2, 3, \ldots, n$ となるものが存在する. $\sigma_i \circ \tau$ は L の $\overline{K}$ への K–埋め込みであるが, 仮定より, $\sigma_i \circ \tau(L) = L$ なので, $\theta_i = \sigma_i(\theta_1) \in L$ となり, $f(X) = 0$ の根は全て L の元である.

4. $\Longrightarrow$ 1. M を K の拡大体で, $M \supset L$ とする. $\sigma \in \mathrm{Aut}(M/K)$ を取る. $\theta \in L$ とすると, 仮定より θ は K 上代数的である. $f(X) = \mathrm{Irr}(\theta, K : X)$ を θ の最小多項式とする. このとき, σ は K–同型写像なので, $\sigma(\theta)$ も $f(X) = 0$ の根である. $f(X) = 0$ の根は全て L の元だから, $\sigma(\theta) \in L$ となり, $\sigma(L) \subset L$ を得る. σ^{-1} に同様のことを考えると, $\sigma^{-1}(L) \subset L$ となり, $\sigma(L) = L$ が従う.

定義 4.5.3　$\overline{K}$ を K の代数的閉包とし, L, L' を K を含む $\overline{K}$ の部分体とする.

1. $\sigma \in \mathrm{Aut}(\overline{K}/K)$ が存在して, $\sigma(L) = L'$ であるとき, L, L' は K 上共役な体という. このとき, σ を L, L' の K 上の共役写像という.
2. 任意の $\sigma \in \mathrm{Aut}(\overline{K}/K)$ に対して, $\sigma(L) = L$ であるとき, L は K 上正規拡大体であるという.

定理 4.5.2 から, 定義 4.5.3, 2. は別の 3 つの同値な条件があることがわかる.

定理 4.5.3（有限次正規拡大の特徴づけ）　L/K が有限次正規拡大体であるための必要十分条件は, L がある多項式 $f(X) \in K[X]$ の分解体となることである.

証明.　L/K を有限次正規拡大体であるとする. 有限次の拡大体であるから, K 上代数的な元, $\theta_1, \ldots, \theta_n$ が存在して, $L = K(\theta_1, \ldots, \theta_n)$ である. $f_i(X) \in K[X]$ を θ_i の最小多項式とする. 定理 4.5.2, 4. より, $f_i(X) = 0$ の根は全て L の中にある. すなわち, $f_i(X) = \prod_{j=1}^{n_i}(X - \theta_{ij})$ と L で因数分解される.

$$f(X) = \prod_{i=1}^{n} f_i(X) = \prod_{i=1}^{n}\prod_{j=1}^{n_i}(X - \theta_{ij}) \in K[X]$$

とすると, $L = K(\theta_1, \ldots, \theta_n) \subset K(\{\theta_{ij}\}) \subset L$ より, $L = K(\{\theta_{ij}\})$ で, L は $f(X)$ の分解体である.

逆に, L を $f(X) \in K[X]$ の分解体とする. $f(X) = 0$ の根を $\theta_1, \ldots, \theta_n$ とすると, $L = K(\theta_1, \ldots, \theta_n)$ で, θ_i は K 上代数的だから, L/K は有限次代数拡大である (定理 4.3.1). M を K の拡大体で $M \supset L$ となるものとし, $\sigma \in \mathrm{Aut}(M/K)$ とする. $f(X) \in K[X]$ だから, $\sigma(\theta_i)$ も $f(X) = 0$ の根である. すなわち, σ は $f(X) = 0$ の根の集合 $\{\theta_1, \ldots, \theta_n\}$ の置換を与える. よって, $\sigma(L) = K(\sigma(\theta_1), \ldots, \sigma(\theta_n)) = K(\theta_1, \ldots, \theta_n) = L$ となり, L は K 上正規拡大体である.

系 4.5.1 L/K を有限次拡大, $\overline{K}$ を L を含む K の代数的閉包とする. このとき, L を含む $\overline{K}$ の部分体 M で, M/K が正規拡大となるものが存在する.

証明. L/K は有限次拡大体だから, K 上代数的な元 $\theta_1, \ldots, \theta_n$ が存在して, $L = K(\theta_1, \ldots, \theta_n)$ となる. $f_i(X) \in K[X]$ を θ_i の最小多項式とし, $f(X) = \prod f_i(X)$ の $\overline{K}$ での最小分解体を M とすれば, それが求めるものである.

正規拡大に関するいくつかの性質をまとめておく.

命題 4.5.2 L/K を正規拡大とする.

1. M/K を任意の拡大体とする. このとき, LM/M も正規拡大である.
2. $L \supset M \supset K$ を中間体とすると, L/M も正規拡大である.
3. M/K を代数拡大体とし, L_1, L_2 を中間体とする. L_1, L_2 が K 上正規拡大体なら, $L_1 \cap L_2$, L_1L_2 も K 上正規拡大である.

証明. 1. Ω を LM の任意の拡大体とし, $\sigma \in \mathrm{Aut}(\Omega/M)$ とする. $\sigma \in \mathrm{Aut}(\Omega/K)$ でもあるので, 定理 4.5.2, 1 より, $\sigma(L) = L$ である. $\sigma(M) = M$ も成立しているので, $\sigma(LM) = \sigma(L)\sigma(M) = LM$ となって, 定理 4.5.2 より, LM は M 上正規拡大である.

2. $\overline{K}$ を L を含む K の代数的閉包とする. $\sigma \in \mathrm{Aut}(\overline{K}/M)$ とすると, $\sigma \in \mathrm{Aut}(\overline{K}/K)$ でもある. L は K 上正規拡大なので, $\sigma(L) = L$ となる.

3. $\sigma \in \mathrm{Aut}(M/K)$ に対して, σ は全単射だから, $\sigma(L_1 \cap L_2) = \sigma(L_1) \cap \sigma(L_2)$ が成立し, σ は準同型写像だから, $\sigma(L_1L_2) = \sigma(L_1)\sigma(L_2)$ が成立する. L_1, L_2 が K 上正規拡大なので, $\sigma(L_1) = L_1$, $\sigma(L_2) = L_2$ となり証明を得る.

例 4.5.3 $\mathbb{Q}$ 上の $X^3 - 2$ の分解体 $\mathbb{Q}(\sqrt[3]{2}, \omega)$ について考える. $\mathbb{Q}(\sqrt[3]{2}, \omega) \supset \mathbb{Q}(\sqrt[3]{2}) \supset \mathbb{Q}$ となる部分体の列に対して, $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}(\sqrt[3]{2})$ は正規拡大であるが, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ は正規拡大ではない.

4.6 分離性

この節では, 根の重複 (重根) を問題にする.

$$f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in K[X]$$

とする. K の代数的閉包 $\overline{K}$ において,

$$f(X) = a_n(X - \theta_1)^{m_1} \cdots (X - \theta_l)^{m_l}, \qquad \theta_i \in \overline{K},\ \theta_i \neq \theta_j\ (i \neq j),\ m_i \geqq 1$$

と分解されたとする. このとき, m_i を根 θ_i の重複度といい, $m_i \geqq 2$ のとき, θ_i は $f(X)=0$ の重根 (m_i 重根) という. 全ての重複度が 1 のとき, すなわち, $f(X)=0$ が重根を持たないとき, $f(X)$ は K 上分離的であるという. そうでないとき, すなわち, ある i について $m_i \geqq 2$ となるとき, $f(X)$ は非分離的であるという. なお, 0 次の多項式は常に分離的であるとする.

上の $f(X)$ に対して,

$$f'(X) = na_nX^{n-1} + (n-1)a_{n-2}X^{n-1} + \cdots + 2a_2X + a_1$$

を $f(X)$ の形式的微分という. 形式的という言葉がつくのは, 一般に K 上では極限という概念を考えることができないためであるが, 通常の微分積分学での微分と同じ式である.

問 4.6.1　形式的微分において, 積の微分法の公式 $(fg)' = f'g + fg'$ が成立することを示せ.

補題 4.6.1　$f(X) \in K[X]$ が非分離的である ($\overline{K}$ で重根を持つ) 必要十分条件は, $f(X)=0$ と $f'(X)=0$ が共通根を持つことである.

証明.　$f(X)$ が分離的でなく, $f(X) = (X-\theta)^m g(X),\ m \geqq 2$ と重根を持つとする. このとき, $f'(X) = m(X-\theta)^{m-1}g(X) + (X-\theta)^m g'(X)$ となり, $f'(\theta)=0$ となるので, $f(X)=0$ と $f'(X)=0$ は共通根を持つ. 逆に, θ を $f(X)=0$ と $f'(X)=0$ の共通根とする. $f(X)=0$ の根であることから, $f(X) = (X-\theta)g(X)$ と因数分解される. このとき, $f'(X) = g(X) + (X-\theta)g'(X)$ である. $f'(\theta)=0$ より, $g(\theta)=0$ となる. よって, $g(X) = (X-\theta)h(X)$ と因数分解され, $f(X) = (X-\theta)^2 h(X)$ となり, $f(X)=0$ は θ を重根に持ち分離的ではない.

定理 4.6.1　1. $\mathrm{char}(K)=0$ なら K 上の既約な多項式は分離的である.

2. $\mathrm{char}(K) = p > 0$ とし, $f(X) \in K[X]$ を既約な多項式とする. このとき, 分離的な既約多項式 $f_s(X) \in K[X]$ と自然数 e が存在して, $f(X) = f_s(X^q),\ q = p^e$ と書ける.

証明.　$\overline{K}$ を K の代数的閉包とし,

$$f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0, \quad (a_n \neq 0)$$

とする.

1. $\theta \in K$ を $f(X)=0$ の根の 1 つとする. $f(X)$ は既約なので, $\dfrac{1}{a_n}f(X)$ は θ の最小多項式である. $f(X)=0$ が分離的でなく, θ を重根に持つとすると, $f'(\theta)=0$ である. $\dfrac{1}{a_n}f$ が θ の最小多項式であることより, $f(X)$ は $f'(X)$ を割り切る. $\deg f' < \deg f$ なので, $f'(X)=0$ を得る. $f'(X)$ の X^{i-1} の係数は, ia_i で, $\mathrm{char}(K)=0$ より, $i \neq 0,\ (i=1,2,\ldots,n)$ である. よって, $f'(X)=0$ であるためには, $a_i=0,\ (i=1,\ldots,n)$ となる. このとき, $\deg f = 0$ となる. これは, $f(X)$ が分離的でないことに矛盾する.

2. 上と同様に, $\theta \in \overline{K}$ を $f(X)=0$ の根ととる. f が分離的なら, $f=f_s,\ e=0$ で証明が終わる. $f(X)=0$ が θ を重根に持つとする. 上と同様 f の既約性と次数の最小性を利用すると, $f'(X)=0$ を得る. $f'(X)$ の X^{i-1} の係数について, $ia_i=0,\ i=1,2,\ldots,n$ が成立するが, $\mathrm{char}(K)=p$ なので,

$$ia_i = 0 \Longleftrightarrow p|i \text{ または } a_i = 0$$

となる. よって, $p \nmid i$ なら $a_i=0$ となり, $f(X)$ の係数は p の倍数の次数の部分にだけあるので,

$$f(X) = a_{mp}X^{mp} + a_{(m-1)p}X^{(m-1)p} + \cdots + a_pX^p + a_0$$

となる．ここで，

$$f_1(X) = a_{mp}X^m + a_{(m-1)p}X^{m-1} + \cdots + a_pX + a_0$$

とおくと，$f(X) = f_1(X^p)$ である．$f_1(X)$ が分離的なら，$f_s = f_1$, $e = 1$ で証明が終わる．$f_1(X)$ が分離的でないなら，$f_1(X)$ にこの操作を繰り返す．これを繰り返すことにより，$f_s(X)$ と e が定まる．$f(X)$ が既約だったので，$f_s(X)$ も既約である．

例 4.6.1　k を正標数 p の体とし，$K = k(t)$ を t を不定元とする 1 変数の有理関数体とする．$f(X) = X^p - t \in K[X]$ とすると，これは K 上既約である．実際，既約でないと仮定して因数分解が可能であるとすると，因子の個数だけ t の p 乗根が $\overline{K}$ に存在するはずである．しかし，θ, $\theta' \in \overline{K}$ を t の p 乗根とすると，$\left(\dfrac{\theta}{\theta'}\right)^p = 1$ を得る．$\mathrm{char}(k) = p$ なので，$x^p - 1 = (x-1)^p$ となり，1 の p 乗根は 1 だけであり，$\theta = \theta'$ となる．つまり，$\overline{K}$ 内で t の p 乗根はひとつだけであり，$\sqrt[p]{t} \notin K$ なので，$x^p - t$ は K 上既約である．$\mathrm{char}(k) = p$ なので，$f'(X) = 0$ である．上の定理を適用すると，$f(X) = f_1(X^p)$, $f_1(X) = X - t$ である．

上の定理の 2. において，既約な多項式 $f(X) \in K[X]$ から定まる $f_s(X)$ を f の被約多項式という．また，$\deg f_s$ を $\deg_s f$ と書いて f の被約次数，p^e を $\deg_i f$ と書いて非分離次数，e を非分離指数という．定義から明らかに，$\deg f = \deg_s f \cdot \deg_i f$ が成立する．$\deg_s f = 1$ のとき，f は純非分離的であるという．$\mathrm{char}(K) = 0$ のときには，全ての既約多項式は分離的なので，$f_s = f$, $e = 0$, $\deg_s f = \deg f$, $\deg_i f = 1$ とする．

θ を K 上代数的な元とする．このとき，θ の最小多項式 $\mathrm{Irr}(\theta, K : X)$ の被約次数，非分離次数，非分離指数を，それぞれ，θ の被約次数，非分離次数，非分離指数という．非分離次数が 1 のとき θ は K 上分離的であるといい，非分離次数が 1 より大きいとき，θ は K 上非分離的であるという．K 上非分離的かつ，$\deg_s \mathrm{Irr}(\theta, K : X) = 1$ のとき，θ は K 上純非分離的であるという．K の元は，常に分離的であることに注意する．

定義 4.6.1　L/K を代数拡大とする．

1. L の任意の元が K 上分離的であるとき，L/K を分離拡大という．そうでないとき，L/K は非分離的であるという．
2. $\overline{K}$ を K の代数的閉包とする．このとき，

   $$[L : K]_s = \left|\mathrm{Emb}_K(L, \overline{K})\right|$$

   を L/K の分離次数という．特に，$[L : K]_s = 1$ のとき，L/K は純非分離的であるという．

定理 4.6.2　L/K を代数拡大，M をその中間体とするとき，

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

が成立する．

証明.　K の代数的閉包を $\overline{K}$ とする．φ を $\tau \in \mathrm{Emb}_K(L, \overline{K})$ の M への制限で定まる写像とする．

$$\varphi : \mathrm{Emb}_K(L, \overline{K}) \to \mathrm{Emb}_K(M, \overline{K}), \quad \varphi(\tau) = \tau_{|M}, \quad \tau \in \mathrm{Emb}_K(L, \overline{K})$$

定理 4.4.1, 2. より，任意の $\tau' \in \mathrm{Emb}_K(M, \overline{K})$ は $\mathrm{Emb}_K(L, \overline{K})$ に拡張できるので，φ は全射である．

$\tau, \tau' \in \mathrm{Emb}_K(L, \overline{K})$ に対して, $\varphi(\tau) = \varphi(\tau')$ とすると, $\tau_{|M} = \tau'_{|M}$ である. この共通の像 $\tau(M) = \tau'(M)$ を M と同一視する. この時, $\tau, \tau' \in \mathrm{Emb}_M(L, \overline{K})$ と見ることができる. したがって, これらは, $|\mathrm{Emb}_M(L, \overline{K})|$ 個ある. この数が, (M と同一視する) M の $\overline{K}$ への K–埋め込み $\tau(M) \subset \overline{K}$ の取り方によらないのことを示せばよい. 命題 4.4.2 により, 2 つの M の K–埋め込み $\tau, \tau' \in \mathrm{Emb}_K(M, \overline{K})$ に対して, $\sigma \in \mathrm{Aut}(\overline{K}/K)$ が存在して, $\tau' = \sigma \circ \tau$ とできる. この時, 対応

$$\sigma : \mathrm{Emb}_{\tau(M)}(L, \overline{K}) \to \mathrm{Emb}_{\tau'(M)}(L, \overline{K}), \quad \rho \mapsto \sigma \circ \rho, \quad \rho \in \mathrm{Emb}_{\tau(M)}(L, \overline{K})$$

は σ^{-1} が逆写像を与えるので, 全単射である. よって, $\mathrm{Emb}_M(L, \overline{K})$ の個数は, M の K–埋め込みの取り方によらず, 一定である.

定理 4.6.3 L/K を有限次拡大とする.

1. $\mathrm{char}(K) = p$ のとき, 非負整数 e が存在して, $[L : K] = [L : K]_s p^e$ となる.
2. L/K が分離拡大であることと, $[L : K] = [L : K]_s$ は同値である.

証明. 1. 単拡大 $L = K(\theta)$ についてまず考える. θ の被約次数を m, 非分離次数を $q = p^e$ とする. $f(X)$ を θ の K 上の最小多項式とすると, f の被約多項式 f_s を用いて, $f(X) = f_s(X^q)$ となる. $\overline{K}$ を L を含む K の代数的閉包とする. f_s の $\overline{K}$ での因数分解を $f_s(X) = (X - \alpha_1) \cdots (X - \alpha_m)$ とすると, f の因数分解は, $f(X) = (X - \theta_1)^q \cdots (X - \theta_m)^q$, $\theta_i = \alpha_i^{\frac{1}{q}}$ となる. $L \cong K[X]/(f)$ で, $[L : K] = \deg f$ である. $\mathrm{Emb}_K(L, \overline{K})$ は $K[X]/(f) \ni \overline{X} \mapsto \theta_i \in \overline{K}$, $i = 1, \ldots, m$ と 1 対 1 に対応するから, $[L : K]_s = m$ であり, $[L : K] = \deg f = m \cdot p^e = [L : K]_s p^e$ が成立する. 特に, θ が K 上分離的であることと, $e = 0$ は同値である.

一般の場合は, L/K が有限次拡大なので, 有限個の生成元を用いて, $L = K(\theta_1, \ldots, \theta_n)$ と書ける. $L = K(\theta_1, \ldots, \theta_{n-1})(\theta_n)$, $M = K(\theta_1, \ldots, \theta_{n-1})$ とし, 生成元の個数に関する帰納法を用いる. 帰納法の仮定より, $[M : K] = [M : K]_s p^e$ であり, 単拡大の場合の証明より, $[L : M] = [L : M]_s p^{e'}$ である. 命題 4.1.1, 定理 4.6.2 を利用すれば, $[L : K] = [L : M][M : K] = [L : M]_s [M : K]_s p^{e+e'} = [L : K]_s p^{e+e'}$ となり, 証明を得る.

2. L/K が有限次拡大体であることから, $L = K(\theta_1, \ldots, \theta_n)$ として良い. $M = K(\theta_1, \ldots, \theta_{n-1})$ とする. θ_n が K 上分離的とすると M 上でも分離的である. 従って, 上の単拡大の議論から,

$$[L : M] = [M(\theta_n) : M] = [M(\theta_n) : M]_s = [L : M]_s$$

である. 上の証明と同様に, 生成元の個数に関する帰納法を利用すると, 任意の $\theta \in L$ が分離的なら, $[L : K]_s = [L : K]$ が成立する.

逆に $[L : K] = [L : K]_s$ とする. 任意の $\theta \in L$ に対して,

$$[L : K] = [L : K(\theta)][K(\theta) : K] = [L : K(\theta)]_s p^e \cdot [K(\theta) : K]_s p^{e'} \leqq [L : K(\theta)]_s [K(\theta) : K]_s = [L : K]_s$$

だから, $e = e' = 0$ となる. 従って, $[K(\theta) : K]_s = [K(\theta) : K]$ となり, 単拡大のときの証明から θ は K 上分離的である.

上の証明から, 次の系を得る.

系 4.6.1 K 上分離的な元から生成される体は, 分離的である.

命題 4.6.1 体の拡大は, 全て有限次であるとする.

1. $K \subset M \subset L$ とするとき,

$$L/K \text{ が分離的} \iff L/M, M/K \text{ が共に分離的.}$$

2. $L/K,\ M/K$ が共に分離的なら, LM/M も分離的である.
3. $L/K,\ M/K$ が共に分離的なら, LM/K も分離的である.

証明. 1. $[L:K] = [L:M][M:K]$ と $[L:K]_s = [L:M]_s[M:K]_s$ であることと, 分離次数が拡大次数を超えないことより明らか.

2. L の元は K 上分離的なので, M 上も分離的である. 従って, LM は M 上分離的な元から生成されるから, 分離拡大である.

3. 体の拡大 $LM \supset M \supset K$ を考えて, 1., 2. を適用すればよい.

任意の代数拡大が分離的である体を**完全体 (perfect field)** という. 自明な例として, 代数的閉体と標数 0 の体は完全体である. 正標数だと有限体は完全体になることが知られている (I). 以下では, 特に断らない限り, 体の拡大は常に分離的であると仮定する.

定理 4.6.4　有限生成代数拡大 $L = K(\theta_1, \theta_2, \ldots, \theta_n)$ において, $\theta_2, \ldots, \theta_n$ が K 上分離的なら, $\theta \in L$ が存在して, $L = K(\theta)$ となる. 特に, 有限次分離拡大は単拡大である.

証明.　L が有限体の場合, $L^\times$ が巡回群になることが証明されるので (4.8 節), その生成元が K 上 L を生成する.

K を無限体と仮定する. $n = 2$ として良い ($n \geqq 3$ なら帰納法を用いる). $L = K(\alpha, \beta)$ として, β が K 上分離的であるとする. α の K 上の最小多項式を $f(X)$, β の K 上の最小多項式を $g(X)$ とする. $\overline{K}$ における $f(X) = 0$ の根 (α と共役な数) を $\alpha_1, \ldots, \alpha_m,\ (\alpha_1 = \alpha)$, $g(X) = 0$ の根 (β と共役な数) を $\beta_1, \ldots, \beta_n,\ (\beta_1 = \beta)$ とする. β は K 上分離的なので, β_i は全て異なることに注意する. $c \in K$ を

$$\alpha_i + c\beta_j, \quad 1 \leqq i \leqq m,\ 1 \leqq j \leqq n$$

が全て異なるように選ぶ.

$$\alpha_i + c\beta_j = \alpha_{i'} + c\beta_{j'} \iff c = -\frac{\alpha_i - \alpha_{i'}}{\beta_j - \beta_{j'}}$$

なので, 右辺の数とならないように c を選べばよいが, K は無限体なので, これは可能である. $\gamma = \alpha + c\beta$ とするとき, $K(\gamma) = K(\alpha, \beta)$ が成立する. 実際, $K(\gamma) \subset K(\alpha, \beta)$ は明らかである. 逆を示すために,

$$h(X) = f(\gamma - cX) \in K(\gamma)[X]$$

を考える. $h(\beta) = f(\gamma - c\beta) = f(\alpha) = 0$ である. $j = 2, \ldots, n$ に対して, i' が存在して,

$$\alpha + c\beta - c\beta_j = \alpha_{i'}$$

が成立すれば, $\alpha + c\beta = \alpha_{i'} + c\beta_j$ となるが, これは c の取り方からありえないので, $h(\beta_j) \neq 0,\ j = 2, \ldots, n$ を得る. β の分離性より, $g(X) = 0$ は重根を持たないので, $g(X)$ と $h(X)$ の最大公約多項式は, $X - \beta$ となる. $g(X)$ も $K(\gamma)[X]$ の元なので, (Euclid の互除法を考えると) $h(X), g(X)$ の最大公約多項式 $X - \beta$ も $K(\gamma)[X]$ の元であり, これは, $\beta \in K(\gamma)$ を示している. このとき $\alpha = \gamma - c\beta$ となり, $K(\alpha, \beta) \subset K(\gamma)$ である.

問 4.6.2　$\mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{Q}(\sqrt[3]{2} + \omega)$ を示せ.

4.7 Galois の基本定理

L/K を代数的拡大とし, $G = \mathrm{Aut}(L/K)$ とする. 部分体 $L \supset M \supset K$ に対して,

$$G(M) = \{\sigma \in G \mid \sigma(x) = x,\ \forall x \in M\}$$

とおく. これが G の部分群になることは, 容易に分かる. 同様に, 部分群 $H \subset G$ に対して

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

とおく. これが L の部分体になることも, 容易に分かる. 次のことは, 定義から直ちに従う.

1. $K \subset L^G$
2. $H \subset G(L^H)$
3. $K \subset M_1 \subset M_2 \subset L \Longrightarrow G(M_1) \supset G(M_2), \quad G(L) = \{e\}.$
4. $H_1 \subset H_2 \Longrightarrow L^{H_1} \supset L^{H_2}$
5. $G(K) = G(L^G) = G$

1. から 4. は明らかである. 5. は次のようにして示される. 定義より $G \supset G(K)$ である. 1. より, $K \subset L^G$ だから 定義と 3. を用いて, $G \supset G(K) \supset G(L^G)$. ここで, 2. を用いると, $G \subset G(L^G)$ となるので, $G \subset G(L^G) \subset G(K) \subset G$ となり $G = G(L^G) = G(K)$ である.

まず, 次の定理が成り立つことを示す.

定理 4.7.1 L/K を代数的拡大, $G = \mathrm{Aut}(L/K)$ とする. 上の記号の下で, 次は同値である.

1. L/K は分離的かつ正規拡大である.
2. $K = L^G$
3. G のある部分群 H に対して, $K = L^H$

証明. 1.$\Longrightarrow$ 2. K の元は G で動かないので, $K \subset L^G$ は明らか. $\theta \in L$, $\theta \notin K$ とする. L/K は代数的拡大なので, θ は K 上代数的である. $f(X) \in K[X]$ を θ の K 上の最小多項式とする. L/K は分離的なので, $f(X)$ は分離的な多項式である. また, $\theta \notin K$ なので, $\deg f > 1$ である. L/K は正規拡大なので, $f(X)$ は L で一次式の積に分解する. $f(X) = \prod_i (X - \theta_i)$, $\theta_1 = \theta$, $\theta_i \in L$ とする. $\theta \mapsto \theta_2$ という対応は, 命題 4.5.1, 3. より, $\sigma \in \mathrm{Aut}(\overline{K}/K)$ の元を定める. θ は分離的なので, $\theta_2 \neq \theta$ で, L は正規拡大なので, $\sigma(L) = L$ となり, $\sigma \in \mathrm{Aut}(L/K)$ と思える. この σ に対して, $\sigma(\theta) \neq \theta$ なので, $\theta \notin L^G$ である.

2. $\Longrightarrow$ 3. $H = G$ と取れば良い.

3. $\Longrightarrow$ 1. $K = L^H$ となる部分群 H を固定する. $\theta \in L$ として, θ の K 上の最小多項式を $f(X) \in K[X]$ とする. $\overline{K}$ を L を含む K の代数的閉包とすると, f は $\overline{K}$ において, 1 次式の積に分解する.

$$f(X) = (X - \theta_1)(X - \theta_2)\cdots(X - \theta_n), \quad \theta_i \in \overline{K},\ \theta = \theta_1$$

$\sigma \in H$ とすると, $f(\sigma(\theta)) = \sigma(f(\theta)) = 0$ であるので, $\sigma(\theta) \in \{\theta_1, \ldots, \theta_n\}$ である. 従って, H は集合 $\{\theta_1, \ldots, \theta_n\}$ に作用する. この作用の θ の H–軌道を $\{\alpha_1, \ldots, \alpha_m\}$ とし, $g(X) = (X - \alpha_1)\cdots(X - \alpha_m)$ とする. $g(X)$ を展開したときの係数は, $\alpha_1, \ldots, \alpha_m$ の基本対称式であるが, 集合 $\{\alpha_1, \ldots, \alpha_m\}$ は H の作用

で不変なので, これらの基本対称式も H の作用で不変になる. すなわち, $g(X) \in K[X]$ である. 作り方から $g(\theta) = 0$ で, $f(X)$ は θ の最小多項式だから, $f(X)|g(X)$ である. また, 作り方から $\deg g \leqq \deg f$ かつ $\deg g \geqq 1$ なので, $f(X) = g(X)$ が成立する. $g(X)$ の作り方から, $g(X) = 0$ は重根を持たないので, θ は K 上分離的である. また, $\sigma(\theta) \in L$ だから, θ の K 上の最小多項式は L で 1 次式の積に分解する. K 上既約な $h(X) \in K[X]$ が L に根を持てば, その根の K 上の最小多項式の定数倍であるから, 上の議論より L で 1 次式の積に分解される. よって, L/K は正規拡大である.

定義 4.7.1 体の拡大 L/K が Galois 拡大であるとは, 上の定理のどれか (従って全て) が満たされることを言う. このとき, $\mathrm{Aut}(L/K) = \mathrm{Gal}(L/K)$ と書いて, 拡大 L/K の Galois 群という.

命題 4.7.1 L/K を有限次拡大とする. L/K が Galois 拡大であるための必要十分条件は, L が K 上分離的な多項式の分解体であることである.

証明. L/K が Galois 拡大なら, L は K 上分離的かつ正規拡大である. 定理 4.6.4 より, $\theta \in L$ が存在して, $L = K(\theta)$ となる. θ の K 上の最小多項式を f とすると, L/K は正規拡大だから, $f(X) = 0$ は L で 1 次式の積に分解され, L は f の分解体になる. また L/K は分離的だから, $f(X) = 0$ は重根を持たない. すなわち, f は K 上分離的である.

逆に, L を K 上分離的な多項式の分解体とすると, 正規性が分解体であることから従い (定理 4.5.3), 分離的な元で生成されることから, L/K の分離性が従う (系 4.6.1).

例 4.7.1 $K = \mathbb{Q}$ として, $X^3 - 2 = 0$ を考える. $X^3 - 2$ は $\mathbb{Q}$ 上分離的である. よって, この分解体 $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$ は $\mathbb{Q}$ 上の Galois 拡大である.

定理 4.7.2 L/K が有限次 Galois 拡大であるための必要十分条件は, $[L : K] = |\mathrm{Aut}(L/K)| < \infty$ である.

証明. $\overline{K}$ を K の代数的閉包とする. 一般に, 有限次代数拡大 L/K に対して, $|\mathrm{Aut}(L/K)| \leqq |\mathrm{Emb}_K(L, \overline{K})|$ が成立する. 実際, $\tau \in \mathrm{Emb}_K(L, \overline{K})$ を固定すると, $\sigma \in \mathrm{Aut}(L/K)$ に対して, $\tau \circ \sigma$ も $\mathrm{Emb}_K(L, \overline{K})$ を定め, この対応は中への単射を与えるからである. よって次の不等式が成立する.

$$|\mathrm{Aut}(L/K)| \leqq |\mathrm{Emb}_K(L, \overline{K})| = [L : K]_s \leqq [L : K]$$

定理 4.5.2, 3. より, 正規拡大であることと, 左側で等号が成立すること (上で述べた対応 $\tau \mapsto \tau \circ \sigma$ が全射) が同値であり, 定理 4.6.3, 2. より, 分離拡大であることと右側の等号が成立することが同値である.

命題 4.7.2 L を体, G を $\mathrm{Aut}(L)$ の有限部分群とする. $K = L^G$ とおくと, L/K は有限次 Galois 拡大で, $\mathrm{Gal}(L/K) = G$ である.

証明. $K = L^G$ なので, G の元は, $\mathrm{Aut}(L/K)$ の元とみなすことができる. この時, 定理 4.7.1 より, L/K は Galois 拡大である. G と K の取り方から, $G = \mathrm{Gal}(L/K)$ となるのは明らか. この時, $[L : K] = |G| < \infty$ である.

Galois 対応

以下では, 特に断らない限り, 拡大体は全て有限次とする. L/K を有限次 Galois 拡大, $G = \mathrm{Gal}(L/K)$ とする. 本節の冒頭の, L, K の中間体と G の部分群の対応を Galois 対応という. 具体的に書くために, 次の記

号を導入する.

$$\mathcal{H} = \{H \subset G \mid H \text{ は } G \text{ の部分群 }\}, \qquad \mathcal{M} = \{K \subset M \subset L \mid M \text{ は中間体 }\}.$$
$$\varphi : \mathcal{M} \longrightarrow \mathcal{H}, \qquad \mathcal{M} \ni M \mapsto \varphi(M) = G(M) = \{\sigma \in G \mid \sigma(x) = x,\ \forall x \in M\} \in \mathcal{H}.$$
$$\psi : \mathcal{H} \longrightarrow \mathcal{M}, \qquad \mathcal{H} \ni H \mapsto L^H = \{x \in L \mid \sigma(x) = x,\ \forall \sigma \in H\} \in \mathcal{M}.$$

上の対応, φ, ψ を Galois 対応という.

定理 4.7.3（Galois の基本定理） L/K を有限次 Galois 拡大とする.

1. 中間体 $L \supset M \supset K$ に対して, L/M は Galois 拡大で, $\mathrm{Gal}(L/M) = G(M)$ である. 逆に, $H \subset \mathrm{Gal}(L/K)$ を部分群とすると, L/L^H は Galois 拡大で, $\mathrm{Gal}(L/L^H) = H$ となる. 特に, 上で与えた Galois 対応は全単射で, 互いに逆写像となっている.
2. 中間体 $L \supset M \supset K$ に対して, M/K が Galois 拡大になるための必要十分条件は, $G(M)$ が $\mathrm{Gal}(L/K)$ の正規部分群であることである. このとき, $\mathrm{Gal}(M/K) \cong \mathrm{Gal}(L/K)/G(M)$ が成立する. 逆に, $H \lhd \mathrm{Gal}(L/K)$ を正規部分群とすると, L^H/K は Galois 拡大になり, $\mathrm{Gal}(L^H/K) \cong \mathrm{Gal}(L/K)/H$ となる. 特に, Galois 対応で, $\mathrm{Gal}(L/K)$ の正規部分群と, L に含まれる K の正規拡大が 1 対 1 対応する.

証明. 1. L/M が分離的であることは, 命題 4.6.1, 2. より従い, 正規拡大であることは, 命題 4.5.2, 2. から従う. よって, L/M は Galois 拡大である. $\sigma \in G(M)$ とすると, $\sigma \in \mathrm{Aut}(L)$ かつ $\sigma_{|M} = \mathrm{id}_M$ なので, $\sigma \in \mathrm{Aut}(L/M)$ である. $\sigma \in \mathrm{Aut}(L/M)$ とすると, $\sigma \in \mathrm{Aut}(L)$ かつ $\sigma_{|M} = \mathrm{id}_M$ なので $\sigma \in G(M)$ である. よって, $\mathrm{Gal}(L/M) = G(M)$ となる.

逆に部分群 $H \subset \mathrm{Gal}(L/K)$ を取る. L/K は有限次拡大で, $|\mathrm{Gal}(L/K)| = [L : K]$ なので, H は有限部分群である. よって命題 4.7.2 より, L/L^H は Galois 拡大で, $\mathrm{Gal}(L/L^H) = H$ である.

2. 上の 1. の証明を利用すると, 中間体 M に対して, $L^{G(M)} = M$ が成立し, 部分群 H に対して, $G(L^H) = H$ が成立することに注意する. 実際, $L \supset L^{G(M)} \supset M$ であるが, $[L : L^{G(M)}] = [L, M] = |G(M)|$ なので, $L^{G(M)} = M$ である. 部分群 H に対しては, $L^{G(M)} = M$ に $M = L^H$ を代入すると, $G(L^H) = \mathrm{Gal}(L/L^{G(L^H)}) = \mathrm{Gal}(L/L^H) = H$ となり, 主張の証明を得る.

中間体 M に対して, M/K は自動的に分離的である. M/K が正規拡大であるとする. このとき, 任意の $\sigma \in \mathrm{Aut}(L/K)$ に対して, $\sigma(M) = M$ が成立する. よって, 任意の $x \in M$ について, $\sigma(x) \in M$ である. $\tau \in G(M)$ とすると,

$$\sigma^{-1}(\tau(\sigma(x))) = \sigma^{-1}(\sigma(x)) = x$$

なので, $G(M) \lhd \mathrm{Gal}(L/K)$ が成立する. 逆に $G(M) \lhd \mathrm{Gal}(L/K)$ とする. $\sigma \in \mathrm{Gal}(L/K)$, $\tau \in G(M)$ に対して, $\sigma^{-1}\tau\sigma \in G(M)$ だから, $x \in M$ に対して, $\tau\sigma(x) = \sigma(x)$. すなわち, $\sigma(x) \in L^{G(M)}$ となり, 上のことより $L^{G(M)} = M$ だから, $\sigma(x) \in M$ となる. x は任意なので, $\sigma(M) = M$ となり, M は K 上正規拡大である (定理 4.5.2, 1.). このとき, $f : \mathrm{Gal}(L/K) \ni \sigma \mapsto \sigma_{|M} \in \mathrm{Aut}(M/K)$ を考える. f は明らかに準同型写像である. $\tau \in \mathrm{Aut}(M/K)$ は, $\widetilde{\tau} \in \mathrm{Aut}(L/K)$ に拡張できるので, この写像は全射である. $\mathrm{Ker}(f) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma_{|M} = \mathrm{id}_M\} = G(M)$ なので, 準同型定理から, $\mathrm{Gal}(M/K) \cong \mathrm{Gal}(L/K)/G(M)$ を得る.

$H \lhd \mathrm{Gal}(L/K)$ とし, $M = L^H$ とする. M/K は分離的であるので, 正規拡大になることを示す. 上と同様に, $\sigma \in \mathrm{Gal}(L/K)$, $\tau \in H$ に対して, $\sigma^{-1}\tau\sigma \in H$ だから, $x \in L^H$ に対して, $\tau\sigma(x) = \sigma(x)$ が成立する. よって, $\sigma(x) \in L^H$ となり, $\sigma(L^H) = L^H$ が成立する. よって, L^H は K 上正規である. $\mathrm{Gal}(L^H/K) \cong \mathrm{Gal}(L/K)/H$

の証明も, 上と同様である.

Galois の基本定理の 1. は, 下のように, 中間体集合と部分群の集合との間に, 包含関係が逆転した全単射が存在することを述べている.

$$\begin{array}{ccc} L & \longleftrightarrow & \{e\} \\ \cup & & \cap \\ M = L^H & \longleftrightarrow & G(M) = H \\ \cup & & \cap \\ K & \longleftrightarrow & \mathrm{Gal}(L/K) \end{array}$$

定理 4.7.4（Galois の推進定理） L/K を有限次 Galois 拡大, M/K を体の拡大とする. このとき, 体の拡大 LM/M 及び $L/(L\cap M)$ は Galois 拡大で, $\mathrm{Gal}(LM/M) \cong \mathrm{Gal}(L/(L\cap M))$ が成立する. ここで, 体 K, L, M は, 適当なある 1 つの体の部分体であると仮定している.

証明. LM/M が正規なのは, 命題 4.5.2, 1. より, LM/M が分離的なのは, 命題 4.6.1, 2. より従う. また, $L \supset L\cap M \supset K$ を考えると, $L/(L\cap M)$ が Galois 拡大であることも同様に示される.

$\sigma \in \mathrm{Gal}(LM/M)$ に対して, σ の L への制限を考える. $\sigma_{|L\cap M} = \mathrm{id}_{L\cap M}$ であるので, これは, $\mathrm{Aut}(L/(L\cap M))$ の元を定める. この対応を f とすると, これは明らかに群の準同型写像である.

$$f : \mathrm{Gal}(LM/M) \longrightarrow \mathrm{Gal}(L/(L\cap M)), \quad f(\sigma) = \sigma_{|L},\ \sigma \in \mathrm{Gal}(LM/M)$$

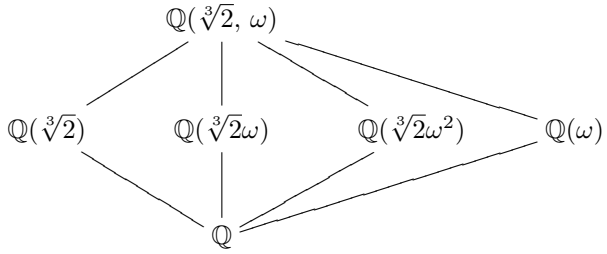
$f(\sigma) = \mathrm{id}_L$ なら, $\sigma = \mathrm{id}_{LM}$ なので, f は単射である. $\sigma \in \mathrm{Gal}(L/(L\cap M))$ とすると, これは自然に $\mathrm{Gal}(LM/M)$ の元と見ることができるので, f は全射である.

定義 4.7.2（方程式の Galois 群） $f(X) \in K[X]$ を分離的な多項式とする. $f(X) = 0$ の分解体 L を考えるとこれは K 上 Galois 拡大となる. $\mathrm{Gal}(L/K)$ を方程式 $f(X) = 0$ の Galois 群という.

例 4.7.2 $\mathbb{Q}$ 上の $X^3 - 2 = 0$ の分解体 $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$ を考える. $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$ は Galois 拡大である. $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ の元は, 生成元 $\sqrt[3]{2}$, ω の像で定まる. 命題 4.5.1 より, Galois 群の元の作用で, 最小多項式は変化しない ($\mathbb{Q}$ 上共役な元に写る). $\sqrt[3]{2}$ と $\mathbb{Q}$ 上共役な元は, $\sqrt[3]{2}\omega$, $\sqrt[3]{2}\omega^2$ であり, ω と $\mathbb{Q}$ 上共役な元は, ω^2 である. そこで,

$$\sigma : \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega \\ \omega \mapsto \omega \end{cases}, \qquad \tau : \begin{cases} \sqrt[3]{2} \mapsto \sqrt[3]{2} \\ \omega \mapsto \omega^2 \end{cases}$$

とすると, これは $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ の元を定める. 例えば, $\sigma(\sqrt[3]{2}\omega^2) = \sigma(\sqrt[3]{2})\sigma(\omega)^2 = \sqrt[3]{2}\omega^3 = \sqrt[3]{2}$ である. 簡単な計算から, $\sigma^3 = \tau^2 = \mathrm{id}$, $\tau\sigma\tau^{-1} = \tau\sigma\tau = \sigma^{-1}$ がわかる. $\sigma \mapsto (1,2,3) \in S_3$, $\tau \mapsto (1,2) \in S_3$ と対応させることにより, $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) \cong S_3$ となる. このとき, $\sigma\tau\sigma^{-1} \leftrightarrow (2,3)$, $\sigma^{-1}\tau\sigma \leftrightarrow (1,3)$ である. S_3 の自明でない部分群は 4 つあり, $\mathbb{Z}/2\mathbb{Z}$ と同型な 3 つ, $H_1 = \{e, (1,2)\}$, $H_2 = \{e, (2,3)\}$, $H_3 = \{e, (1,3)\}$ と $\mathbb{Z}/3\mathbb{Z}$ に同型な 3 次の交代群 $A_3 = \{e, (1,2,3), (1,3,2)\}$ である. それぞれに Galois 対応で対応する $\mathbb{Q}(\sqrt[3]{2}, \omega)$ の部分体 (不変体) を求めると, $L^{H_1} = \mathbb{Q}(\sqrt[3]{2})$, $L^{H_2} = \mathbb{Q}(\sqrt[3]{2}\omega)$, $L^{H_3} = \mathbb{Q}(\sqrt[3]{2}\omega^2)$, $L^{A_3} = \mathbb{Q}(\omega)$ となる. Galois の基本定理から, 拡大 $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}(\sqrt[3]{2}\omega)$, $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}(\sqrt[3]{2}\omega^2)$, $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}(\omega)$ は全て Galois 拡大になる. また, $S_3 \rhd A_3$ なので, $\mathbb{Q}(\omega)/\mathbb{Q}$ も Galois 拡大になり, その Galois 群は, $S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$ となる. これ以外の体の拡大, 例えば, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ は, Galois 拡大ではない (正規拡大ではない).



例 4.7.3（対称式） k を体, $X_1,\dots,X_n$ を不定元とし, $R = k[X_1,\dots,X_n]$ を k 上の n 変数多項式環, $L = k(X_1,\dots,X_n)$ を R の全商体とする. n 次対称群 S_n は, R に変数の置換で作用する. すなわち, $\sigma \in S_n$ に対して, $\sigma(X_i) = X_{\sigma(i)}$ で S_n の R への作用を定義する. S_n の R への作用は, 自然に L に拡張することができる. すなわち,

$$\sigma(f)(X_1,\dots,X_n) = f(X_{\sigma(1)},\dots,X_{\sigma(n)}),\quad \sigma \in S_n,\ f \in k(X_1,\dots,X_n)$$

この作用は, L の自己同型写像になる. $K = L^{S_n}$ とする. K の元, すなわち, 変数の置換を行っても変化しない式を, k 上の対称式という. 命題 4.7.2 より, 拡大 L/K は Galois 拡大となり, $\mathrm{Gal}(L/K) = S_n$ となる. よって特に, $[L:K] = |S_n| = n!$ である.

T を不定元とする. $F(T) \in K[T]$ を

$$F(T) = (T-X_1)\cdots(T-X_n) = T^n - (X_1+\cdots+X_n)T^{n-1} + \cdots + (-1)^n X_1\cdots X_n$$

で定義する. この式の T^{n-k} の符号を無視した係数,

$$s_k(X_1,\dots,X_n) = \sum_{i_1<\cdots<i_k} X_{i_1}\cdots X_{i_k} \in K = L^{S_n}$$

を k 次の基本対称式という. $L = k(X_1,\dots,X_n)$ の $s_1,\dots,s_n$ から生成される部分体 $K' = k(s_1,\dots,s_n)$ を考える. 明らかに, $k(s_1,\dots,s_n) \subset K = L^{S_n}$ である. 体の拡大 $k(X_1,\dots,X_n) \supset k(s_1,\dots,s_n) = K'$ を考えると, $k(X_1,\dots,X_n)$ は, K' 上の方程式 $F(T) = 0$ の分解体である. $F(T)$ は明らかに分離的なので, L/K は Galois 拡大となる. $\mathrm{Gal}(K/K')$ の元は, $F(T) = 0$ の根の置換を定めるので ($\mathrm{Gal}(L/K')$ が与える $F(T) = 0$ の根の置換は, $\mathrm{Gal}(L/K')$ から S_n の中への単射なので), $|\mathrm{Gal}(L/K')| \leqq n!$ である. よって, $L \supset K \supset K'$ より,

$$n! \geqq |\mathrm{Gal}(L/K')| = [L:K'] = [L:K][K:K'] = n!\,[K:K']$$

となり, $K = K'$ を得る. すなわち, 対称式は基本対称式の有理式となることがわかる.

注意 4.7.1 もっと細かく,「対称多項式は基本対称式の多項式であり, 基本対称式は代数的に独立である」, すなわち, $k[X_1,\dots,X_n]^{S_n} = k[s_1,\dots,s_n]$ が成立する (E).

4.8 1 のベキ根

補題 4.8.1 G を有限可換群とする. 任意の自然数 n に対して, $|\{x \in G \mid x^n = e\}| \leqq n$ が成立するなら, G は巡回群である.

証明. $|G| = m$ とする. G の中で最大位数を持つ元を a とし, その位数を k とする. $k = m$ なら G は a から生成される巡回群となる. $k < m$ とする. a から生成される部分群を H とし, $b \in G \setminus H\ (\neq \emptyset)$ とする. b の位数を l とすると, G がアーベル群なので, ab の位数は, k, l の最小公倍数となる. k の取り方から, この最小公倍数は k 以下となり, ab の位数は k であり, l は k の約数である. $b \neq e$ なので, $l \neq 1$ である. このとき, G の中で l 乗して e となる元は, $e, a^{k/l}, a^{2k/l}, \ldots, a^{(l-1)k/l}, b$ と $l+1$ 個以上あるため, 定理の条件を満たさない. よって $k = m$ である.

K を可換体とする. 自然数 n に対して, K の 1 の n 乗根の集合を,

$$\mu_n(K) = \{x \in K \mid x^n = 1\}$$

とおく.

系 4.8.1 $\mu_n(K)$ は巡回群である.

証明. K において, $X^l = 1$ となる元は, これを方程式の根の集合であると思うと, l 個以下である. 従って, 上の補題より, $\mu_n(K)$ は巡回群である.

Ω を代数的閉体とする. $\zeta^n = 1, \zeta^k \neq 1, k = 1, 2, \ldots, n-1$ となる元を 1 の原始 n 乗根といい, ζ_n で記すことにする. ζ_n を 1 つ固定する. $(\mathrm{char}(\Omega), n) = 1$ とすると, 方程式 $X^n - 1 = 0$ は分離的である. この時, 1 の n 乗根は n 個あり, 他の 1 の原始 n 乗根 ($\mu_n(\Omega)$ の生成元) は, $\zeta_n^d, (d, n) = 1,\ 1 \leqq d \leqq n-1$ の形である. 従ってこの時, 1 の原始 n 乗根は $\varphi(n)$ 個 (φ は Euler の関数) 存在する. n が $\mathrm{char}(\Omega)$ の倍数の時には, $X^n - 1 = 0$ が分離的ではないので, このようにはならない (標数が p の場合, $X^p - 1 = (X-1)^p$ なので, 1 の p 乗根は 1 つしかない).

例 4.8.1 $K = \mathbb{C}$ であるとき, $e^{\frac{2\pi}{n}\sqrt{-1}} = \cos\dfrac{2\pi}{n} + \sqrt{-1}\sin\dfrac{2\pi}{n}$ は 1 の原始 n 乗根である. 他の原始 n 乗根は, $e^{\frac{2d\pi i}{n}} = \cos\dfrac{2d\pi}{n} + \sqrt{-1}\sin\dfrac{2d\pi}{n},\ (d, n) = 1$ の形になる.

命題 4.8.1 Ω を代数的閉体であるとするとき, 次の 1.〜 3. は同値である.

1. Ω は 1 の原始 n 乗根を含む.
2. $\mu_n(\Omega)$ は位数 n の巡回群である.
3. $p = \mathrm{char}(\Omega)$ とするとき, $p \nmid n$ ($0 \nmid n$ と約束する).

証明. 2.$\Longrightarrow$ 1. は明らか.

1. $\Longrightarrow$ 3. $p | n$ とし, $n = pk$ とする.

$$x^n - 1 = x^{pk} - 1 = (x^p - 1)(x^{p(k-1)} + \cdots + x^p + 1) = (x-1)^p(x^{p(k-1)} + \cdots + x^p + 1)$$

だから, $|\{x \in \Omega \mid x^n = 1\}| < n$ となる. もし, Ω が原始 n 乗根を含めば, $|\{x \in \Omega \mid x^n = 1\}| = n$ となるので, Ω は原始 n 乗根を含まない.

3. $\Longrightarrow$ 2. $p \nmid n$ とすると, $X^n - 1$ は分離的な多項式となり, $|\mu_n(\Omega)| = n$ となる. このとき, $\mu_n(\Omega)$ は位数 n の巡回群となるので, その生成元は 1 の原始 n 乗根である.

定理 4.8.1 $\mathrm{char}(K) \nmid n$ とする. ζ_n を 1 の原始 n 乗根とすると, $K(\zeta_n)/K$ は Galois 拡大で, $\mathrm{Gal}(K(\zeta_n)/K)$ は $(\mathbb{Z}/n\mathbb{Z})^\times$ の部分群と同型である.

証明. $X^n-1=0$ の根は ζ_n^k, $k=0,1,\dots,n-1$ なので, $K(\zeta_n)/K$ は $X^n-1=0$ の分解体であり, 特にこの拡大は正規拡大である. $\mathrm{char}(K)\nmid n$ なので, X^n-1 は K 上分離的であり, $K(\zeta_n)/K$ は分離拡大である. よって, $K(\zeta_n)/K$ は Galois 拡大である. $\sigma\in\mathrm{Gal}(K(\zeta_n)/K)$ とする. $\sigma(\zeta_n)=\zeta_n^{j(\sigma)}$ で $j(\sigma)\in\mathbb{Z}/n\mathbb{Z}$ を定める. σ が体の同型写像なので, $\sigma(\zeta_n)$ も $K(\zeta_n)$ の 1 の原始 n 乗根である. よって, $j(\sigma)\in(\mathbb{Z}/n\mathbb{Z})^\times$ である. また, $K(\zeta_n)$ は ζ_n から生成されるので, $j:\mathrm{Gal}(K(\zeta_n)/K)\ni\sigma\mapsto j(\sigma)\in(\mathbb{Z}/n\mathbb{Z})^\times$ は単射である. j が準同型写像であることも明らかなので, 定理を得る.

一般に $K(\zeta_n)/K$ を円分拡大体あるいは円分体 (cyclotomic field) という. $K=\mathbb{Q}$ のとき, 複素平面での単位円 $\{z\in\mathbb{C}\mid |z|=1\}$ の n 等分点を与えるからである. ζ_n の $\mathbb{Q}$ 上の最小多項式を, $\Phi_n(X)$ と書き, 円分多項式 (cyclotomic polynomial) という. $\mathbb{Q}$ は, ±1 以外に 1 のベキ根を含まないので, 上の証明から, $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})\cong(\mathbb{Z}/n\mathbb{Z})^\times$ が成立する. また, $\mathbb{Q}(\zeta_n)$ は $\Phi_n(X)$ の最小分解体であり, その Galois 群は, $\Phi_n(X)$ の根の置換を与えるから,

$$\Phi_n(X)=\prod_{\zeta:1\text{ の原始 }n\text{ 乗根}}(X-\zeta)=\prod_{(d,n)=1}(X-\zeta_n^d)$$

であることもわかる. p が素数なら,

$$\Phi_p(X)=\prod_{i=1}^{p-1}(X-\zeta_p^i)=\frac{X^p-1}{X-1}=X^{p-1}+X^{p-2}+\cdots+X+1$$

である.

問 4.8.1 $\mathbb{Q}$ で, $\Phi_4(X)$, $\Phi_6(X)$, $\Phi_8(X)$, $\Phi_9(X)$, $\Phi_{10}(X)$, $\Phi_{12}(X)$ を $\mathbb{Z}[X]$ の元として求めよ. (それぞれ, $\varphi(n)$ 次の多項式になる. 任意の n に対して, $\Phi_n(X)\in\mathbb{Z}[X]$ であることが証明される. H 節を参照.)

例 4.8.2 $\mathbb{Q}$ 上の $X^7-1=0$ の分解体, $\mathbb{Q}(\zeta_7)/\mathbb{Q}$ を考える. 情報科学演習で述べたように, ζ_7 は, $\sqrt{-7}$ を利用すると, 3 次方程式の根であることがわかる (http://www.math.u-ryukyu.ac.jp/~suga/joho/2016/12/node5.html). これが, なぜわかるのかを解説する.

$X^7-1=(X-1)(X^6+X^5+X^4+X^3+X^2+X+1)$ なので, ζ_7 は $X^6+X^5+X^4+X^3+X^2+X+1=0$ の根である. $\sigma\in\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})$ とする. $\sigma(\zeta_7)=\zeta_7^{j(\sigma)}$ で $j(\sigma)$ を定めると, $j:\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})\xrightarrow{\simeq}(\mathbb{Z}/7\mathbb{Z})^\times\cong\mathbb{Z}/6\mathbb{Z}$ を与える. $(\mathbb{Z}/7\mathbb{Z})^\times\ni\overline{3}$ を生成元ととると, $(\mathbb{Z}/7\mathbb{Z})^\times$ には, 2 つの非自明な部分群, $H_1=\{\overline{1},\overline{2},\overline{4}\}$ と $H_2=\{\overline{1},\overline{6}\}=\{\pm\overline{1}\}$ が存在することがわかる. $(\mathbb{Z}/7\mathbb{Z})^\times$ は Abel 群なので, 部分群は自動的に正規部分群になることに注意する. これらに対応する中間体を $\mathbb{Q}(\zeta_7)^{H_1}=M_1$, $\mathbb{Q}(\zeta_7)^{H_2}=M_2$ とする. $a=\zeta_7+\zeta_7^2+\zeta_7^4$ とおくと, $a\in M_1$ である. $M_1/\mathbb{Q}$ は Galois 拡大で, その Galois 群は $\mathbb{Z}/2\mathbb{Z}$ に同型になる. 特に, $M_1/\mathbb{Q}$ は 2 次拡大なので, a は $\mathbb{Q}$ 上の 2 次方程式を満たす.

$$a^2+a+2=(\zeta_7+\zeta_7^2+\zeta_7^4)^2+\zeta_7+\zeta_7^2+\zeta_7^4+2=2(1+\zeta_7+\zeta_7^2+\zeta_7^4+\zeta_7^3+\zeta_7^5+\zeta_7^6)=0.$$

従って, $a=\dfrac{-1\pm\sqrt{-7}}{2}$ となる. $M_1=\mathbb{Q}(a)$ なので, $M_1=\mathbb{Q}(\sqrt{-7})$ を得る. $\mathbb{Q}(\zeta_7)/M_1$ は, Galois 群が $\mathbb{Z}/3\mathbb{Z}$ に同型な Galois 拡大なので, 3 次拡大である. 特に, ζ_7 は M_1–係数の 3 次方程式の根となる. 実際には,

$$\alpha=\frac{-1+\sqrt{-7}}{2},\quad \beta=\frac{-1-\sqrt{-7}}{2}$$

とおくと,

$$X^6+X^5+X^4+X^3+X^2+X+1=(X^3-\alpha X^2+\beta X-1)(X^3-\beta X^2+\alpha X-1)$$

となるので, ζ_7 は上の右辺の因数の方程式の根である (これの一般の素数 p に対する一般化は J 節を参照).

M_2 についても同様の考察をしてみる. $b=\zeta_7+\zeta_7^6=\zeta_7+\zeta_7^{-1}$ とすると $b\in M_2$ である. $\mathrm{Gal}(M_2/\mathbb{Q})\cong\mathbb{Z}/3\mathbb{Z}$ なので, b は $\mathbb{Q}$ 上の 3 次方程式の根である. 実際,

$$\begin{aligned}(\zeta_7+\zeta_7^6)^3+(\zeta_7+\zeta_7^6)^2-2(\zeta_7+\zeta_7^6)-1&=\zeta_7^3+3\zeta_7+3\zeta_7^6+\zeta_7^4+\zeta_7^2+2+\zeta_7^5-2\zeta_7-2\zeta_7^6-1\\&=\zeta_7^3+\zeta_7+\zeta_7^6+\zeta_7^4+\zeta_7^2+\zeta_7^5+1=0\end{aligned}$$

となるので, b は $\mathbb{Q}$ 上の 3 次方程式, $X^3+X^2-2X-1=0$ の根である. この方程式の根を θ_1, θ_2, θ_3 とすると, 1 の 7 乗根は, $X^2-\theta_iX+1=0,\ i=1,2,3$ の根となる.

4.9 巡回拡大と 2 項方程式

一般に, L/K を Galois 拡大とするとき, $\mathrm{Gal}(L/K)$ の群の性質で拡大体の名前をつける. 表題に挙げた巡回拡大とは, $\mathrm{Gal}(L/K)$ が (有限) 巡回群となる Galois 拡大のことである. 同様に, $\mathrm{Gal}(L/K)$ が Abel 群なら Abel 拡大, 可解群なら可解拡大という.

定理 4.9.1 K が 1 の原始 n 乗根 ζ_n を含む体とし, $d|n$ とする. L/K を K の拡大体としたとき, L/K が Galois 拡大で $\mathrm{Gal}(L/K)$ が d 次の巡回群である必要十分条件は, ある $a\in K$ が存在して, $L\subset K(\sqrt[n]{a})$ となることである.

証明. まず, L/K が Galois 拡大で, $\mathrm{Gal}(L/K)$ が n 次の巡回群であると仮定する. $\sigma\in\mathrm{Gal}(L/K)$ を生成元とする. $\sigma:L\to L$ を K–線形変換と見る. $\sigma^n=\mathrm{id}_L$ なので, 線形変換 σ の固有値は, 1 の n 乗根であり, $\sigma^k\neq\mathrm{id}_L,\ k=1,\dots,n-1$ より, σ は原始 n 乗根 ζ_n を固有値に持つ. このとき, σ の固有値 ζ_n に対応する固有ベクトル b が, K の代数的閉包, $\overline{K}$–係数に係数拡大したベクトル空間 (テンソル積を知っているのなら, $\overline{K}\otimes_K L$) 内に存在する. 仮定より, $\zeta_n\in K$ なので (固有ベクトルの計算は, はき出し法なので) $b\in L$ がわかる. $\sigma(b^n)=\sigma(b)^n=(\zeta_nb)^n=b^n$ なので, $b^n\in K$ である. $a=b^n$ とおくと, $b=\sqrt[n]{a}$, $L\supset K(\sqrt[n]{a})$ となる. $\zeta_n\in K$ なので, 方程式 $X^n-a=0$ の根は $\sqrt[n]{a},\ \sqrt[n]{a}\zeta_n,\dots,\sqrt[n]{a}\zeta_n^{n-1}$ となり, $x^n-a=0$ は K 上分離的な方程式であり, $K(\sqrt[n]{a})$ はその分解体となる. すなわち, $K(\sqrt[n]{a})/K$ は Galois 拡大となる. $\sigma(\sqrt[n]{a}\zeta_n^i)=\sqrt[n]{a}\zeta_n^{i+1}$ なので, $x\in K(\sqrt[n]{a})$ に対して, $\sigma(x)=x\Leftrightarrow x\in K$ が従う. σ は $\mathrm{Gal}(L/K)$ を生成しているので, $K(\sqrt[n]{a})$ は Galois 拡大 L/K の自明な部分群に対応する不変体であり, $L=K(\sqrt[n]{a})$ となる.

$d|n$ とすると, K は 1 の原始 d 乗根 $\zeta_n^{(n/d)}$ を含む. L/K が Galois 拡大で, $\mathrm{Gal}(L/K)$ が d 次の巡回群とすると, 上と同じ議論で, $b\in K$ が存在して, $L=K(\sqrt[d]{b})$ となる. $a=\sqrt[d]{b}^n=b^{(n/d)}$ とすると, $a\in K$ で, $L\subset K(\sqrt[n]{a})$ となる.

逆に, $K\ni\zeta_n$ なら $K(\sqrt[n]{a})$ は, K 上の分離的な多項式 X^n-a の分解体なので, $K(\sqrt[n]{a})/K$ は Galois 拡大である. 対応 $\sqrt[n]{a}\mapsto\sqrt[n]{a}\zeta_n^i$ が $K(\sqrt[n]{a})$ の K–同型となる最小の正整数 i をとると, これが $\mathrm{Gal}(K(\sqrt[n]{a})/K)$ の生成元となり, $\mathrm{Gal}(K(\sqrt[n]{a})/K)$ は n 次の巡回群の部分群となる. このとき, 中間体 $L\subset K(\sqrt[n]{a})$ に Galois 対応で対応する $\mathrm{Gal}(K(\sqrt[n]{a})/K)$ 部分群 H は, ある n の約数 m に対する位数 m の巡回群になる. $\mathrm{Gal}(K(\sqrt[n]{a})/K)$ は Abel 群なので, $H\lhd\mathrm{Gal}(K(\sqrt[n]{a})/K)$ となり, L/K は Galois 拡大で, その Galois 群 ($\mathrm{Gal}(K(\sqrt[n]{a})/K)/H$ と同型な群) は, n の約数を位数に持つ巡回群となる.

注意 4.9.1 上の証明に現れる, 線形写像 σ の固有ベクトルが, 1.1 節で 3 次方程式を解く際に現れた, Lagrange

の分解式に他ならない. 1.1 節のような, $a \in K$ を σ で動かした和 (1.1 節では, $\sigma = (1,2,3)$, $\sigma^3 = e$, $\zeta_3 = \omega$)

$$b = a + \zeta_n^{-1}\sigma(a) + \cdots + \zeta_n^{-n+1}\sigma^{n-1}(a)$$

を考えると, $\sigma(b) = \zeta_n b$ となる. 証明では, $b \neq 0$ であることを保証する必要があるので, ここでは線形代数の結果を用いてそれを示した.

例 4.9.1 上で, K を 1 の原始 4 乗根 $\sqrt{-1}$ を含む体, $K = \mathbb{Q}(\sqrt{-1})$ とし, $a = 4$ とする. $\sqrt[4]{4}$ を K に付け加えた体は, $L = K(\sqrt[4]{4}) = K(\sqrt{2})$ となる. $\mathrm{Gal}(L/K)$ は, $\sqrt{2} \mapsto \sqrt{2} \cdot (\sqrt{-1})^2 = -\sqrt{2}$ から生成される群で, 位数 2 の巡回群である.

系 4.9.1 $\mathrm{char}(K) \nmid n$ で, K は 1 の原始 n 乗根 ζ_n を含むとする. このとき, $a_1, a_2, \ldots, a_n \in K^\times$ に対して, $L = K(\sqrt[n]{a_1}, \sqrt[n]{a_2}, \ldots, \sqrt[n]{a_l})$ は K 上の Galois 拡大で, $\mathrm{Gal}(L/K)$ は Abel 群になる.

証明. $\zeta_n \in K$ なので, L は $(X^n - a_1)(X^n - a_2)\cdots(X^n - a_l) = 0$ の分解体になり, L/K は分離拡大になる. $K_i = K(\sqrt[n]{a_i}) \subset L$, $i = 1, \ldots, n$ とする. 定理 4.9.1 より, K_i/K は Galois 拡大で, $\mathrm{Gal}(K_i/K)$ は巡回群になる. $\varphi : \mathrm{Gal}(L/k) \to \mathrm{Gal}(K_1/K) \times \cdots \times \mathrm{Gal}(K_l/K)$ を $\sigma \in \mathrm{Gal}(L/K)$ に対して次で定義する.

$$\varphi(\sigma) = (\sigma_{|K_1}, \ldots, \sigma_{|K_l}) \in \mathrm{Gal}(K_1/K) \times \cdots \times \mathrm{Gal}(K_l/K)$$

これは明らかに群の準同型写像で, 定義から,

$$\mathrm{Ker}(\varphi) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\sqrt[n]{a_i}) = \sqrt[n]{a_i},\ i = 1, \cdots, l\} = \{\mathrm{id}_L\}$$

となるので単射である. よって, $\mathrm{Gal}(L/K)$ は Able 郡 $\mathrm{Gal}(K_1/K) \times \cdots \times \mathrm{Gal}(K_l/K)$ の部分群と同型になり, 特に Abel 郡である.

2 項方程式 $X^n - a = 0$ の分解体とその Galois 群

$X^n - a = 0$ の分解体の Galois 群を記述するために,

$$GL_2(\mathbb{Z}/n\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}/n\mathbb{Z},\ ad - bc \in (\mathbb{Z}/n\mathbb{Z})^\times \right\}$$

の次の部分群を考える.

$$\mathrm{Aff}_1(\mathbb{Z}/n\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in (\mathbb{Z}/n\mathbb{Z})^\times,\ b \in \mathbb{Z}/n\mathbb{Z} \right\}$$

これを $\mathbb{Z}/n\mathbb{Z}$ 上の 1 次の affine(アファイン) 変換群という.

問 4.9.1
1. $\mathrm{Aff}_1(\mathbb{Z}/n\mathbb{Z})$ が $GL_2(\mathbb{Z}/n\mathbb{Z})$ の部分群である事を示せ.
2. $N = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{Z}/n\mathbb{Z} \right\}$ とすると, $\mathrm{Aff}_1(\mathbb{Z}/n\mathbb{Z}) \rhd N$ を示せ.
3. $[\mathrm{Aff}_1(\mathbb{Z}/n\mathbb{Z}), \mathrm{Aff}_1(\mathbb{Z}/n\mathbb{Z})] = N$ を示し, $\mathrm{Aff}_1(\mathbb{Z}/n\mathbb{Z})$ が可解群であることを示せ.
4. $\mathrm{Aff}_1(\mathbb{Z}/4\mathbb{Z})$ は位数 8 の 2 面体群と同型であることを示せ.

以下では, 簡単のため, $\mathrm{char}(K) \nmid n$ を仮定する. $a \in K$ とし, 方程式 $X^n - a = 0$ の最小分解体を L とする. $\mathrm{char}(K) \nmid n$ なので, $X^n - a$ は K 上分離的な多項式となり, L/K は Galois 拡大である. $G = \mathrm{Gal}(L/K)$ とする. $\sqrt[n]{a}$ を 1 つ固定すると, $\sqrt[n]{a}\zeta_n$ も $X^n - a = 0$ の根なので, $\zeta_n \in L$ であり, $L = K(\sqrt[n]{a}, \zeta_n)$ となる.

$\rho \in G$ に対して, $j(\rho) \in (\mathbb{Z}/n\mathbb{Z})^\times$, $i(\rho) \in \mathbb{Z}/n\mathbb{Z}$ を次で定める.

$$\rho(\zeta_n) = \zeta_n^{j(\rho)}, \qquad \rho(\sqrt[n]{a}) = \sqrt[n]{a} \cdot \zeta^{i(\rho)}$$

このとき,

$$\varphi(\rho) = \begin{pmatrix} j(\rho) & i(\rho) \\ 0 & 1 \end{pmatrix} \in \mathrm{Aff}_1(\mathbb{Z}/n\mathbb{Z}), \qquad \rho \in G$$

は群の単射準同型写像となる. 実際, ρ, $\rho' \in G$ とすると,

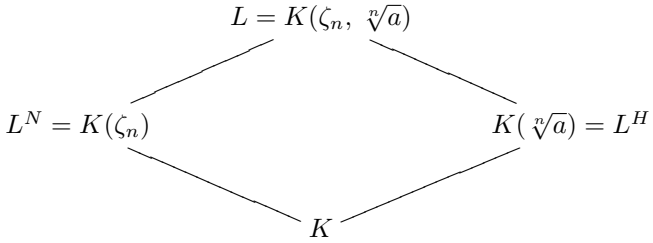
$$\begin{aligned} \rho(\rho'(\zeta_n)) &= \rho(\zeta_n^{j(\rho')}) = \zeta_n^{j(\rho)j(\rho')} \\ \rho(\rho'(\sqrt[n]{a})) &= \rho(\sqrt[n]{a} \cdot \zeta_n^{i(\rho')}) = \rho(\sqrt[n]{a})\rho(\zeta_n^{i(\rho')}) = \sqrt[n]{a} \cdot \zeta_n^{i(\rho)} \cdot \zeta_n^{j(\rho)i(\rho')} = \sqrt[n]{a} \cdot \zeta_n^{j(\rho)i(\rho')+i(\rho)} \end{aligned}$$

であり, 一方,

$$\begin{pmatrix} j(\rho) & i(\rho) \\ 0 & 1 \end{pmatrix} \begin{pmatrix} j(\rho') & i(\rho') \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} j(\rho)j(\rho') & j(\rho)i(\rho') + i(\rho) \\ 0 & 1 \end{pmatrix}$$

となるので, G の作用の合成と行列の積が対応している. 単射性は, $j(\rho) = 1$, $i(\rho) = 0$ なら, $\rho(\zeta_n) = \zeta_n$, $\rho(\sqrt[n]{a}) = \sqrt[n]{a}$ から, $\rho = \mathrm{id}_L$ となり, $\mathrm{Ker}(\rho) = \{\mathrm{id}_L\}$ となることより従う.

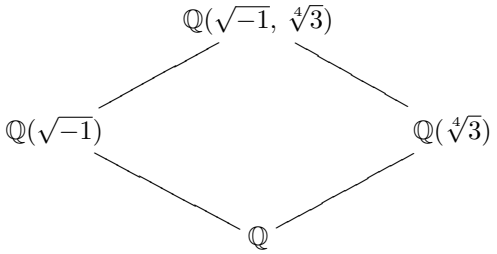
$j : G \to (\mathbb{Z}/n\mathbb{Z})^\times$ は群の準同型写像になる. $\mathrm{Ker}(j) = N$ とおくと, これは G の正規部分群で, $L^N = K(\zeta_n)$ となる. $H = \{\rho \in G \mid i(\rho) = 0\}$ も G の部分群であり, $L^H = K(\sqrt[n]{a})$ となる. $H \cap N = \{e\}$ であり, φ での像を考えると, $G = HN$ となることもわかる.



もっとも重要なことは, $X^n - a = 0$ の分解体について, 次が成立する ($\mathrm{char}(K) \nmid n$ とする) ことである.

> $\mathrm{Gal}(K(\zeta_n, \sqrt[n]{a})/K)$ は, $\mathrm{Aff}_1(\mathbb{Z}/n\mathbb{Z})$ の部分群に同型である. 特に $\mathrm{Gal}(K(\zeta_n, \sqrt[n]{a})/K)$ は, 可解群である.

例 4.9.2 $K = \mathbb{Q}$ として, $X^4 - 3 = 0$ の分解体を ($\mathbb{C}$ 内の部分体として) 考える. 1 の原始 4 乗根は, $\pm\sqrt{-1}$ であり, 次のような拡大体の列を得る.



上で与えた φ は, 上への同型写像 $\mathrm{Gal}(\mathbb{Q}(\zeta_n, \sqrt[4]{3})/\mathbb{Q}) \cong \mathrm{Aff}_1(\mathbb{Z}/4\mathbb{Z})$ を与える. 特に, $[\mathbb{Q}(\sqrt{-1}, \sqrt[4]{3}) : \mathbb{Q}] = 8$ である.

4.10 代数的可解性

正標数で起こる例外を排除するため, この節で考える体は, 全て標数 0 であるとする. 方程式が代数的に解けるという言葉は, その方程式の全ての根が, ベキ根を 4 則演算を利用して書ける事であると定義される. より正確には, 次のように定義される.

定義 4.10.1 $f(X) \in K[X]$ とし, L を f の分解体とする. 次のような体の拡大の列,

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_m, \quad K_i = K_{i-1}(\sqrt[n_i]{a_i}) \ (n_i \in \mathbb{N}),\ a_i \in K_{i-1} \tag{4.1}$$

が存在して, $L \subset K_m$ となるとき, f は代数的に可解であるという. ここで, ベキ乗根は, 1 のベキ根も許す事にする. このような拡大体を, べき根拡大という.

次の定理は, Galois による有名な定理であり,「可解群」という言葉の語源でもある.

定理 4.10.1（Galois） $\mathrm{char}(K) = 0$ とする. $f(X) = 0$ が代数的に可解であるための必要十分条件は, その方程式の Galois 群が可解群であることである.

証明. $f(X) = 0$ が代数的に可解であるとし, L を $f(X) = 0$ の分解体とする. 拡大体の列 (4.1) が存在して, $L \subset K_m$ とする. $n = n_1 \cdots n_m$ とし, ζ_n を 1 の原始 n 乗根とする. $K_0' = K_0(\zeta_n)$, $K_i' = K_0' K_i$ としてもベキ根拡大になり, $L \subset K_m'$ なので, 初めから K_0 は原始 n 乗根を含むと仮定して良い. K_m を含む K の代数的閉包を $\overline{K}$ とする.

$K = K_0$ は 1 の原始 n_1 乗根を含むので $K_0(\sqrt[n_1]{a_1})$ は K 上の Galois 拡大になり, $\mathrm{Gal}(K_1/K)$ は巡回群で, 特に可換である. K_1/K_0 は代数拡大なので, $a_2 \in K_1$ は, K_0 上代数的である. $L_1 = K_1$ とする. a_2 の $\overline{K}$ での K 上の共役元 (a_2 の K 上の最小多項式の $\overline{K}$ での根) を, $a_2 = a_{21}, a_{22}, \ldots, a_{2j_2}$ とし, $L_2 = K_1(\sqrt[n_2]{a_{21}}, \ldots, \sqrt[n_2]{a_{2j_2}})$ とすると $L_2 \supset K_2$ である. $\zeta_{n_2} \in K_1$ なので, 系 4.9.1 より, L_2/K_2 は Galois 拡大で, $\mathrm{Gal}(L_2/K_2)$ は Abel 群である. さらに, L_2 は, $(X^{n_2} - a_{21})(X^{n_2} - a_{22}) \cdots (X^{n_2} - a_{2j_2}) = 0$ の分解体であるが, $a_{21}, \ldots, a_{2j_2}$ が a_2 の K_0 上の全ての共役元であるため, $(X^{n_2} - a_{21})(X^{n_2} - a_{22}) \cdots (X^{n_2} - a_{2j_2}) \in K_0[X]$ である. すなわち, L_2/K_0 正規拡大になり, Galois 拡大になる (分離性は $\mathrm{char}(K) = 0$ から自動的に従う).

$a_3 \in K_2 \subset L_2$ に対しても上と同じ操作をすると, L_2 上の Abel 拡大体 L_3 で, $L_3 \supset K_3$ かつ L_3/K_0 が Galois 拡大となるものが作れる. この操作を繰り返すことにより, 次のような拡大体の列が作れる.

$$K = K_0 \subset L_1 = K_1 \subset L_2 \subset L_3 \subset \cdots \subset L_m,$$
$$K_i \subset L_i \ (i = 1, \ldots, m), \quad \mathrm{Gal}(L_{i+1}/L_i) \text{ は可換}, \qquad L_i/K_0 \text{は Galois 拡大 } (i = 1, \ldots, m)$$

$G = \mathrm{Gal}(L_m/K_0)$ とし, Galois 対応で L_i に対応する G の部分群を G_i とする. 体の拡大 $K_0 \subset L_i \subset L_m$ を考える. L_m/K_0 が Galois 拡大なので, L_m/L_i も Galois 拡大で, $\mathrm{Gal}(L_m/L_i) = G_i$ である. 一方, 体の拡大 $L_i \subset L_{i+1} \subset L_m$ において, L_{i+1}/L_i が Galois 拡大なので, $G_i \rhd G_{i+1}$ である. さらに $\mathrm{Gal}(L_{i+1}/L_i) \cong G_i/G_{i+1}$ は可換群になる. すなわち, $G \rhd G_1 \rhd \cdots \rhd G_m = \{e\}$ で G_i/G_{i+1} がすべて可換群になるので, G は可解群になる. Galois 対応で $L \subset L_m$ に対応する G の部分群を N とすると, L/K_0 は Galois 拡大だから $G \rhd N$ であり, $\mathrm{Gal}(L/K_0) \cong G/N$ となる. G が可解群なので, $\mathrm{Gal}(L/K_0) \cong G/N$ も可解群である.

逆に, $G = \mathrm{Gal}(L/K)$ が可解群であるとする. このとき, G の正規列,

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_{m-1} \rhd G_m = \{e\}$$

で, G_i/G_{i+1} が巡回群であるものがとれる. K_i を Galois 対応で G_i に対応する L の部分体とする. $n = |G|$ として, $K'_0 = K_0(\zeta_n)$ とする. $K'_i = K'_{i-1}K_i$ とすると, 次の拡大体の列ができる.

$$K'_0 \subset K'_1 \subset \cdots \subset K'_i \subset K'_{i+1} \subset \cdots \subset K'_m$$

Galois の推進定理 (定理 4.7.4) から, 体の拡大 K'_{i+1}/K'_i は Galois 拡大で,

$$\mathrm{Gal}(K'_{i+1}/K'_i) \cong \mathrm{Gal}(K_{i+1}/(K_{i+1} \cap K'_i)) \subset \mathrm{Gal}(K_{i+1}/K_i) \cong G_i/G_{i+1}$$

となる. よって, $\mathrm{Gal}(K'_{i+1}/K'_i)$ は巡回群の部分群と同型であるので, 巡回群になる. ζ_n の取り方から, K'_i は 1 の原始 $|\mathrm{Gal}(K'_{i+1}/K'_i)|$–乗根を含む. よって, 定理 4.9.1 より, $a \in K'_i$ が存在して, $K'_{i+1} \subset K'_i(\sqrt[d_i]{a})$, $d_i = |\mathrm{Gal}(K'_{i+1}/K'_i)|$ となる. $L \subset K_m \subset K'_m$ なので, $f(X) = 0$ の根はべき根を用いた表示ができる.

一般の方程式

k を標数 0 の体とし, $a_1, \ldots, a_n$ を不定元とする. $K = k(a_1, \ldots, a_n)$ とする. n 次方程式の根の公式 (代数的な解法) を求めるということは,

$$f(T) = T^n + a_1 T^{n-1} + \cdots + a_n \in K[T]$$

に対して, $f(T) = 0$ の根を, $a_1, \ldots, a_n$ のベキ根と 4 則を利用して書き下すことに他ならない.

$f(T) = 0$ の根を $\theta_1, \ldots, \theta_n$ とする. $s_k(\theta_1, \ldots, \theta_n)$ を $\theta_1, \ldots, \theta_n$ の k 次基本対称式とすると, $a_k = (-1)^k s_k$ である. K 上の $f(T) = 0$ の分解体は, $K(\theta_1, \ldots, \theta_n)$ である. 例 4.7.3 より, $k(\theta_1, \ldots, \theta_n)/k(a_1, \ldots, a_n)$ の Galois 群は n 次対称群となる. 5 次以上の対称群は可解群ではないので, 次を得る.

系 4.10.1 (Abel, Galois) $\mathrm{char}(K) = 0$ とする. K 上の 5 次以上の一般の方程式には, 代数的な解法が存在しない. すなわち, ベキ根と 4 則だけを用いた「根の公式」を作ることができない.

正標数の場合は, ベキ乗根を定める方程式 $X^n - a = 0$ が分離的でないことが起こるので, 上のような明解な形で代数的可解性を定式化できない. 標数 $p\,(> 0)$ の場合には, p 次の巡回拡大は, Artin–Schreier(アルチン–シュライアー) 拡大と呼ばれるものが, ベキ根拡大の代用物として利用される. このあたりの詳しい内容は, [3] を参照していただきたい.

上で, 1 のベキ根 $\sqrt[n]{1}$ を考えたが, これ自身, 最初の体の元のベキ根による表記ができるかという問題もある. 実際に n が小さい場合に 1 の原始 n 乗根の 1 つ ζ_n を具体的に書くと,

$$\zeta_3 = -\zeta_6 = \frac{-1 + \sqrt{-3}}{2}$$
$$\zeta_4 = \sqrt{-1}$$
$$\zeta_5 = \frac{\sqrt{5} - 1}{4} + \frac{\sqrt{10 + 2\sqrt{5}}}{4}\sqrt{-1}$$

となる. 7 乗根についても, 例 4.8.2 で見たように, 3 次方程式と 2 次方程式の積み上げで根が求まるので, ベキ根を用いて表示可能である (3 次方程式は, 平方根と立方根を用いて解ける).

実際に, 任意の 1 の原始 n 乗根は, 有理数のベキ根を用いて書ける事が次のように示される. $L_n = \mathbb{Q}(\{\zeta_k\}_{k \leqq n})$ とおく. $\mathbb{Q} = L_1 = L_2 \subset L_3 \subset L_4 \subset \cdots \subset L_n$ であり, $L_n = L_{n-1}(\zeta_n)$ である.

命題 4.10.1　$\mathbb{Q}$ 上で考える. ζ_n を 1 の原始 n 乗根, $L_n = \mathbb{Q}(\zeta_1, \ldots, \zeta_n)$ とする. このとき, 体の拡大の列

$$K_0 = \mathbb{Q} \subset K_1 \subset \cdots \subset K_N$$

で次を満たすものが存在する.

1. 拡大 K_i/K_{i-1} は素数 p_i に対する p_i 次拡大 $(i = 1, \ldots, N)$.
2. $K_{i+1} \subset K_i(\sqrt[p_i]{a_i}), \quad a_i \in K_i$
3. $L_n \subset K_N$

証明.　$L_n \supset L_{n-1}$ の間に定理を満たす列が存在することを示せばよい. $L_n = L_{n-1}(\zeta_n)$ だから, $[L_n : L_{n-1}] \leqq \varphi(n) < n$ である. $\mathrm{Gal}(L_n/L_{n-1})$ は $(\mathbb{Z}/n\mathbb{Z})^\times$ の部分群と同型で, 特に Abel 群である. 有限生成 Abel 群の基本定理 (定理 2.7.3) を利用すると, $\mathrm{Gal}(L_n/L_{n-1})$ の部分群の列と, 素数の列 p_i で,

$$G_0 = \mathrm{Gal}(L_n/L_{n-1}) \rhd G_1 \rhd \cdots \rhd G_N = \{e\}, \qquad G_i/G_{i+1} \cong \mathbb{Z}/p_i\mathbb{Z}$$

となるようにできる. $p_i \leqq n-1$ なので, $L_{n-1} \ni \zeta_{p_i}$ である. $K_i = L_n^{G_i}$ とすると, Galois の基本定理から, $\mathrm{Gal}(K_{i+1}/K_i) \cong G_i/G_{i+1} \cong \mathbb{Z}/p_i\mathbb{Z}$ である. よって, 定理 4.9.1 より, ある $a_i \in K_i$ が存在して, $K_{i+1} \subset K_i(\sqrt[p_i]{a_i})$ である.

上の命題から, $\mathbb{Q}$ 上の 1 のベキ根は, ベキ根と 4 則を繰返し計算することで得られることがわかる.

4.11　判別式

最高次の係数が 1 でない場合は議論が煩雑になるので, 以下では, monic な多項式だけを考える.

定義 4.11.1　$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in K[X]$ を monic な多項式とする. $f(X) = 0$ の根を $\theta_1, \ldots, \theta_n \in \overline{K}$ ($\overline{K}$ は K の代数的閉包) とする. このとき,

$$D(f) = \prod_{i<j} (\theta_i - \theta_j)^2$$

を f の判別式 (determinant または discriminant) という.

定義から, 次の命題は明らかである.

命題 4.11.1　$f(X) = 0$ が重根を持つ必要十分条件は, $D(f) = 0$ である.

例 4.11.1

1. $f(X) = X^2 + aX + b$ とし, その根を α, β とすると, 根と係数の関係より, $D(f) = (\alpha - \beta)^2 = (\alpha + \beta)^2 - 4\alpha\beta = a^2 - 4b$.
2. $f(X) = X^3 + pX + q$ とする. $f(X) = 0$ の根を $\theta_1, \theta_2, \theta_3$ とすると, $X^3 + pX + q = (X - \theta_1)(X - \theta_2)(X - \theta_3)$ である. 両辺を微分すると, $3X^2 + p = (X - \theta_1)(X - \theta_2) + (X - \theta_2)(X - \theta_3) + (X - \theta_3)(X - \theta_1)$ となる. 両辺に $\theta_1, \theta_2, \theta_3$ を代入すると,

$$\begin{cases} 3\theta_1^2 + p = (\theta_1 - \theta_2)(\theta_1 - \theta_3) \\ 3\theta_2^2 + p = (\theta_2 - \theta_1)(\theta_2 - \theta_3) \\ 3\theta_3^2 + p = (\theta_3 - \theta_1)(\theta_3 - \theta_2) \end{cases}$$

を得る. 両辺の積を取ると,

$$\begin{aligned}
-D(f) &= (3\theta_1^2+p)(3\theta_2^2+p)(3\theta_3^2+p) \\
&= 27(\theta_1\theta_2\theta_3)^2 + 9(\theta_1^2\theta_2^2+\theta_2^2\theta_3^2+\theta_3^2\theta_1^2)p + 3(\theta_1^2+\theta_2^2+\theta_3^2)p^2 + p^3 \\
&= 27q^2 + 9\left\{(\theta_1\theta_2+\theta_2\theta_3+\theta_3\theta_1)^2 - 2\theta_1\theta_2\theta_3(\theta_1+\theta_2+\theta_3)\right\}p \\
&\qquad +3\left\{(\theta_1+\theta_2+\theta_3)^2 - 2(\theta_1\theta_2+\theta_2\theta_3+\theta_3\theta_1)\right\}p^2 + p^3 \\
&= 27q^2 + 4p^3
\end{aligned}$$

となる. 従って, $D(f) = -(4p^3+27q^2)$ を得る.

問 4.11.1　1. $f(X) \in \mathbb{Q}[X]$ を monic な 3 次式とするとき, $f(X)=0$ が虚数根を持つことと, $D(f)<0$ は同値であることを示せ.

2. $f(X) \in \mathbb{Q}[X]$ を monic な 4 次式としたとき, $f(X)=0$ は虚数根を持つが $D(f)>0$ となる f の例を与えよ.

上の問でもわかるように, 実係数の方程式が虚数根を持つことの判定に判別式を利用できるのは, 3 次方程式までである.

一般に, $\theta_i, \ldots, \theta_n$ に対して, その差積を

$$\Delta(\theta_1, \ldots, \theta_n) = \prod_{i<j}(\theta_i - \theta_j)$$

とおくと, 定義から, $D(f) = \Delta(\theta_1, \ldots, \theta_n)^2$ である. 線形代数学で学んだように[*6], $\sigma \in S_n$ とすると, $\Delta(\theta_{\sigma(1)}, \ldots, \theta_{\sigma(n)}) = \mathrm{sgn}(\sigma)\Delta(\theta_1, \ldots, \theta_n)$ が成立する. 両辺を 2 乗すると $D(f)$ は, 根の置換をしても変化しないことがわかる. よって, 次が証明された.

命題 4.11.2　$f(X) \in K[X]$ を monic な多項式とする.

1. f の判別式 $D(f)$ は, f の根の置換によって不変である. 特に, $D(f)$ は f の係数の多項式になる.
2. f の根の差積 $\sqrt{D(f)}$ は, 根の偶置換によって不変である.

上の命題の 2. を用いると, 次の定理がわかる.

定理 4.11.1　K を標数 0 の体とし, $f(X) \in K[X]$ を K 上既約な monic n 次多項式とする. L を K の分解体とするとき, $\mathrm{Gal}(L/K) \subset A_n$ である必要十分条件は, $\sqrt{D(f)} \in K$ である.

証明.　L を $f(X)=0$ の分解体とし, $G = \mathrm{Gal}(L/K)$ とする. G は $f(X)=0$ の根の置換を与えるので, $G \subseteq S_n$ である. $H = G \cap A_n$ とおき, この部分群に対応する部分体 L^H を考える. 上のことから, $\sqrt{D(f)} \in L^H$ である. $G \subset A_n$ なら $G = H$ で $L^H = L^G = K$ となるので, $\sqrt{D(F)} \in K$ となる. 逆に, $\sqrt{D(f)} \in K$ なら, G の任意の元は根の偶置換として作用しなければならないので, $G \subset A_n$

一般に方程式の Galois 群を求めるのは難しいが, 上の定理から判別式の値は, Galois 群に対するひとつの制限を与えることがわかる.

命題 4.11.2, 1. より, $D(f)$ はもとの方程式の係数の多項式となることはわかるが, それを定義から具体的に

[*6] 差積は Vandermonde の行列式と符合しか違わない.

書き下すことは, 上で見たように, 3 次方程式でも大変である. さらに高次の (例えば 4 次でも) 方程式になると, その結果はかなり複雑である.

判別式に対しては, 実は別の計算式を与えることができ, それを用いると少しは易しい計算にできる. 判別式の定義から, 重根の判定条件が出るが, 重根の判定条件はもうひとつあり, $f(X)$ と $f'(X)$ が共通根を持つという事実である. これと終結式 (resultant) の理論を用いると, 判別式は行列式で表示できる[*7] (F). なお, Maple のような数式処理システムでは, 適当なコマンド (手続き) で判別式を計算することができる.

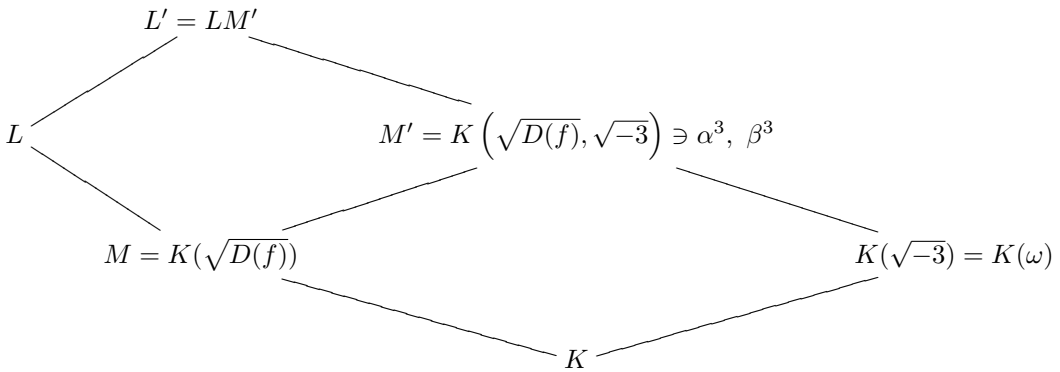
4.12 3 次方程式

ここでは, 一般の 3 次方程式の解法を Galois 理論に基づいて述べる. 話を簡単にするために, 体の標数は 2, 3 ではない (あるいは体は $\mathbb{Q}$ である) として考える. 1 の 3 乗根 $\omega = \dfrac{-1 \pm \sqrt{-3}}{2}$ が必要であるが, $K(\omega) = K(\sqrt{-3})$ であることに注意する.

最初に述べたように, 3 次方程式は $X^3 + pX + q = 0$ の形であるとして良い. ここで, p, q は不定元であるとする. すなわち, 一般の方程式を考える. $\theta_1, \theta_2, \theta_3$ の根とする. 根と係数の関係を再記すると,

$$\begin{cases} \theta_1 + \theta_1 + \theta_3 = 0 \\ \theta_1\theta_2 + \theta_2\theta_3 + \theta_3\theta_1 = p \\ \theta_1\theta_2\theta_3 = -q \end{cases}$$

である. 例 4.11.1, 2. より $D(f) = -(4p^3 + 27q^2)$ である. L を f の分解体とすると, $\mathrm{Gal}(L/K) \cong S_3$ であり, S_3 の導来列は, $S_3 \triangleright A_3 \triangleright \{e\}$ で $S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$, $A_3 \cong \mathbb{Z}/3\mathbb{Z}$ である. $M = L^{A_3} = K(\sqrt{D(f)})$ とする. Galois の基本定理から, $\mathrm{Gal}(L/M) \cong A_3$ であり, $M' = M(\omega) = K(\sqrt{D}, \sqrt{-3})$ とおくと, M' は 1 の 3 乗根を含む. $L' = L(\sqrt{-3}) = LM'$ を考えると, Galois の推進定理から, $\mathrm{Gal}(L'/M') \cong \mathrm{Gal}(L/(L \cap M')) \subset \mathrm{Gal}(L/M')$ となる.



定理 4.9.1 を考えると, $a \in M'$ が存在して, $L' = M'(\sqrt[3]{\alpha})$ となる. 定理 4.9.1 の証明 (注意 4.9.1) から,

$$\alpha = \theta_1 + \omega\theta_2 + \omega^2\theta_3$$

となるはずである. 実際, 少し面倒な計算であるが (1.1 節参照),

$$\omega = \frac{-1 + \sqrt{-3}}{2}, \qquad \sqrt{D(f)} = (\theta_1 - \theta_2)(\theta_1 - \theta_3)(\theta_2 - \theta_3)$$

[*7] 判別式も行列式も英語では determinant である. 行列式という言葉は (行列も) ある種の「意訳」で, 本来の意味からは, ずれている (matrix と同じ語源の言葉として, ロシアの人形マトリョーシカがある. 映画「マトリックス」も参考にすること.)

とすると,

$$\alpha^3 = -\frac{27}{2}q + \frac{3}{2}\sqrt{-3}\sqrt{D}$$

となることが示される. 同様に, $\beta = \theta_1 + \omega^2\theta_2 + \omega\theta_3$ とおくと, $\beta^3 = -\frac{27}{2}q - \frac{3}{2}\sqrt{-3}\sqrt{D}$ となるので, 1.1 節で述べた, 根の公式を得る.

4.13 4 次方程式

3 次方程式と同様の変形で, $f(X) = X^4 + pX^2 + qX + r$ として, $f(X) = 0$ の形の方程式を考えれば十分である. $\theta_1, \theta_2, \theta_3, \theta_4$ をこの方程式の根とし, $L = K(\theta_1, \theta_2, \theta_3, \theta_4)$ を $f(X)$ の分解体とする. 根と係数の関係は, 次で与えられる.

$$\begin{cases} \theta_1 + \theta_2 + \theta_3 + \theta_4 = 0 \\ \theta_1\theta_2 + \theta_1\theta_3 + \theta_1\theta_4 + \theta_2\theta_3 + \theta_2\theta_4 + \theta_3\theta_4 = p \\ \theta_1\theta_2\theta_3 + \theta_1\theta_2\theta_4 + \theta_1\theta_3\theta_4 + \theta_2\theta_3\theta_4 = -q \\ \theta_1\theta_2\theta_3\theta_4 = r \end{cases}$$

4 次対称群 S_4 の導来列は, 次のようになる.

$$S_4 \rhd A_4 \rhd V_4 \rhd \{e\}, \qquad V_4 = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

この導来列に応じて定まる部分体を考える. $L^{A_4} = K(\sqrt{D(f)})$ である. V_4 から定まる L の部分体を, $M = L^{V_4}$ とする. M の元は, V_4 の作用で不変であるので, $\theta_1, \theta_2, \theta_3, \theta_4$ の多項式で, V_4 で不変な元を探すと, 次があるのが簡単にわかる.

$$\begin{cases} \alpha = (\theta_1 + \theta_2)(\theta_3 + \theta_4) \\ \beta = (\theta_1 + \theta_3)(\theta_2 + \theta_4) \\ \gamma = (\theta_1 + \theta_4)(\theta_2 + \theta_3) \end{cases}$$

α, β, γ を S_4 の巡回置換 $(1,2,3)$ の $\{\theta_1, \theta_2, \theta_3, \theta_4\}$ への作用で動かすと, 長さ 3 の巡回置換になることがわかる. 同様に互換 $(1,2)$ を $\{\theta_1, \theta_2, \theta_3, \theta_4\}$ に作用させると, β, γ の互換が生じる. S_4 は, V_4 と $(1,2,3)$, $(1,2)$ で生成されるので, α, β, γ の基本対称式は S_4 の作用で不変になり, これらは K 上の 3 次方程式の根になることがわかる.

命題 4.13.1 上の α, β, γ は, 方程式 $X^3 - 2pX^2 + (p^2 - 4r)X + q^2 = 0$ の 3 つの根である. この方程式を分解方程式, 左辺を分解多項式という.

証明. 次の根と係数の関係を示せばよい.

$$\begin{cases} \alpha + \beta + \gamma = 2p \\ \alpha\beta + \beta\gamma + \gamma\alpha = p^2 - 4r \\ \alpha\beta\gamma = -q^2 \end{cases}$$

それぞれを計算する.

$$\begin{aligned} \alpha + \beta + \gamma &= (\theta_1 + \theta_2)(\theta_3 + \theta_4) + (\theta_1 + \theta_3)(\theta_2 + \theta_4) + (\theta_1 + \theta_4)(\theta_2 + \theta_3) \\ &= 2(\theta_1\theta_2 + \theta_1\theta_3 + \theta_1\theta_4 + \theta_2\theta_3 + \theta_2\theta_4 + \theta_3\theta_4) = 2p \end{aligned}$$

となり, 最初の式を得る.

$$\alpha\beta\gamma = (\theta_1+\theta_2)(\theta_3+\theta_4)(\theta_1+\theta_3)(\theta_2+\theta_4)(\theta_1+\theta_4)(\theta_2+\theta_3)$$

であるが, $\theta_1+\theta_2+\theta_3+\theta_4=0$ を利用すると.

$$\alpha\beta\gamma = -\left\{(\theta_1+\theta_2)(\theta_1+\theta_3)(\theta_1+\theta_4)\right\}^2$$

となる. ここで,

$$\begin{aligned}(\theta_1+\theta_2)(\theta_1+\theta_3)(\theta_1+\theta_4) &= \theta_1^3+(\theta_2+\theta_3+\theta_4)\theta_1^2+(\theta_2\theta_3+\theta_3\theta_4+\theta_2\theta_4)\theta_1+\theta_2\theta_3\theta_4\\ &= (\theta_1+\theta_2+\theta_3+\theta_4)\theta_1^2+\theta_1\theta_2\theta_3+\theta_1\theta_3\theta_4+\theta_1\theta_2\theta_4+\theta_2\theta_3\theta_4\\ &= -q\end{aligned}$$

となるので, 3 番目の式を得る. 2 番目の式については,

$$\begin{aligned}\alpha\beta &= (\theta_1+\theta_2)(\theta_3+\theta_4)(\theta_1+\theta_3)(\theta_2+\theta_4)\\ &= (\theta_1+\theta_2+\theta_3+\theta_4)(\theta_1\theta_2\theta_3+\theta_1\theta_2\theta_4+\theta_1\theta_3\theta_4+\theta_2\theta_3\theta_4)+(\theta_1\theta_4-\theta_2\theta_3)^2\\ &= (\theta_1\theta_4-\theta_2\theta_3)^2\end{aligned}$$

が成立することを利用する. $\beta\gamma$, $\gamma\alpha$ は, 上の添え字を $(2,3,4)$ の巡回置換を施した式なので, $\beta\gamma=(\theta_1\theta_2-\theta_3\theta_4)^2$, $\gamma\alpha=(\theta_1\theta_3-\theta_2\theta_4)^2$ となる. 一方, 少し面倒な計算であるが,

$$p^2 = \sum_{1\leqq i<j\leqq 4}\theta_i^2\theta_j^2 - 2\theta_1\theta_2\theta_3\theta_4$$

がわかる. これらを組み合わせると 2 番目の式が得られる.

3 次方程式には, 代数的な解法があるので, α,β,γ が代数的に計算できる.

$$\alpha = (\theta_1+\theta_2)(\theta_3+\theta_4), \qquad \theta_1+\theta_2+\theta_3+\theta_4=0$$

より, $\theta_1+\theta_2$, $\theta_3+\theta_4$ は, 2 次方程式 $X^2+\alpha=0$ の根である. よって, $\theta_1+\theta_2=\sqrt{-\alpha}$, $\theta_3+\theta_4=-\sqrt{-\alpha}$ とできる. 同様にして, 次を得る.

$$\begin{cases}\theta_1+\theta_2=\sqrt{-\alpha}, & \theta_3+\theta_4=-\sqrt{-\alpha}\\ \theta_1+\theta_3=\sqrt{-\beta}, & \theta_2+\theta_4=-\sqrt{-\beta}\\ \theta_1+\theta_4=\sqrt{-\gamma}, & \theta_2+\theta_3=-\sqrt{-\gamma}\end{cases}$$

ただし, 平方根の取り方は独立ではなく,

$$\sqrt{-\alpha}\sqrt{-\beta}\sqrt{-\gamma} = (\theta_1+\theta_2)(\theta_1+\theta_3)(\theta_1+\theta_4) = -q$$

が成立するように取る必要がある. 上で得られた $\theta_i+\theta_j$ の式を連立方程式と見て逆に解くと, 次が得られる.

$$\begin{aligned}\theta_1 &= \frac{1}{2}\left(\sqrt{-\alpha}+\sqrt{-\beta}+\sqrt{-\gamma}\right)\\ \theta_2 &= \frac{1}{2}\left(\sqrt{-\alpha}-\sqrt{-\beta}-\sqrt{-\gamma}\right)\\ \theta_3 &= \frac{1}{2}\left(-\sqrt{-\alpha}+\sqrt{-\beta}-\sqrt{-\gamma}\right)\\ \theta_4 &= \frac{1}{2}\left(-\sqrt{-\alpha}-\sqrt{-\beta}+\sqrt{-\gamma}\right)\end{aligned}$$

これは, Ferrari(フェラリ) の公式と呼ばれる.

命題 4.13.2　これまでの記号を用いる.

1. $p, q, r \in K$ としたとき, $f(X)$ が重根を持たなければ, α, β, γ は互いに異なる.
2. $f(X)$ の判別式と, その分解方程式の判別式は一致する.

証明.

$$\begin{aligned}\alpha - \beta &= (\theta_1 + \theta_2)(\theta_3 + \theta_4) - (\theta_1 + \theta_3)(\theta_2 + \theta_4) = \theta_1\theta_3 + \theta_2\theta_4 - \theta_1\theta_2 - \theta_3\theta_4 \\ &= (\theta_1 - \theta_4)(\theta_3 - \theta_2)\end{aligned}$$

となる. 上の式の添字に, $(2,3,4)$ の巡回置換を順に施すと, 次を得る.

$$\beta - \gamma = (\theta_1 - \theta_2)(\theta_4 - \theta_3), \qquad \gamma - \alpha = (\theta_1 - \theta_3)(\theta_2 - \theta_4)$$

これより, 1. が従う. また,

$$(\alpha - \beta)^2(\beta - \gamma)^2(\gamma - \alpha)^2 = \prod_{1 \leqq i < j \leqq 4} (\theta_i - \theta_j)^2$$

となり, 判別式の一致がわかる.

注意 4.13.1　1.　命題 4.13.1 における, $M = L^{V_4}$ の生成元 α, β, γ の取り方は, いろいろあり得る. 実際, 参考文献 [14] では, 次の 3 つを生成元と取っている.

$$\tau_1 = \theta_1\theta_2 + \theta_3\theta_4, \quad \tau_2 = \theta_1\theta_3 + \theta_2\theta_4, \quad \tau_3 = \theta_1\theta_4 + \theta_2\theta_3$$

生成元の選び方を変えれば, 分解多項式の形もそれに応じて変化し, 解法も変化する (最終的な根は, どう選んでも同じになる.). 命題 4.13.1 と上の選び方との関係は, 次で与えられる.

$$\alpha = \tau_2 + \tau_3, \quad \beta = \tau_1 + \tau_3, \quad \gamma = \tau_1 + \tau_2$$

$L^{V_4} = M$ の 3 つの生成元の選び方は, 次のように決まる.

- 元の方程式の 4 つの根 θ_1, θ_2, θ_3, θ_4 の 2 次の斉次式である.
- 上の 2 次の斉次式で, V_4 の作用で不変な空間は, K 上の 4 次元ベクトル空間である (証明を考えよ) が, そのうち, S_4 の作用で動く元から選ぶ (S_4 の作用で不変な元は K の元なので選べない.).
- 上の空間の中からひとつの元を選んで, τ_1 とすると, 残りのふたつは, S_4 の $\{\theta_1, \theta_2, \theta_3, \theta_4\}$ への作用 (例えば, 巡回置換 $(1,2,3)$) で動かして決める (S_4–軌道. $\mathrm{Gal}(M/K) \cong S_4/V_4 \cong S_3$ なので, もうふたつが出てくる.).

歴史的にも, Lagrange は, 上のように分解多項式をいく通りにも取り替えられることに, 気付いていたようである. 元の方程式の根から作られる上の 3 つの数への S_4 の作用が, 3 次の対称群の作用と同じである (i.e. $S_4/V_4 \cong S_3$) が, 4 次方程式の解法の根拠であることに気付くことができていれば, Lagrange は Galois より先に, Galois 理論に到達できたかもしれない.

2. $M = L^{V_4}$ を定める分解多項式を上の状況で変更した場合, 命題 4.13.2, 2. は, 次のように変更される.

命題 4.13.2 2'. 分解多項式の判別式は元の方程式の判別式の 0 でない平方数倍になる.

実際, μ_1, μ_2, μ_3 を分解多項式の 3 つの根として, その差積

$$\Delta(\mu_1, \mu_2, \mu_3) = (\mu_1 - \mu_2)(\mu_1 - \mu_3)(\mu_2 - \mu_3)$$

を考える．μ_i の取り方から，これは $\theta_1, \theta_2, \theta_3, \theta_4$ の多項式として 0 ではなく，$\theta_1, \theta_2, \theta_3, \theta_4$ の 6 次の多項式になる．S_4 による θ_i への作用を上の交代式に作用させると，$\Delta(\mu_1, \mu_2, \mu_3)$ は，θ_i の交代式になる．実際，μ_i は V_4 の作用で不変だから，S_4 の $\Delta(\mu_1, \mu_2, \mu_3)$ への作用は，$S_4/V_4 \cong S_3$ の μ_i への置換の作用になるからである．よって，定理 E.2 の証明と同じ議論をすると，定数 $C(\neq 0)$ が存在して，

$$\Delta(\mu_1, \mu_2, \mu_3) = C\Delta(\theta_1, \theta_2, \theta_3, \theta_4)$$

となり，判別式は根の差積の平方なので上の主張を得る．

3. **Ferrari の解法** ([15])．4 次方程式の解法を最初に発見した Ferrari の方法を解説する．出発点の方程式を $X^4 + pX^2 + qX + r = 0$ としてよいことは，これまでと同様である．λ をうまく選んで，

$$(X^2 + \lambda)^2 = (mX + n)^2$$

の形に変形することを考える．

$$X^4 + pX^2 + qX + r = (X^2 + \lambda)^2 + (p - 2\lambda)X^2 + qX + r - \lambda^2$$

なので，上の形にできるためには，上の式の最後の X の 2 次式の部分が 1 次式の平方になることになり，それは，2 次方程式 $(2\lambda - p)X^2 - qX + \lambda^2 - r = 0$ が重根を持つことになる．2 次方程式の判別式を利用すると，その条件は，

$$q^2 - 4(2\lambda - p)(\lambda^2 - r) = 0$$

となり，λ に関する上の 3 次方程式が解ければ，元の 4 次方程式も解けることになる．

上に現れる λ の正体は何かを調べてみる．元の 4 次方程式の根を $\theta_1, \theta_2, \theta_3, \theta_4$ とする．上の解法で，もとの 4 次方程式は，次のように因数分解される．

$$(X^2 + mX + \lambda + n)(X^2 - mX + \lambda - n) = 0$$

θ_1, θ_2 を前の因子の根，θ_3, θ_4 を後の因子の根とすると，根と係数の関係より，次を得る．

$$\theta_1\theta_2 = \lambda + n, \qquad \theta_3\theta_4 = \lambda - n$$

これより，$\lambda = \dfrac{\theta_1\theta_2 + \theta_3\theta_4}{2}$ を得るので，λ は分解体の V_4 不変な元 (i.e. $\lambda \in L^{V_4}$) であることがわかる．つまり，Ferrari は，4 次方程式の分解多項式をうまい方法で見つけることができた，と言える．

4.14 方程式の Galois 群

この節でも，方程式の最高次の係数は 1 とする．

命題 4.14.1 $f(X) \in K[X]$ を K 上既約かつ分離的な多項式とする．$f(X)$ が n 次式で，$\theta_1, \ldots, \theta_n$ を f の根とする．$L = K(\theta_1, \ldots, \theta_n)$ を $f(X)$ の分解体とするとき，$\mathrm{Gal}(L/K)$ は根の集合 $\{\theta_1, \ldots, \theta_n\}$ に推移的に作用する．

証明 根の集合の $\mathrm{Gal}(L/K)$ の作用での軌道分解を $\{\theta_1, \ldots, \theta_n\} = \mathcal{O}_1 \cup \cdots \cup \mathcal{O}_k$ とすると，$f_i(X) = \prod_{\theta \in \mathcal{O}_i} (X - \theta)$ とおくと，$\mathcal{O}_i$ が $\mathrm{Gal}(L/K)$ の軌道であることから，$f_i(X) \in K[X]$ であり，作り方から，$f_i(X)$ は f の因子である．よって，f が既約なら $k = 1$ であり，f は根の集合に推移的に作用する．

上のことから，既約かつ分離的な n 次方程式の Galois 群は S_n の部分群で，$\{1, \ldots, n\}$ に推移的に作用する群と同型である．特に $|\mathrm{Gal}(L/K)|$ は n の倍数である．

3 次方程式の Galois 群

$f(X) \in K[X]$ を分離的かつ既約な 3 次多項式とする．これまでに述べたことから, f の Galois 群は次で与えられる．

定理 4.14.1　上の記号の下で, $D(f)$ を f の判別式とすると,

1. $\sqrt{D(f)} \in K$ なら, f の Galois 群は 3 次交代群 A_3 に同型である．
2. $\sqrt{D(f)} \notin K$ なら, f の Galois 群は 3 次対称群 S_3 に同型である．

4 次方程式の Galois 群

$f(X)$ を K 上の分離的かつ既約な 4 次多項式とする．$f(X) = 0$ の根を $\theta_1, \theta_2, \theta_3, \theta_4$ とし f の分解体を $L = K(\theta_1, \theta_2, \theta_3, \theta_4)$ とする．上で述べた 4 次方程式の解法より, f に対して分解多項式 g が定まる．これは, K 上の 3 次多項式であり, さらに f の判別式と g の判別式は一致する．

f の Galois 群を G と書く．命題 4.14.1 より, G は S_4 の部分群で, $f(X) = 0$ の根の集合 $\{\theta_1, \theta_2, \theta_3, \theta_4\}$ に推移的に作用する．特に, $|G|$ は 4 の倍数 (かつ 24 の約数) である．簡単な計算により, このような G は, 以下のように分類される．

1. 位数 4: (a) $G =< (1,2,3,4) >,\ G =< (1,3,4,2) >, G =< (1,4,2,3) >$　　(4 次の巡回群)
   (b) $G = V_4 = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$(Klein の 4 元群, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ と同型)
2. 位数 8: $P_1 = V_4 \cup (1,2)V_4,\ P_2 = V_4 \cup (1,3)V_4,\ P_3 = V_4 \cup (1,4)V_4$
   (これらは, S_4 の Sylow 2–部分群で, すべて互いに共役である．また, 位数 8 の 2 面体群と同型.)
3. 位数 12: 4 次交代群 A_4
4. 位数 24: 4 次対称群 S_4

S_4 の導来列は, $S_4 \rhd A_4 \rhd V_4 \rhd \{e\}$ である．この導来列に Galois 対応で対応する L の部分体 (部分群に対応する固定体) を, $K \subset K(\sqrt{D(f)}) \subset M \subset L$ とする．M は, 分解方程式 $g(X) = 0$ の分解体であり, $\alpha = (\theta_1 + \theta_2)(\theta_3 + \theta_4)$, $\beta = (\theta_1 + \theta_3)(\theta_1 + \theta_4)$, $\gamma = (\theta_1 + \theta_4)(\theta_2 + \theta_3)$ とすると, $M = K(\alpha, \beta, \gamma)$ である．

まず, 判別式の性質と分解方程式の性質から, 次のことが容易に分かる．

定理 4.14.2　上の記号の下で, 分解多項式 $g(X)$ が K 上既約であるとする．

1. $\sqrt{D(f)} \in K$ なら f の Galois 群は A_4 である．
2. $\sqrt{D(f)} \notin K$ なら f の Galois 群は S_4 である．

逆に, $\mathrm{Gal}(L/K)$ が S_4 または A_4 なら, $g(X)$ は K 上既約で, $\mathrm{Gal}(L/K) = S_4 \Leftrightarrow \sqrt{D(f)} \notin K$, $\mathrm{Gal}(L/K) = A_4 \Leftrightarrow \sqrt{D(f)} \in K$ となる．

証明.　$g(X)$ が K 上既約であるので, 3 次方程式の議論から, 体の拡大 $K \subset M \subset L$ において, $[M : K] = 3$ または, $[M : K] = 6$ である．よって, $[L : K] = [L : M][M : K]$ は 3 の倍数となる．一方, $[L : K] = |\mathrm{Gal}(L/K)|$ は 4 の倍数なので, $[L : K]$ は, 12 の倍数となる．よって, 上の部分群の分類から, $\mathrm{Gal}(L/K)$ は S_4 か A_4 となり, 定理 4.11.1 から, 前半部分を得る．

逆に, $\mathrm{Gal}(L/K) \supset A_4$ とする．このとき, $[L : K]$ は 12 または 24 となり 3 の倍数となる．部分体の列,

$L \supset M \supset K$ を考えると, $\mathrm{Gal}(L/M) \subset V_4$ より, $[L : M]$ が 3 の倍数になることはありえない. よって, $[M : K]$ は 3 の倍数である必要があり, 特にこのとき $g(X)$ は K 上既約である.

$g(X)$ が K 上既約である場合は上でつくされるので, 可約な場合を考える. この場合, 上の部分群の分類から $\mathrm{Gal}(L/K)$ は Klein の 4 元群, 位数 8 の 2 面体群, 位数 4 の巡回群のいずれかである.

$g(X)$ が K 上 1 次式の積に分解される場合を考える. すなわち, $g(X) = (X-\alpha)(X-\beta)(X-\gamma)$, $\alpha, \beta, \gamma \in K$ となる場合である. この場合, $M = K$ であり, $[L : K] = 4$ で $\mathrm{Gal}(L/K) = V_4$ となる. 逆に, $\mathrm{Gal}(L/K) = V_4$ なら, $M = K$ が成立するはずだから, $g(X) = 0$ の根はすべて K に含まれ, $g(X)$ は K 上 1 次式の積に分解する.

次に, $g(X)$ が K で 1 次式と 2 次式の積に分解される場合を考える. $g(X) = 0$ の根 α, β, γ のうち, $\alpha = (\theta_1 + \theta_2)(\theta_3 + \theta_4) \in K$ で, $\beta, \gamma \notin K$ として良い. $\alpha \in K$ であるということは, 任意の $\sigma \in \mathrm{Gal}(L/K)$ に対して, $\sigma(\alpha) = \alpha$ が成立するということである. 上で現れた S_4 の部分群で, $\sigma(\alpha) = \alpha$ が常に成立するような部分群は, P_1 と $< (1, 4, 2, 3) >$ の 2 つだけである. 体の拡大 L/M を考えると, $f(X) \in M[X]$ と見て, L は f の最小分解体であることに注意する. また, $\mathrm{Gal}(L/M) = \mathrm{Gal}(L/K) \cap V_4$ である.

$\mathrm{Gal}(L/K) = P_1$ であるとすると, $\mathrm{Gal}(L/M) = V_4$ となり, この群は $f(X) = 0$ の根 $\{\theta_1, \theta_2, \theta_3, \theta_4\}$ に推移的に作用する. すなわち, $f(X)$ は M 上既約になる.

$\mathrm{Gal}(L/K) =< (1, 4, 2, 3) >$ とすると, $\mathrm{Gal}(L/M) = \{e, (1, 2)(3, 4)\}$ となり, この群は $\{\theta_1, \theta_2, \theta_3, \theta_4\}$ に推移的に作用しない. すなわち, $f(X)$ は M 上可約 (2 次式の積) になる.

以上をまとめて, 次を得る.

命題 4.14.2　上の記号を用いることにする.

1. 分解方程式 $g(X) = 0$ が K 上 1 次式の積に分解するなら, $\mathrm{Gal}(L/K) = V_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
2. 分解方程式 $g(X) = 0$ が K 上 2 次式と 1 次式の積に分解するなら,
   (a)　$f(X)$ が $M = L^{\mathrm{Gal}(L/K) \cap V_4}$ 上既約なら, $\mathrm{Gal}(L/K) \cong Dih_8$ (位数 8 の 2 面体群)
   (b)　$f(X)$ が $M = L^{\mathrm{Gal}(L/K) \cap V_4}$ 上可約なら, $\mathrm{Gal}(L/K) \cong \mathbb{Z}/4\mathbb{Z}$

例 4.14.1 (［3］にある例)　以下の例では, $K = \mathbb{Q}$ とする. また, 既約性の判定は, 各自の演習問題とする.

1. $f(X) = X^4 - X - 1$ とする. f は $\mathbb{Q}$ 上既約であり, f の分解多項式は, $g(X) = X^3 + 4X + 1$ となる. $g(X)$ は $\mathbb{Q}$ 上既約であり, $D(g) = -(4 \cdot 4^3 + 27) = -283 = D(f)$ だから, $\sqrt{D(f)} \notin \mathbb{Q}$ となり, f の Galois 群は S_4 である.
2. $f(X) = X^4 + 6X^2 + 8X + 9$ とする. f は $\mathbb{Q}$ 上既約であり, f の分解多項式は, $g(X) = X^3 - 12X^2 + 64 = (X-4)^3 - 3 \cdot 4^2(X-4) - 4^3$ となる. $g(X)$ は $\mathbb{Q}$ 上既約である. $D(g) = -(4(-3 \cdot 4^2)^3 + 27 \cdot 4^6) = 4^6 3^4 = D(f)$ だから, $\sqrt{D(f)} = 4^3 3^2 \in \mathbb{Q}$ となり, f の Galois 群は A_4.
3. $f(X) = X^4 - 4X^2 + 1$ とする. f は $\mathbb{Q}$ 上既約であり, f の分解多項式は, $g(X) = X^3 + 8X^2 + 12X = X(X+2)(X+6)$ となる. よって, f の Galois 群は, $V_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
4. $f(X) = X^4 + X^2 - 1$ とする. f は $\mathbb{Q}$ 上既約であり, f の分解多項式は, $g(X) = X^3 - 2X^2 + 5X = X(X^2 - 2X + 5)$ となる. $g(X)$ の分解体は, $M = \mathbb{Q}(\sqrt{-1})$ であり, $f(X)$ は M 上既約である. 実際, $f(\alpha) = 0$ なら, $\alpha^2 = \dfrac{-1 \pm \sqrt{5}}{2}$ となるが, $\sqrt{5} \notin M$ なので, f は M 上 1 次の因子を持たない. また, $(X^2 + \alpha X + \beta)(X^2 + \gamma X + \delta) = f$ となる $\alpha, \beta, \gamma, \delta \in M$ が存在しないことも, 容易に示すことができる. よって, f の Galois 群は, 位数 8 の 2 面体群 Dih_8 に同型である.

5. $f(X) = X^4 - 4X^2 + 2$ とする．f は $\mathbb{Q}$ 上既約であり，f の分解多項式は，$g(X) = X^3 + 8X^2 + 8X = X(X^2 + 8X + 8)$ となる．$g(X)$ の分解体は，$\mathbb{Q}(\sqrt{2})$ であり，M 上 $f(X) = (X^2 - (2 + \sqrt{2}))(X^2 - (2 - \sqrt{2}))$ と分解されるから，f の Galois 群は，位数 4 の巡回群 $\mathbb{Z}/4\mathbb{Z}$ である．

5 次方程式についても，Galois 群を決定するアルゴリズムは存在するようである．しかし，それはかなり複雑なものになる．詳しくは，[2] (日本語訳，下) を参照してほしい．一般の高次方程式に対して，その Galois 群を求める簡単なアルゴリズムは無いと思われる．

Galois 理論に関しては，次のような問題が考えられる．

与えられた有限群 G に対して，G を Galois 群に持つような ($\mathbb{Q}$ 上の) 既約な多項式を求めよ．

これは，「Galois の逆問題」と呼ばれて，いろいろな研究がなされているようだが，一般的には未解決である．

4.15 作図問題

次が，古代ギリシアの 3 大作図問題と呼ばれるものである．

1. 角の 3 等分を作図せよ．
2. 2 倍の体積を持つ立方体を作図せよ (倍積問題)．
3. 円と同じ面積を持つ正方形を作図せよ (円積問題)．

ここで作図とは，次の条件を満たすことだけが許される．

- 使える道具は「定規」と「コンパス」のみ．
- 定規は 2 点を結ぶ直線を引くだけ (長さを測るメモリはついていない)．
- コンパスは円を描くだけ (同じ長さを測るだけ)．
- 操作は有限回で終了する．

上の問題は，長い間，解が分からなかったが，Descarte(デカルト) によって座標幾何が発見されたため，「方程式の問題」になった．3 大作図問題以外にも，正 n 角形の作図という問題もある．ここでは，これらについての解答を与える．

簡単に分かることであるが，数の和と差は作図できる．さらに 3 角形の相似を利用すれば，数の積と商も作図可能である．従って，作図可能な点の 4 則演算が作図で可能である．

問 4.15.1　数の積と商の作図方法を与えよ．

これら以外に作図できる点は，これまでに作図できた点から作られる 2 次方程式の根で与えられる点である．実際，上の作図方法から，新たに作図可能な点は，座標平面内で，次の 3 つの方法で得られる点である．

1. 直線と直線の交点 (交点の座標は，4 則演算を用いた計算で得られる)．
2. 直線と円の交点 (交点の座標は，2 次方程式を解くことで得られる)．
3. 円と円の交点 (交点の座標は，2 次方程式を解くことで得られる)．

a ($a > 0$) が作図可能なら，$\left(\dfrac{a-1}{2}, 0\right)$ を中心とする半径 $\dfrac{a+1}{2}$ の円の y 軸との交点は $(0, \pm\sqrt{a})$ なので，$\sqrt{a}$ は作図可能である．

これらのことから, 作図可能な点 (の座標) は,

有理数から始めて, 平方根を付け加えることを繰り返して得られる体の中にある.

ということがわかる.

さて, 上のことを踏まえると, 3 大作図問題は, 全て「不可能である」ということが結論される. なお, この否定的な解決に必要なのは拡大体の議論であって, Galois 理論は不要である.

円積問題につては, この講義では証明を与えることはできないが, 次が知られている.

定理 4.15.1（Lindemann, 1882） π は超越数である. すなわち, 有理数を係数とする方程式の根にはなりえない.

これにより, 円積問題は否定的に解決される. 実際, 半径 1 の円の面積, π を持つ正方形を作図するには, 1 辺が $\sqrt{\pi}$ の正方形が必要である. 数の積が作図可能だから, $\sqrt{\pi}$ が作図可能なら, π が作図可能であるということになるが, これは, π の超越性に矛盾する.

倍積問題

これは, $\sqrt[3]{2}$ の作図可能性を問題にしている. $\mathbb{Q}(\sqrt[3]{2})$ は $\mathbb{Q}$ の 3 次拡大体である. しかし, 作図可能な点は, $\mathbb{Q}$ 上 2 次拡大体を積み上げた体の中にあることが必要である. 特に, α が作図可能なら, ある $\mathbb{Q}$ の拡大体 L で, $[L:\mathbb{Q}] = 2^k$ かつ $\alpha \in L$ となるものが存在する. もし, $\sqrt[3]{2} \in L$ であるとすると, $M = \mathbb{Q}(\sqrt[3]{2})$ とすると, $2^k = [L:\mathbb{Q}] = [L:M][M:\mathbb{Q}] = 3[L:M]$ となり, 矛盾する. よって, 倍積問題は不可能であることがわかる.

角の 3 等分

角度によっては 3 等分した角度を作図できることもある. 実際, $90^\circ = \dfrac{\pi}{2}$ の 3 等分, $30^\circ = \dfrac{\pi}{6}$ は作図可能である. しかし, 3 等分をする一般的なアルゴリズムがあるわけではない. 例えば, $60^\circ = \dfrac{\pi}{3}$ の 3 等分, $20^\circ = \dfrac{\pi}{9}$ の作図は不可能であることが, 以下の考察からわかる.

さて, 20° の作図を考える. 20° が作図できれば, 直角 3 角形の作図から, $\cos 20^\circ$ も作図できる. ここで, cos の 3 倍角の公式 $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$ に $\theta = 20^\circ$ を代入すると,

$$\frac{1}{2} = 4\cos^3 20^\circ - 3\cos 20^\circ$$

が成立するから, $\cos 20^\circ$ は方程式,

$$8X^3 - 6X - 1 = 0$$

の根である. この方程式は, $\mathbb{Q}$ 上既約であるので, $\mathbb{Q}(\cos 20^\circ)$ は $\mathbb{Q}$ の 3 次拡大体である. すなわち, $\cos 20^\circ$ は $\mathbb{Q}$ 上 3 次拡大体に属する. 倍積問題とまったく同様にして, このような点は作図可能な点の集合に入らないことがわかる. よって, $\cos 20^\circ$ は作図可能ではない.

正 n 角形の作図 (これは Galois 理論を利用する)

座標平面を複素平面であると見る. 複素平面の中で, 単位円に内接する正 n 角形の作図を考えると, 複素数における 1 の原始 n 乗根,

$$\zeta_n = e^{\frac{2\pi\sqrt{-1}}{n}} = \cos\frac{2\pi}{n} + \sqrt{-1}\sin\frac{2\pi}{n} \in \mathbb{C}$$

が作図可能であるかという問題になる．作図可能性を複素平面で考えても, 上で述べてきたことは全く同様に成立する．すなわち, 与えられた複素数の和, 差, 積, 商は作図可能であり, 平方根も作図可能である．さらに共役な複素数も作図可能である．

問 4.15.2　複素数の 4 則演算及び平方根の作図方法を考えよ．(積, 商, 平方根については, 極形式を考えた方が易しいと思う.)

座標平面と同様に, 新たに作図可能な点は, もとの作図可能な点 (複素数) を係数とする 2 次方程式の根に限られることがわかる．実際, 例えば, 円と直線の交点を求めることを考える．複素数 $z = x + \sqrt{-1}y$ に対して, 共役複素数を $\overline{z} = x - \sqrt{-1}y$ とする．共役複素数を利用すると, 座標平面内の直線の方程式 $ax + by + c = 0$ は,

$$\overline{A}z + A\overline{z} + c = 0, \quad A = \frac{a + \sqrt{-1}b}{2}$$

となる．同様に, $B \in \mathbb{C}$ を中心とした半径 r の方程式は,

$$|\overline{z} - B|^2 = r^2 \Longleftrightarrow z\overline{z} - \overline{B}z - B\overline{z} + B\overline{B} = r^2$$

となる．従って, 円と直線の交点 z は, A, $\overline{A}$, B, $\overline{B}$, c, r^2 の 2 次方程式の根となり, 本質的に付け加えられる点は, 平方根で与えられる．このとき, $\overline{z}$ も同様に, もとの体の元の平方根を利用して与えられることもわかる．円と円の交点でも同様である．

まとめると, 作図可能な複素平面内の点は,

> 有理点 $x + \sqrt{-1}y$ (x, $y \in \mathbb{Q}$) から始めて, 平方根を付け加えることを繰り返して得られる体の中にある．

ということになり, 実数の作図可能性とほぼ同じ結果になる．

上のことを ζ_n に応用すると, $\mathbb{Q}(\zeta_n)$ が $\mathbb{Q}$ の 2 次の拡大体の積み上げに含まれるかという問題になる．$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ であり (正確な証明は, 系 H.1), $|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$ である．$\varphi(n)$ は n の素因数分解を $n = 2^k p_1^{k_1} \cdots p_r^{k_r}$ とすると,

$$\varphi(n) = n\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_r}\right) = 2^{k-1}p_1^{k_1-1}\cdots p_r^{k_r-1}(p_1 - 1)\cdots(p_r - 1)$$

である．$(\mathbb{Z}/n\mathbb{Z})^\times$ は可換群なので, これが 2 のべき乗になることが, 正 n 角形が作図できるための必要十分条件である．その条件は, $k_1 = k_2 = \cdots = k_r = 1$ で, p_i は $p_i = 2^{m_i} + 1$ の形の素数となる．

補題 4.15.1　$2^m + 1$ ($m \geqq 1$) が素数になるためには, $m = 2^l$ の形であることが必要である．

証明.　$m = 1$ の場合は明らか ($l = 0$ と取れる) なので, $m \geqq 2$ とする．m が奇数 $q(q > 1)$ で割り切れて, $m = qj$ であるとすると,

$$2^{qj} + 1 = (2^j)^q + 1 = (2^j + 1)((2^j)^{q-1} - (2^j)^{q-2} + \cdots + 1)$$

となり, $2^m + 1$ は素数でない．

これまでのことをまとめると次を得る．

定理 4.15.2　正 n 角形が作図可能であるための n の必要十分条件は, $2^{2^{m_i}}+1$ の形の素数 p_i を用いて, $n=2^k p_1\cdots p_r$ と書かれることである.

$F_n=2^{2^n}+1$ の形の素数を Fermat(フェルマー) 素数という. 知られている Fermat 素数は,

$$F_0=3,\quad F_1=5,\quad F_2=17,\quad F_3=257,\quad F_4=65537$$

の 5 つだけらしい. $F_5=4294967297=641\times 6700417$ という素因数分解は, Euler が発見した. Fermat 素数が無限にあるのか, 有限個しかないのかという問題は, 未解決である.

ちなみに, 現在の情報処理センターの maple を用いると, F_5 から F_8 までは素因数分解を与えることができ, 素数でないこともわかる. F_9 を素因数分解しようとすると, 数時間の実行ののちに, エラーとなる. ちなみに F_9 も素数ではない.

注意 4.15.1　複素数の作図問題の解を少し正確に述べると, 次のようになる.

$$z\in\mathbb{C}\text{ が作図可能}\iff\mathbb{Q}\text{ の Galois 拡大体 }L\text{ で, }[L:\mathbb{Q}]=2^n\text{ となるものが存在して, }z\in L$$

上で, Galois 拡大であるという条件は必要である. 単に 2 の冪乗の拡大体に含まれるだけでは, 作図可能であるとは言えない. 例えば, $x^4-x-1=0$ の根は $\mathbb{Q}$ の 4 次の拡大体を定めるが, これの分解体の Galois 群は, 例 4.14.1 にあるように S_4 であり, 根の表示には 3 次方程式の根 (3 乗根) が必要になり, 根の作図はできない.

A　有限生成 Abel 群の基本定理 (単因子論)

R を PID とし, M を有限生成な R–加群とする. 線形代数学や代数学序論などで学んだ行列の基本変形を利用して, M の構造を決定するのが, 単因子論である. $R=\mathbb{Z}$ とすると, これは有限生成 Abel 群の基本定理になり, $R=\mathbb{C}[X]$ とすれば, 複素行列の Jordan 標準系の理論に応用される.

単因子について述べる前に, 行列の基本変形について復習する. 考えるものは, 線形代数学で学んだものと同じであるが, 行列の要素は, 可換環 R の元であるとする.

R の元を成分とする行列の基本変形は, 次の 3 つの操作をいう.

(T1)　ある行もしくは列を単元倍する.
(T2)　2 つの行もしくは 2 つの列を入れ替える.
(T3)　ある行もしくはある列に別の行もしくは列のスカラー倍を加える.

(T1) が線形代数学とずれる部分で, 線形代数学では 0 でないスカラー倍としていたが, ここでは R が環なので, 逆変換の存在を保証するために単元倍に変わってる. 基本変型が可逆な変形であることは直ちにわかるが, これらの操作が, 可逆な行列の積で与えられることからもわかる. 実際, 次の n 次正方行列を導入する.

$$E_{ij}(\alpha,\beta,\gamma,\delta)=\begin{pmatrix} 1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & 1 & & & & & & \\ & & & \alpha & \cdots & \beta & & & \\ & & & & 1 & & & & \\ & & & \vdots & \ddots & \vdots & & & \\ & & & & & 1 & & & \\ & & & \gamma & \cdots & \delta & & & \\ & & & & & & 1 & & \\ & & & & & & & \ddots & \\ & & & & & & & & 1 \end{pmatrix},\quad \alpha,\beta,\gamma,\delta\in R\quad \alpha\delta-\beta\gamma\in R^{\times}$$

ここで, α は i,i–成分, β は i,j–成分, γ は j,i–成分, δ は j,j–成分にあり, 数字が書かれていない成分は, 全て 0 であるとしている. この行列を, 基本行列という. $\det E_{ij}(\alpha,\beta,\gamma,\delta)=\alpha\delta-\beta\gamma\in R^{\times}$ だから, この行列は逆行列を持つ. すなわち, $E_{ij}(\alpha,\beta,\gamma,\delta)\in GL_n(R)$ である. 基本変形は, 行列の積を用いて次で実現される.

(T1)　i 行の単元倍：$E_{ii}(\alpha,0,0,1)$ を左から掛ける.
　　i 列の単元倍：$E_{ii}(\alpha,0,0,1)$ を右から掛ける.
(T2)　i 行, j 行の入れ替え：$E_{ij}(0,1,1,0)$ を左から掛ける.
　　i 列, j 列の入れ替え：$E_{ij}(0,1,1,0)$ を右から掛ける.
(T3)　i 行に j 行の γ 倍を加える: $E_{ij}(1,\gamma,0,1)$ を左から掛ける $(i<j)$.
　　i 行に j 行の β 倍を加える: $E_{ij}(1,0,\beta,1)$ を左から掛ける $(i>j)$.
　　i 列に j 列の γ 倍を加える: $E_{ij}(1,\gamma,0,1)$ を右から掛ける $(i<j)$.
　　i 列に j 列の β 倍を加える: $E_{ij}(1,0,\beta,1)$ を右から掛ける $(i>j)$.

$A,B\in M_{m,n}(R)$ が基本変形で移りあえるとき, 互いに相似であるといい, $A\sim B$ と書くことにする. これは, 同値関係になる. 線形代数学で学んだ行列の基本変形の議論を, PID の元を成分とする行列に適用すると, 次の定理が得られる.

定理 A.1　R を PID とし, $A \in M_{m,n}(R)$ を R を成分にもつ $m \times n$ 行列とする. このとき, $d_1, \ldots, d_r \in R$ で, $d_i \mid d_{i+1},\ (i = 1, \ldots, r-1),\ d_r \neq 0$ となるものが単元倍を除いて一意的に存在し, M を基本変形することにより, 次の形の対角行列にできる.

$$\begin{pmatrix} d_1 & & & & & \\ & d_2 & & & & \\ & & \ddots & & & \\ & & & d_r & & \\ & & & & 0 & \\ & & & & & \ddots \end{pmatrix}$$

$(d_1, \ldots, d_r)$ を A の単因子という.

証明.　まず, 基本変形で上の形の対角行列にできることを示す. 次で与えられる R のイデアルの族 $\mathcal{I}$ を考える.

$$\mathcal{I} = \{Rb_{ij} \subset R \mid B = (b_{ij}),\ B \sim A\}$$

すなわち, A と相似な行列の成分から生成される単項イデアルを全て集めたものである. $\mathcal{I}$ に包含関係で順序を入れる. $\mathcal{I}$ の全順序部分集合

$$Rb_1 \subset Rb_2 \subset \cdots$$

を考える. 定理 3.6.2 の証明と同じことをすれば, このイデアルの増大列に対して, ある $l \in \mathbb{N}$ が存在して, $Rb_l = Rb_{l+1} = \cdots$ となる. この b_l を含む A と相似な行列を B とすれば, B の他の要素は b_l の倍数である. 実際, b_l の倍数でない要素 b_{ij} が存在すれば, これと b_l から生成される R のイデアル (b_l, b_{ij}) を考えると, $(b_l, b_{ij}) \supsetneqq Rb_l$ である. しかし, R は単項イデアル整域だから, ある b が存在して, $(b_l, b_{ij}) = Rb$ となる. このとき, $b = \alpha b_l + \beta b_{ij}$ となる $\alpha, \beta \in R$ が存在するが, 行列の基本変型の操作を考えると, $\alpha b_l + \beta b_{ij}$ を要素とする B と相似な行列を作ることができる. これは, b_l の取り方に矛盾する.

以上のことから, b_l を要素に持ち, 他の成分は b_l の倍数となる行列 B が, A と相似な行列として取れる. 行と列の置換をして, b_l を 1 行 1 列の成分にする. これを要 (pivot) として, 1 行, 1 列に対してはき出し (基本変型) をすれば, 各成分が b_{11} の倍数なので, A は次の形の行列に相似であることがわかる ($d_1 = b_{11} = b_l$ とする).

$$\begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & B' & \\ 0 & & & \end{pmatrix}$$

ここで, B' に対して上と同じ操作を繰り返す. その際, B' の作り方から, B' の要素は全て d_1 の倍数であることに注意する. 特に, 同じ操作で現れる対角成分の先頭要素は, d_1 の倍数である. この操作を繰り返すことにより, 定理の形の行列に基本変型で写ることが証明される.

A の部分行列で, i 次の正方行列であるものの行列式の値全体から生成される R のイデアルの生成元を e_i とする. 基本変型の定義と行列式の性質から, 基本変型を行っても行列式は単元倍しか変化しないので, e_i も基本変形によって単元倍しか変化しない. 従って, A が定理の形の対角行列に基本変型で写されたとすると,

$$d_1 = e_1, \quad d_1 d_2 = e_2, \quad d_1 d_2 d_3 = e_3, \ldots$$

を満たさなければならない. PID は UFD なので, このような d_1, d_2, ... は単元倍を除いて一意的に定まる.

注意 A.1　上の証明でわかるように, 1 番目から i 番目の単因子の積は, A の $i \times i$ 小行列の行列式全体の最大公約数である. R が Euclid 整域なら, この数は Euclid の互除法で具体的に計算するアルゴリズムがあるが, 一般の PID では, それがあるとは限らない. また, Euclid 整域なら, 対角行列にするための基本変形のアルゴリズムも, 互除法を用いて与えることができる.

単因子論を利用して, 有限生成 Abel 群の基本定理を証明するが, その前に次の補題を証明しておく.

補題 A.1　R を PID, M を有限生成 R–加群とすると, R の部分加群も有限生成である.

証明.　M の生成元の個数に関する帰納法を用いる. M が 1 つの生成元 u から生成されているとする. $N \subset M$ を N の部分 R–加群とする.

$$I = \{\, r \in R \mid ru \in N \}$$

とおくと, I は R のイデアルになる. 実際, $r_1, r_2 \in I$ なら $(r_1 + r_2)u = r_1u + r_2u \in N$ より, $r_1 + r_2 \in I$ であり, $a \in R$ に対して $(ar_1)u = a(r_1u) \in N$ より $ar_1 \in I$ となる. R は PID なので, $b \in R$ が存在して $I = (b)$ となる. このとき, N は bu で生成される. 実際, $bu \in N$ は定義より明らかで, N は部分加群だから, $Rbu \subset N$ である. 逆に, $n \in N$ とすると, M が u で生成されているから, $r \in R$ が存在して, $n = ru$ となる. このとき, I の定義から $r \in I$ となるが, I は b で生成されているので, $r = r'b$ となり, $n = r'bu$ となる. よって, 生成元が 1 つのときの補題が証明された.

$n-1$ 個の生成元を加群 M に対して, 補題が成立すると仮定する. M を n 個の生成元 $u_1, \ldots, u_n$ を持つ R–加群とし, $N \subset M$ をその部分加群とする. u_1 が生成する M の部分加群 Ru_1 による商加群を $M_1 = M/Ru_1$ とし, $f : M \to M_1 = M/Rx_1$ を自然な射影とする. M_1 は $n-1$ 個の元 $f(u_2), \ldots, f(u_n)$ から生成されるので, その部分加群 $f(N)$ は有限生成である. その生成元を $v_2, \ldots, v_m$ とし, その原像を $w_2, \ldots, w_m \in M$ とする. 準同型定理から, $f(N) \cong N/(N \cap Ru_1)$ である. ここで, $N \cap Ru_1$ は 1 つの元から生成される R–加群の部分加群なので, 上の議論から, これの生成元 w_1 が存在する. このとき, $w_1, w_2, \ldots, w_m$ は N の生成元である. 実際, $x \in N$ に対して, $f(x) = \sum_{i=2}^{m} a_i v_i$ とすると, $f\left(x - \sum_{i=2}^{m} a_i w_i\right) = 0$ だから, $x - \sum_{i=1}^{m} a_i w_i \in N \cap Ru_1$ となり, x は $w_1, w_2, \ldots, w_m$ の線形結合で表示される.

定理 A.2　R を PID, M を有限生成 R–加群とすると, 自然数 $l \in \mathbb{N}$ と $d_1, \ldots, d_r \in R$ で $d_i | d_{i+1}$, $(i = 1, \ldots, r-1)$ が存在して, R–加群として

$$M \cong R/d_1R \oplus \cdots \oplus R/d_rR \oplus R^l$$

となる. $R = \mathbb{Z}$ とすると, これは有限生成 Abel 群の基本定理である.

証明.　M の生成元を $\{u_1, \ldots, u_n\}$ とする. $N = R^n$ とし, N の標準基底を $e_1, \ldots, e_n$ とする. R–加群の準同型写像, $\varphi : N \to M$ を次で定義する.

$$\varphi\left(\sum_{i=1}^{n} r_i e_i\right) = \sum_{i=1}^{n} r_i u_i, \quad r_i \in R$$

$\{u_1, \ldots, u_n\}$ が M を生成するから, φ は全射である. 従って, 準同型定理より, $M \cong N/\mathrm{Ker}(\varphi)$ である. N は有限生成 R–加群なので, 上の補題から, $\mathrm{Ker}(\varphi)$ は有限生成である. その生成元を $\{v_1, \ldots, v_m\}$ とする. v_i を

標準基底の線形結合で書く.

$$v_i = a_{i1}e_1 + \cdots + a_{in}e_n, \quad i = 1, 2, \ldots, m$$

これによって得られる行列

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$$

を $\mathrm{Ker}(\varphi)$ の生成行列と呼ぶことにする.

$\mathrm{Ker}(\varphi)$ の生成元 $\{v_1, \ldots, v_n\}$ を次のように取り替えることができる.

(L1) v_i をその単元倍に変える.

(L2) v_i と v_j を入れ替える.

(L3) $c \in R$ と $j \neq i$ に対して, v_i を $v_i + cv_j$ に変える.

上の操作を行っても, 生成元になる. 実際, (L1), (L2) は明らかだし, (L3) についても, $v_i = (v_i + cv_j) - cv_j$ に注意すれば良い. これらの操作は, 生成行列に対しての行基本変形 (基本行列を左からかける操作) に対応するのは, 明らかである. すなわち, 行基本変形を施した行列に対応する生成元は, 元の部分加群と同じ部分加群を生成する.

次に, R–加群の同型写像 $g : N \to N$ を考える. $N/\mathrm{Ker}(\varphi) \cong N/g(\mathrm{Ker}(\varphi))$ である. 一方, g は同型写像なので, $\{g(e_1), \ldots, g(e_n)\}$ も R^l の基底になる. 逆に, R^l の基底 $\{f_1, \ldots, f_n\}$ を与えると, $e_i \mapsto f_i$, $(i = 1, \ldots, n)$ で R^l の R–同型写像が定まる. すなわち, R^l の R–同型写像は, 基底の取り換えに他ならない. そこで, 次の基底の取り換えを考える.

(R1) i 番目の基底をその単元倍に変える.

(R2) i 番目の基底と j 番目の基底を入れ替える.

(R3) $c \in R$ と $j \neq i$ に対して, i 番目の基底に j 番目の基底の c 倍を加える.

これらの操作で, 基底が基底に移されることは, (L1)–(L3) の場合と同様にわかる. また, これらの操作を行うと, $\mathrm{Ker}(\varphi)$ の生成行列は, 対応する列基本変形が施されることも容易にわかる. よって, 定理 A.1 より, $N = R^l$ の基底をうまく選ぶと, $\mathrm{Ker}(\varphi)$ の生成行列が

$$\begin{pmatrix} d_1 & & & & & & \\ & d_2 & & & & & \\ & & \ddots & & & & \\ & & & d_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \end{pmatrix}, \qquad d_i \mid d_{i+1},\ i = 1, 2 \ldots$$

とできる. このとき $M \cong R/d_1R \oplus \cdots \oplus R/d_rR \oplus R^l, \quad (l = n - r)$ となるのは, 明らかである.

B $\mathbb{Z}\left[\dfrac{1+\sqrt{-19}}{2}\right]$ (注意 3.5.1)

$\alpha = \dfrac{1+\sqrt{-19}}{2}$ とする. ここでは, $R = \mathbb{Z}[\alpha] = \{a + b\alpha \mid a, b \in \mathbb{Z}\}$ と固定する. R は, PID であるが, Euclid 整域ではないことの初等的な証明を与える. PID であることは, ここに述べた証明よりも, 2 次体の整

数論において類数公式を証明しておき, R の類数を計算して, それが 1 となることを利用するのが標準的な手法のようである. ここでは, 類数公式を用いない証明を与える.

$\overline{\alpha} = \dfrac{1-\sqrt{-19}}{2}$ (α の複素共役) とし, $x = a + b\alpha$, $a, b \in \mathbb{Z}$ に対して, $\overline{x} = a + b\overline{\alpha}$ (x の複素共役) とする. α, $\overline{\alpha}$ は, 方程式 $X^2 - X + 5 = 0$ の 2 根になることに注意する. $\alpha\overline{\alpha} = 5$ なので, $\dfrac{1}{\alpha} = \dfrac{1-\sqrt{-19}}{10}$ であり, 特に R の商体は $\mathbb{Q}(\sqrt{-19})$ となる.

$x \in R$ に対して, $N(x) = x\overline{x}$ とする. $N(x)$ を x のノルムという. これは, x を複素数と見たときの大きさの 2 乗である. $x = a + b\alpha \in R$ $(a, b \in \mathbb{Z})$ とすると, $N(x) = a^2 + ab + 5b^2$ である.

補題 B.1　1. 任意の $x \in R$ に対して, $N(x) \in \mathbb{N} \sqcup \{0\}$ である.

2. $x, y \in R$ に対して, $N(xy) = N(x)N(y)$
3. $x \in R$ に対して,
   (a) $N(x) = 0 \Longleftrightarrow x = 0$.
   (b) $N(x) = 1 \Longleftrightarrow x = \pm 1$. これと 2. より, $R^\times = \{\pm 1\}$.
4. $x \in R$, $(x \neq 0)$ に対して, x から生成される単項イデアルを $(x) = xR$ とするとき, $|R/xR| = N(x)$.

証明. 1, 2, 3 は, 容易に示すことができるので, 演習問題とする.

4. は上の節の単因子論 (A) の応用である. R を 1, α から生成される自由 $\mathbb{Z}$–加群 $R = \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot\alpha$ とみる. $x = a + b\alpha \in R$ $(a, b \in \mathbb{Z})$ とし, x を掛けるという $\mathbb{Z}$–加群の準同型写像を, この基底に対して行列表示する. $\alpha^2 - \alpha + 5 = 0$ を利用すると,

$$\begin{aligned} x\cdot 1 &= a\cdot 1 + b\cdot\alpha, \\ x\cdot\alpha &= a\alpha + b\alpha^2 = -5b\cdot 1 + (a+b)\cdot\alpha \end{aligned}$$

より, 求める行列表示は, $\begin{pmatrix} a & -5b \\ b & a+b \end{pmatrix}$ である. 特に, この行列の行列式は, $N(x)$ に一致する. $\mathbb{Z}$ は PID なので, 単因子論を利用して, R の $\mathbb{Z}$–基底を取り替えることにより[*8], x の行列表示は $\begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}$ $(d_i \in \mathbb{N})$ の形にできる. さらにこの際, 行列式の値は符号 ($\mathbb{Z}$ の単元倍) だけが変化するので, $d_1 d_2 = N(x)$ である. この基底を利用すると, 加法群として $R/xR \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z}$ である. よって, $|R/xR| = d_1 d_2 = N(x)$ が成立する.

問 B.1　上の補題の 1, 2, 3 を証明せよ.

定理 B.1　R は Euclid 整域ではない.

証明.　R が Euclid 整域であるとし, $\varphi : R \to N$ を定義 3.5.1 にある, R から整列集合 N への写像とする. $S = R \setminus \{0, \pm 1\}$ とする. N は整列集合なので, $\varphi(S)$ には最小元が存在する. $x \in S$ を $\varphi(x)$ が $\varphi(S)$ の最小元になる元とする. このとき, $|R/xR| \leqq 3$ である. 実際, $a \in R$ とすると, $a = xq + r$, $\varphi(r) < \varphi(x)$ となる $q, r \in R$ が存在するが, x の取り方から, $r = 0, \pm 1$ となり, R の任意の元は xR を法として, $0, \pm 1$ と一致する. すなわち $|R/xR| \leqq 3$ である. 一方, $x \neq 0, \pm 1$ なら, $N(x) \geqq 4$ が成立する (下の問 B.2) ので, 補題 B.1, 4. より $|R/xR| \geqq 4$ となり矛盾する.

問 B.2　$x \in R$, $x \neq 0, \pm 1$ なら, $N(x) \geqq 4$ を示せ.

[*8] x を掛ける前に使う基底と掛けた後に使う基底は同じものではない

R が PID であることを示すには, 次の補題をまず用意する.

補題 B.2　A を可換環, N を整列集合とする. 写像 $\psi : A \to N$ で次の性質 (P) を持つものが存在すれば, A は PID である[*9].

$$\text{(P)} \begin{cases} 1. \quad x \in R, x \neq 0 \text{ に対して, } \psi(0) < \psi(x). \\ 2. \quad x, y \in A,\ x \neq 0,\ \psi(y) \geqq \psi(x) \implies x \mid y \text{ または } \exists z, w \in A, \text{ s.t. } \psi(0) < \psi(xw + yz) < \psi(x). \end{cases}$$

証明. Euclid 整域が PID になることの証明と同じである. $I \in A$ を A のイデアルとする. $x \in I$ を $\psi(x)$ が $\psi(I \setminus \{0\})$ の最小元を与えるものとする. このとき, $I = (x)$ が成立する. 実際, $y \in I$, $y \neq 0$ とする. x の取り方から, $\psi(y) \geqq \psi(x)$ である. $x \nmid y$ とすると, 仮定より $z, w \in A$ が存在して, $\psi(0) < \psi(xz + yw) < \psi(x)$ となる. $x, y \in I$ なので, $xz + yw \in I$ となるが, これは x の取り方に矛盾する. よって, $x \mid y$ となり, $y \in (x)$ となって, $I = (x)$ である.

上の性質 (P) の ψ が存在する場合, 2. において常に $z = 1$ と取ることができれば, ψ は定義 3.5.1 の φ と同じ性質を持ち, R は Euclid 整域になる.

命題 B.1　$R = Z\left[\dfrac{1+\sqrt{-19}}{2}\right]$ において, ノルム写像 $N : R \to \mathbb{Z}_{\geqq 0} = \{k \in \mathbb{Z} \mid k \geqq 0\}$ は, 補題 B.2 の性質 (P) を持つ. 特に R は PID である.

証明.　$x \in R$, $x \neq 0$ なら $N(x) > N(0) = 0$ が成立するので, N は (P) 1. の性質を満たす.

以下では, R 及びその全商体 $\mathbb{Q}(\sqrt{-19})$ を複素数体 $\mathbb{C}$ の部分環及び部分体とみなして議論をする. そのとき $N(x)$ の値は, 複素数としての大きさの 2 乗であることを利用する. 下の図を補助的に利用する. 図は, 複素平面内で R の点 0, 1, α, $1+\alpha$ を頂点とする平行 4 辺形と 0, 1, α, $1+\alpha$ を中心とする半径 1 の 4 つの円, $\dfrac{\alpha}{2}$, $\dfrac{1}{2}+\dfrac{\alpha}{2}$, $1+\dfrac{\alpha}{2}$ を中心とする半径 $\dfrac{1}{2}$ の 3 つの円が書かれている.

$x, y \in R$ として, $x \neq 0$, $N(y) \geqq N(x)$ かつ $x \nmid y$ とする. $\dfrac{y}{x} \in \mathbb{Q}(\sqrt{-19})$ を考えると, R の定義から, $a \in R$ が存在して,

$$\frac{y}{x} = a + r + s\alpha, \quad s, r \in \mathbb{Q},\ 0 \leqq r < 1,\ 0 \leqq s < 1,\ r + s\alpha \neq 0 \tag{B.1}$$

とできる. すなわち, $r + s\alpha$ を図の平行 4 辺形の中 (一部境界を含む) にとる.

このとき, $r + s\alpha$ に最も近い R の点を b (b は $0, 1, \alpha, 1+\alpha$ のどれか) として, $r' = r + s\alpha - b$ とおくと,

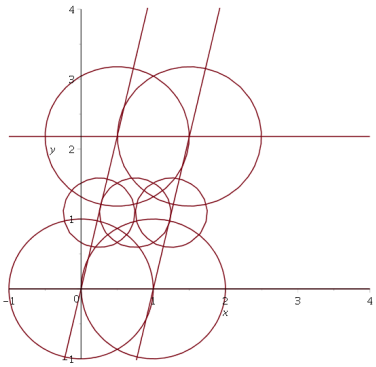
$$\frac{y}{x} = a + b + r', \quad a + b \in R,\ r' \in \mathbb{Q}(\sqrt{-19}),\ r' \neq 0$$

となる. $N(r') < 1$ なら (図において, 半径 1 の 4 つのどれかの円の内部に r が含まれるとき), $w = -(a+b)$, $z = 1$ とおくと,

$$0 < N(r'x) = N(r')N(x) < N(x), \quad r'x = -(a+b)x + y = xw + yz$$

となり, 補題 B.2 の (P) 2. が満たされる.

[*9] 左辺の不等号は本質的である. $w = y$, $z = -x$ とすると, $\psi(xy + y(-x)) = \psi(0)$ となることに注意せよ.



$N(r') \geqq 1$ とする．このとき, 図の小さい 3 つの円を見ると, $r+s\alpha$ と 3 点 $\dfrac{\alpha}{2}$, $\dfrac{1}{2}+\dfrac{\alpha}{2}$, $1+\dfrac{\alpha}{2}$ のどれかとの距離は $\dfrac{1}{2}$ より小さいことがわかる．全体を 2 倍すると, $2(r+s\alpha)$ と α, $1+\alpha$, $2+\alpha$ のどれかとの距離は 1 より小さい．上と同様に考えると, $a' \in R$ が存在して, $N\left(\dfrac{2y}{x}-a'\right) < 1$ である．

ここで, $\dfrac{2y}{x}-a' \neq 0$ なら, $w=-a'$, $z=2$ とすれば, 補題 B.2 の (P) 2. の性質を満たすことは, 上と同様である．

$\dfrac{2y}{x}-a'=0$ とする．このとき, (B.1) で定まる $r+s\alpha$ は, $r+s\alpha \in \dfrac{1}{2}R = \left\{\dfrac{q}{2} \mid q \in R\right\}$ とその取り方から, $\dfrac{\alpha}{2}$ であるか $\dfrac{1+\alpha}{2}$ のいずれかである．これらについて, 場合分けをして考える．

- $\dfrac{y}{x} = a+\dfrac{\alpha}{2}$, $a \in R$ のとき．$\alpha(1-\alpha)=5$ に注意する．$-ax+y=\dfrac{\alpha}{2}x$ の両辺に $1-\alpha$ を掛けると,

  $$-(1-\alpha)ax+(1-\alpha)y = \frac{\alpha(1-\alpha)}{2}x = \frac{5}{2}x$$

  $2x$ を左辺に移して,

  $$-\left\{2+(1-\alpha)a\right\}x+(1-\alpha)y = \frac{1}{2}x \neq 0.$$

  よって, 補題 B.2 (P) 2. において, $w=-2-(1-\alpha)a$, $z=1-\alpha$ を取ることができる．
- $\dfrac{y}{x} = a+\dfrac{1+\alpha}{2}$, $a \in R$ のとき．$\alpha(\alpha+1)=2\alpha-5$ を用いる．$-ax+y=\dfrac{1+\alpha}{2}$ の両辺に α を掛けて,

  $$-a\alpha x+\alpha y = \frac{2\alpha-5}{2}x = \alpha x-\frac{5}{2}x.$$

  左辺に, $(\alpha-2)x$ を移行して,

  $$-(a\alpha+\alpha-2)x+\alpha y = -\frac{1}{2}x \neq 0.$$

  となり, 上と同じように, 補題 B.2 (P) 2. の成立が示される．

問 B.3　領域 $\left\{a+b\dfrac{1+\sqrt{-19}}{2} \mid 0 \leqq a \leqq 1,\ 0 \leqq b \leqq 1\right\}$ が上の図の 7 つの円で被覆されることを示せ．

問 B.4　$\mathbb{Z}\left[\dfrac{1+\sqrt{-15}}{2}\right]$ では, 上のような証明が成立しない．実際, この環は PID ではない．どこがうまくいかなくなるかを確かめよ．

C　代数的閉包の存在

ここでは, 以下の定理 (定理 4.4.1 と同じもの) の証明を与える. 「体 K の全ての代数拡大の集まり $\mathcal{K}$ を考えて, それに包含関係で順序を入れ, Zorn の補題を利用する.」という証明も大丈夫なのだが, $\mathcal{K}$ が集合論的に大きすぎない (例えば, Russel(ラッセル) の逆理のようなものを導かない) ことを保証するのが, 面倒である. 以下の証明は, それを避ける工夫がなされている.

定理 C.1（Steiniz）　1. K を体とするとき, K の代数的閉包 $\overline{K}$ が K 同型を除いて一意的に存在する.

2. L/K を代数的拡大体とし, Ω を代数的閉体であるとする. このとき, 体の埋め込み $\sigma : K \to \Omega$ は, 埋め込み $\widetilde{\sigma} : L \to \Omega,\ \widetilde{\sigma}_{|K} = \sigma$ に拡張することができる.

証明 (Artin).　1. $K[X]^*$ を K の 1 次以上の多項式の集合とする. $f \in K[X]^*$ に対して, 不定元 X_f を対応させ, K 上の無限変数の多項式環, $A = K[X_f \mid f \in K[X]^*]$ を考える. すなわち, A の元は,

$$\sum a_{f_1 \dots f_n} X_{f_1} \cdots X_{f_n}, \quad a_{f_1 \dots f_n} \in K$$

の形の有限和の集まりである ($f_k = f_l$ となることがあっても良い).

A の中で, $\{f(X_f) \mid f \in K[X]^*\}$ から生成されるイデアル I を考える. $I \neq A$ である. 実際, $I = A$ とすると, $1 \in I$ となる. このとき, $f_1, \dots, f_m \in K[X]^*$ と $g_1, \dots, g_m \in A$ が存在して,

$$g_1 f_1(X_{f_1}) + \cdots + g_m f_m(X_{f_m}) = 1 \tag{C.1}$$

となる. $f_i(X) = 0$ の根の 1 つを θ_i を取って, K に $\theta_1, \dots, \theta_m$ を付け加えた体, $K(\theta_1, \dots, \theta_n)$ を考えることができる. (C.1) の左辺を $K(\theta_1, \dots, \theta_m)$ 係数の多項式の関係式と見たとき, $X_{f_1} = \theta_1, \dots, X_{f_m} = \theta_m$ を代入すると, $0 = 1$ となって矛盾する.

A の I を含む極大イデアル $\mathfrak{m}$ が存在する. $K_1 = A/\mathfrak{m}$ とすると, K_1 は体であり, 作り方から, 任意の $f \in K[X]^*$ に対して, $f(X) = 0$ の根の 1 つを含む. この構成方法を繰り返して, 次の拡大体の列を作ることができる.

$$K \subset K_1 \subset K_2 \subset \cdots$$

$\overline{K} = \bigcup_{i=1}^{\infty} K_i$ は, K の代数的閉包になる. 実際, 構成方法から, $\overline{K}$ は K 上代数的である. さらに, $f(X) \in \overline{K}[X]$ とすると, ある n に対して, $f(X) \in K_n[X]$ となり, $f(X) = 0$ の根は $K_{n+1} \subset \overline{K}$ に含まれる.

一意性の証明は, 2. を用いてなされるので, 2. の証明の後に述べる.

2. L/K を代数拡大とする. $\mathcal{M}$ を次で与えられる L の部分体と埋め込み写像の対の集合とする.

$$\mathcal{M} = \{(M, \tau) \mid K \subset M \subset L,\ \tau : M \to \Omega,\ \tau_{|K} = \sigma\}$$

$\mathcal{M}$ に次で順序関係を入れる.

$$(M_1, \tau_1) \preceq (M_2, \tau_2) \Longleftrightarrow M_1 \subseteq M_2,\ \tau_{2|M_1} = \tau_1$$

$\mathcal{M}$ は, この順序で帰納的順序集合となる. 実際, $\mathcal{L} = \{(M_i, \tau_i)\} \subset \mathcal{M}$ を全順序部分集合とすると, $M = \bigcup_i M_i$ は, その上界を与える ($\tau : M \to \Omega$ は, $x \in M$ に対して, $x \in M_i$ となる i を取って, $\tau(x) = \tau_i(x)$ と定めることができる.). Zorn の補題により, $\mathcal{M}$ には極大元 (L', τ') が存在する. よって, $L' = L$ を証明すれば良い.

$L' \subsetneqq L$ とする．$\alpha \in L \setminus L'$ をとり，代数拡大 $L'(\alpha)/L'$ をとる．このとき，$\tau' : L' \to \Omega$ は $L'(\alpha)$ に拡張できる．実際，α の L' 上の最小多項式を $f_\alpha \in L'[X]$ とする．$\tau'(f_\alpha) \in \Omega[X]$ に対して，Ω は代数閉体だから，$\beta \in \Omega$ が存在して，$\tau'(f_\alpha)(\beta) = 0$ となる．このとき，

$$\widetilde{\tau'} : L'(\alpha) \cong L'[X]/(f_\alpha(X)) \longrightarrow \Omega, \qquad \widetilde{\tau'}(\overline{g(X)}) = \tau'(g)(\beta), \quad g(X) \in L'[X]$$

は τ' の $L'(\alpha)$ への拡張となる．これは L' の極大性に矛盾する．

[代数的閉包の一意性の証明] L_1, L_2 を K の代数的閉包とする．L_1/K は代数拡大だから，2. より体の埋め込み $K \to L_2$ は，埋め込み $\tau : L_1 \to L_2$ に拡張される．$K \subset \tau(L_1) \subset L_2$ において，$\tau(L_1)$ は K 上の代数拡大体である．また，L_1 が代数的閉体なので，$\tau(L_1)$ も代数的閉体で，$\tau(L_1)$ の真の代数拡大体は存在しない．よって，$\tau(L_1) = L_2$ が成立し，τ は全射である．

D　代数学の基本定理

ここでは，Galois 理論を利用して代数学の基本定理を示す．もちろん，実数の連続性は必要であり，これは，

> $f(X) \in \mathbb{R}[X]$ を奇数次の多項式とすると，$f(X) = 0$ は実根を持つ．特に，$\mathbb{R}$ の真の奇数次の拡大体は存在しない．

という形で利用する．

定理 D.1（Gauss, 1799）　複素数体は代数的閉体である．

証明. $f(X) \in \mathbb{C}[X]$ とするとき，$f(\theta) = 0$ となる $\theta \in \mathbb{C}$ が存在することを示せばよい．$\overline{f}(X)$ を f の係数をすべて複素共役としたものとすると，容易にわかるように，$F(X) = f(X)\overline{f}(X) \in \mathbb{R}[X]$ である．$F(X) = 0$ の根を θ とすると，θ もしくは $\overline{\theta}$ は $f(X) = 0$ の根であるから，$F(X) \in \mathbb{R}[X]$ が必ず複素数の根を持つことを示せばよい．

$F(X) \in \mathbb{R}[X]$ とする．$F(X)$ は $\mathbb{R}$ 上既約であると仮定してよい．上で述べたように，ことのき，F の次数は偶数であり，$\deg F = 2^k m$, $(m, 2) = 1$ とする．L を F の分解体とする．θ を F の根の 1 つとし，$M = \mathbb{R}(\theta)$ とすると，F の既約性より $[M : \mathbb{R}] = \deg F = 2^k m$ であり，$[L : \mathbb{R}] = [L : M][M : \mathbb{R}]$ だから，$[L : \mathbb{R}] = 2^l m'$, $l \in \mathbb{N}$, $(m', 2) =1$ となる．$|\mathrm{Gal}(L/\mathbb{R})| = [L : \mathbb{R}] = 2^l m'$ なので，$\mathrm{Gal}(L/\mathbb{R})$ の Sylow 2–部分群 P を考える．Galois の基本定理から，P に対する固定体 M' を考えると，$|P| = 2^l$ なので，$[M' : \mathbb{R}] = m'$ となり，M' は $\mathbb{R}$ の奇数次の代数拡大体になる．上の中間値の定理は，$\mathbb{R}$ の奇数次の真の代数拡大体は存在しないことを主張しているから，$m' = 1$ で，$M' = \mathbb{R}$ であり，$|\mathrm{Gal}(L/\mathbb{R})| = 2^l$ を得る．

H を $\mathrm{Gal}(L/\mathbb{R})$ の真の極大部分群とする．すなわち，$G \supsetneqq H \supset \{e\}$ で，H を含む G の部分群は G に限るとする．このとき，群論の簡単な議論から，$|H| = 2^{l-1}$ で $G \rhd H$, $G/H \cong \mathbb{Z}/2\mathbb{Z}$ が示される．再び Galois の基本定理を用いて，H で固定される部分体を M' とする．このとき，体の拡大 $M/\mathbb{R}$ は Galois 拡大で，$\mathrm{Gal}(M/\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$ で，$[M : \mathbb{R}]$=2 である．よって，$M = \mathbb{R}(\sqrt{a})$, $(a \in \mathbb{R},\, a < 0)$ となる．このとき，$M = \mathbb{R}(\sqrt{-1}\sqrt{-a})$ だが，$\sqrt{-a} \in \mathbb{R}$ なので，$M = \mathbb{C}$ となる．

$H \neq \{e\}$ とすると，H に対して真の極大部分群 H' をとると上と同様のことが実行できるので，$M = \mathbb{C}$ に対する 2 次拡大体 M' が L の H' に対する固定体として構成される．しかし，$\mathbb{C}$ では常に平方根をとることができるので，このような 2 次拡大体は存在しない．従って，$H = \{e\}$ で，$L = \mathbb{C}$, $\mathrm{Gal}(L/\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$ が成立し，F は $\mathbb{C}$ に必ず根を持つ．

E　対称多項式

ここでは, 対称式が基本対称式の多項式になること (定理 1.1.2) を, Galois 理論を用いて証明する. 例 4.7.3 の内容を少し精密に考えることにより, 証明はなされる. この定理には, 何通りかの別証明も可能である.

k を体とし, $k[X_1,\ldots,X_n]$ を n 変数多項式環とする. 対称群 S_n は, 変数の置換によって, $k[X_1,\ldots,X_n]$ に作用する. この作用の固定点を, ここでは対称多項式と呼ぶ (通常は対称式と呼ぶが, 例 4.7.3 で, 置換群の作用で不変な有理式を対称式と呼んだので, それと区別するためにそう呼ぶことにする). すなわち, n 変数の多項式 $f(X_1,\ldots,X_n)$ が対称多項式であるとは, 任意の $\sigma\in S_n$ に対して, $f(X_{\sigma(1)},\ldots,X_{\sigma(n)})=f(X_1,\ldots,X_n)$ が成立することである.

$$R=k[X_1,\ldots,X_n]^{S_n}=\{f\in k[X_1,\ldots,X_n]\mid \sigma(f)=f,\ \forall\sigma\in S_n\}$$

を n 変数の対称多項式全体のなす集合とする. これが $k[X_1,\ldots,X_n]$ の部分環になることは, 明らかである. $k[X_1,\ldots,X_n]$ が整域なので, R も整域になる.

根と係数の関係に現れる根の多項式は, 対称式になっている (根の置換で不変). これらを基本対称式 (elementary symmetric polynomial) という. 具体的には, 次で定義される (ここでは, 記号 e_k を用いる. $e_0=1$ とする.).

$$e_k(X_1,\ldots,X_n)=\sum_{1\leqq i_1<\cdots<i_k\leqq n} X_{i_1}\cdots X_{i_k}$$

定理 E.1　$f\in R=k[X_1,\ldots,X_n]^{S_n}$ なら f は, $e_1,\ldots,e_n$ の多項式として表示される. すなわち, ある $g(Y_1,\ldots,Y_n)\in k[Y_1,\ldots,Y_n]$ が存在して, $f(X_1,\ldots,X_n)=g(e_1(X_1,\ldots,X_n),\ldots,e_k(X_1,\ldots,X_n))$ である.

証明.　例 4.7.3 で述べた R の全商体 $L=k(X_1,\ldots,X_n)$ とその部分体 $K=k(e_1,\ldots,e_n)$ を考える. L/K は Galois 拡大であり, $\mathrm{Gal}(L/K)\cong S_n$ である. L は K 上の方程式,

$$F(T)=(T-X_1)(T-X_2)\cdots(T-X_n)$$

の分解体である. 次の中間体の列を考える.

$$\begin{array}{ccccccccc}
K & \subset & K(X_n) & \subset & K(X_n,X_{n-1}) & \subset\cdots\subset & K(X_n,\ldots,X_2) & \subset & K(X_n,\ldots,X_1)\\
\| & & \| & & \| & & \| & & \|\\
K_0 & \subset & K_1=K_0(X_n) & \subset & K_2=K_1(X_{n-1}) & \subset\cdots\subset & K_{n-1}=K_{n-2}(X_2) & \subset & K_{n-1}(X_1)=L
\end{array}$$

このとき, 体の拡大 K_{i+1}/K_i, $(i=0,\ldots,n-1)$ において, K_{i+1} の K_i–ベクトル空間の基底として,

$$X_{n-i}^j,\quad j=0,1,\ldots,n-i-1$$

が取れる. 実際, $K_{i+1}=K_i(X_{n-i})$ であるが, X_{n-i} は多項式

$$F_i(T)=(T-X_1)(T-X_2)\cdots(T-X_{n-i})=0$$

の根である. ここで,

$$F_i(T)=\frac{F(T)}{(T-X_{n-i+1})\cdots(T-X_n)}$$

であるが, 右辺は, $K_i[T]$ の元としての商と考えると, 左辺に対して $F_i(T) \in K_i[T]$ が従う. 特に, $\deg F_i = n-i$ なので, $[K_{i+1} : K_i] \leqq n - i$ である. 一方,

$$n! = [L : K] = [L : K_{n-1}][K_{n-1} : K_{n-2}] \cdots [K_1 : K] \leqq n!$$

となるので, すべての i について, $[K_{i+1} : K_i] = n - i$ を得る. よって, $1, X_{n-i}, \ldots, X_{n-i}^{n-i-1}$ は K_{i+1} の K_i 上の基底になる. このとき, L の K 上のベクトル空間としての基底は,

$$X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}, \quad 0 \leqq i_k \leqq k-1$$

で与えられることに注意する (命題 4.1.1 の証明を参照).

次に, $L = k(X_1, \ldots, X_n)$ の部分環 $k[X_1, \ldots, X_n]$ の元 $f(X_1, \ldots, X_n)$ を上で与えた K 上の基底の線形結合で表すとき, その係数は, $e_1, \ldots, e_n$ の多項式となる. 実際,

$$X_1 = e_1 - (X_2 + \cdots + X_n)$$

を f に代入して, f は, $X_2, \ldots, X_n, e_1$ の多項式となる. 上で与えた体の拡大, $K_{n-1}/K_{n-2} = K_{n-2}(X_2)/K_{n-2}$ において, X_2 は次の方程式を満たす (上で述べた $F_2(T) = 0$ の根, 下の注意 E.1 も参照).

$$X_2^2 - \{e_1 - (X_3 + \cdots + X_n)\} X_2 + \{e_2 - (X_3 + \cdots + X_n)e_1 + \sum_{3 \leqq i \leqq j} X_i X_j\} = 0 \tag{E.1}$$

よって,

$$X_2^2 = \{e_1 - (X_3 + \cdots + X_n)\} X_2 - \{e_2 - (X_3 + \cdots + X_n)e_1 + \sum_{3 \leqq i \leqq j} X_i X_j\}$$

が成立するので, これを f に代入することにより,

$$f(X_1, \ldots, X_n) = g_1(X_3, \ldots, X_n, e_1, e_2)X_2 + g_0(X_3, \ldots, X_n, e_1, e_2), \quad g_1, g_0 \in k[X_3, \ldots, X_n, e_1, e_2]$$

を得る. 以下このような操作を繰り返すことにより, $f \in k[X_1, \ldots, X_n]$ は,

$$f(X_1, \ldots, X_n) = \sum_{0 \leqq i_k \leqq k-1} g_{i_1, \ldots, i_n}(e_1, \ldots, e_n) X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}, \tag{E.2}$$
$$g_{i_1, \ldots, i_n}(e_1, \ldots, e_n) \in k[e_1, \ldots, e_n]$$

となる. 上で, $X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}$ は基底なので, このような表示は一意的であることに注意する. 特に, $i_1 > 0$ なら, $g_{i_1, \ldots, i_n} = 0$ に注意する.

さて, $f \in k[X_1, \ldots, X_n]^{S_n}$ とする. 表示 (E.2) に互換 $(1, j)$, $j = 2, \ldots, n$ を作用させる. 上の注意と表示の一意性から,

$$\text{ある } j \text{ に対して } i_j > 0 \Longrightarrow g_{i_1, \ldots, i_n} = 0$$

が従う. よって, $f = g_{0, \ldots, 0}(e_1, \ldots, e_n)$ となり, f は基本対称式の多項式である.

注意 E.1 上の証明において, X_{n-i} が満たす K_i 上の方程式 $F_i(T) = 0$ の形の $K_i[T]$ の元としての具体的な表示も, 完全対称関数 (complete symmetric function) を用いればできる. 次の形の対称式を, m 次の (l 変数) 完全対称関数という. ($h_0 = 1$ とする.)

$$h_m(X_1, \ldots X_l) = \sum_{i_1 + \cdots + i_l = m} X_1^{i_1} \cdots X_l^{i_l}$$

このとき, $F_i(T)$ は次の式で表される ((E.1) から類推はできる). 証明は, h_n と e_n の母関数 (generating function) を利用すれば容易であるが, ここでは省略する.

$$\begin{aligned} F_i(T) &= T^i - \{e_1 - h_1(X_{i+1}, \ldots, X_n)\} T^{i-1} + \{e_2 - h_1(X_{i+1}, \ldots, X_n)e_1 + h_2(X_{i+1}, \ldots, X_n)\} T^{i-2} \\ &\qquad + \cdots + (-1)^i h_i(X_{i+1}, \ldots, X_n) \\ &= \sum_{j=0}^{i} \left((-1)^j \sum_{k=0}^{j} (-1)^k e_{j-k} h_k(X_{i+1}, \ldots, X_n) \right) T^{i-j} \end{aligned}$$

定理 E.1 で, 対称多項式が基本対称式 $e_1, \ldots, e_n$ の多項式になることが示されたが, 基本対称式は,「代数的に独立である」ことが証明できる.

一般に, 可換体上の多項式環 $k[X_1, \ldots, X_n]$ の元 $f_1, \ldots, f_m$ が代数的に従属しているとは, これらに代数的な関係式が存在していること, すなわち, ある 0 でない k–係数の多項式 $g(Y_1, \ldots, Y_m)$ が存在して, $g(f_1, \ldots, f_m) = 0$ となることを言う. 代数的に従属していないとき, 代数的に独立であるという.

$f_1, \ldots, f_m$ が代数的に従属と仮定する. $g(f_1, \ldots, f_m) = 0$ である次数が最小の $g(Y_1, \ldots, Y_m)(\neq 0)$ に対して, 両辺の X_i での形式的な微分を計算すると,

$$\sum_j \frac{\partial g}{\partial Y_j}(f_1, \ldots, f_m) \frac{\partial f_j}{\partial X_i} = 0, \quad i = 1, \ldots, n$$

を得る. g の取り方から, $\left(\dfrac{\partial g}{\partial Y_1}, \ldots, \dfrac{\partial g}{\partial Y_m} \right) \neq \mathbf{o}$ なので, $f_1, \ldots, f_m$ が代数的に従属していれば, Jacobi(ヤコビ) 行列 $\left(\dfrac{\partial f_i}{\partial X_j} \right)$ に対して,

$$\operatorname{rank} \left(\frac{\partial f_i}{\partial X_j} \right)_{\substack{i=1,\ldots,m \\ j=1,\ldots,n}} < m$$

が成立する. 対偶を取ると, $\operatorname{rank} \left(\dfrac{\partial f_i}{\partial X_j} \right) = m$ なら, $f_1, \ldots, f_m$ は代数的に独立である.

定理 E.2

$$\det \left(\frac{\partial e_i}{\partial X_j} \right) = \prod_{i<j} (X_i - X_j)$$

である. 特に, $e_1, \ldots, e_n$ は代数的に独立である.

証明. 証明の方法は, Vandermonde(ヴァンデルモンド) 行列式が差積の ± 1 倍になることを示すのと同じである. $J(X_1, \ldots, X_n) = \det \left(\dfrac{\partial e_i}{\partial X_j} \right)$ とおく. e_k が対称式なので, 変数 X_i, X_j の置換をすると, 行列 $\left(\dfrac{\partial e_i}{\partial X_j} \right)$ は, 第 i 列と第 j 列の置換が起こる. すなわち,

$$J(X_1, \ldots, X_j, \ldots, X_i, \ldots, X_n) = -J(X_1, \ldots, X_i, \ldots, X_j, \ldots, X_n)$$

が成立する. 特に $X_i = X_j$ なら $J(X_1, \ldots, X_i, \ldots, X_i, \ldots, X_n) = 0$ となり, このことから, $J(X_1, \ldots, X_n)$ は $(X_i - X_j)$ で割り切れる. i, j は任意なので, $J(X_1, \ldots, X_n)$ は $\displaystyle\prod_{i<j} (X_i - X_j)$ で割り切れる. $\deg e_k = k$ なので, 両辺の次数はともに $\dfrac{n(n-1)}{2}$ となり,

$$J(X_1, \ldots, X_n) = C \prod_{i<j} (X_i - X_j)$$

となる. $X_1^{n-1}X_2^{n-2}\cdots X_{n-1}$ の係数を比較すると, 右辺の係数は C である. 行列式の方で, 積 $X_1^{n-1}\cdots X_{n-1}$ を作るためには, X_n が現れないことから, 第 n 行で, (n,n)–成分, $\dfrac{\partial e_n}{\partial X_n}$ を用いた積の項でなければならない. この項には, X_1 があるので, 第 $n-1$ 行では, $(n-1,n-1)$ 成分を選ぶしかない. この考察を繰り返すと, $X_1^{n-1}\cdots X_{n-1}$ の係数に寄与するのは, 行列式の対角成分の積だけなので, $C=1$ を得る.

系 E.1 k を可換体とする. 環として, 次は同型である.

$$k[X_1,\ldots,X_n]^{S_n} \cong k[e_1,\ldots,e_n]$$

F 終結式を用いた方程式の判別式の計算

代数方程式の判別式は, 置換群の作用で不変であるので, 前節の結果より係数の多項式になる. しかし, 定義に従ってそれを計算することは, 3 次方程式でも面倒であることは, 4.11 節で見たとおりである. 当然, 4 次以上となるともっと複雑になる. ただし, ここで述べる終結式を用いると, 判別式が行列式 (判別式も行列式も, 英語にすると determinant) で書け, 少しだけ計算がやさしくなる.

2 つの多項式

$$f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \quad (a_n \neq 0)$$
$$g(X) = b_mX^m + b_{m-1}X^{m-1} + \cdots + b_1X + b_0 \quad (b_m \neq 0)$$

に対して, 次の $(m+n)$ 次正方行列の行列式を, Sylvester(シルベスター) の行列式, あるいは f, g の終結式 (resultant) という.

$$R(f,g) = \begin{vmatrix}
a_n & a_{n-1} & \cdots & \cdots & \cdots & a_0 & 0 & \cdots & \cdots & 0 \\
0 & a_n & a_{n-1} & \cdots & \cdots & \cdots & a_0 & 0 & \cdots & 0 \\
0 & 0 & a_n & a_{n-1} & \cdots & \cdots & \cdots & a_0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & 0 & a_n & a_{n-1} & \cdots & \cdots & \cdots & a_0 \\
b_m & b_{m-1} & \cdots & \cdots & b_1 & b_0 & 0 & \cdots & 0 & 0 \\
0 & b_m & b_{m-1} & \cdots & \cdots & b_1 & b_0 & \cdots & 0 & 0 \\
\vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\
\vdots & \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\
0 & 0 & \cdots & 0 & b_m & b_{m-1} & \cdots & \cdots & b_1 & b_0
\end{vmatrix}$$

ここで, f の係数を並べた行は第 1 行から第 m 行までで, g の係数を並べた行は第 $m+1$ 行から第 $m+n$ 行までである.

$f(X)=0$ の根を $\lambda_1,\ldots,\lambda_n$, $g(X)=0$ の根を $\mu_1,\ldots,\mu_m$ とする. このとき, 次が成立する.

定理 F.1 上の記号と条件のもとで,

$$R(f,g) = a_n^m b_n^m \prod_{i,j}(\lambda_i - \mu_j)$$

が成立する.

証明. $a_n \neq 0$, $b_m \neq 0$ より, 最初の m 行の成分を a_n でくくり出し, 最後の n 行の成分を b_m でくくり出すと,

$$R(f,g) = a_n^m b_m^n \begin{vmatrix} 1 & \frac{a_{n-1}}{a_n} & \cdots & \cdots & \frac{a_0}{a_n} & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \frac{a_{n-1}}{a_n} & \cdots & \frac{a_{n-1}}{a_n} & \frac{a_0}{a_n} & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & \frac{a_2}{a_n} & \frac{a_1}{a_n} & \frac{a_0}{a_n} & \cdots & 0 & 0 \\ 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 1 & \cdots & \cdots & \cdots & \frac{a_1}{a_n} & \frac{a_0}{a_n} \\ 1 & \frac{b_{m-1}}{b_m} & \cdots & \cdots & \cdots & \frac{b_0}{b_m} & 0 & \cdots & 0 & 0 \\ 0 & 1 & \frac{b_{m-1}}{b_m} & \cdots & \cdots & \frac{b_1}{b_m} & \frac{b_0}{b_m} & \cdots & 0 & 0 \\ 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 0 \\ 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 1 & \cdots & \cdots & \cdots & \frac{b_1}{b_m} & \frac{b_0}{b_m} \end{vmatrix}$$

となる. 上の行列式の各成分に方程式の根と係数の関係式 (1.2)

$$\frac{a_{n-k}}{a_n} = (-1)^k \sum_{i_1<i_2<\cdots<i_k} \lambda_{i_1} \cdots \lambda_{i_k}, \qquad \frac{b_{m-k}}{b_m} = (-1)^k \sum_{i_1<i_2<\cdots<i_k} \mu_{i_1} \cdots \mu_{i_k}$$

を代入すると, $\dfrac{R(f,g)}{a_n^m b_m^n}$ は λ_i, μ_j の多項式になることがわかる. λ_i は, 行列の 1 行目から m 行目までの成分に, 高々 1 次式で現れ, μ_j は $m+1$ 行目から $m+n$ 行目までに, 高々 1 次式で現れる. 行列式は, 行列の各行, 各列から成分を 1 つずつ取り出して積を取ったものの和であり, このような積においては, λ_i は高々 n 乗しか作ることができない. 同様に, μ_j の最高次数は, m である. 従って, $R(f,g)$ を λ_i, μ_j の多項式と見た場合, λ_i について高々 m 次式, μ_j について高々 n 次式である.

i を固定して, $R(f,g)$ を λ_i の (m 次の) 多項式と考える. この多項式は, $\mu_1, \ldots, \mu_m$ を根に持つ. 実際, $\lambda_i = \mu_j$ とすると, この共通の値を λ とすると, これは $f(X)$, $g(X)$ の共通根だから, 次が成立する.

$$\begin{pmatrix} a_n & a_{n-1} & \cdots & \cdots & a_0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & a_n & a_{n-1} & \cdots & a_1 & a_0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & a_n & \cdots & a_2 & a_1 & a_0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & 0 & \cdots & 0 & a_n & \cdots & \cdots & \cdots & a_1 & a_0 \\ b_m & b_{m-1} & \cdots & \cdots & \cdots & b_0 & 0 & \cdots & 0 & 0 \\ 0 & b_m & b_{m-1} & \cdots & \cdots & b_1 & b_0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 0 \\ 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & b_0 & 0 \\ 0 & 0 & \cdots & 0 & b_m & b_{m-1} & \cdots & \cdots & b_1 & b_0 \end{pmatrix} \begin{pmatrix} \lambda^{m+n-1} \\ \lambda^{m+n-2} \\ \lambda^{m+n-3} \\ \vdots \\ \lambda^n \\ \lambda^{n-1} \\ \lambda^{n-2} \\ \vdots \\ 1 \end{pmatrix} = \mathbf{o}$$

左辺の積の列ベクトルは $\mathbf{o}$ ではないので, 左辺の行列の行列式は 0 となり, $R(f,g)$ は λ_i の多項式と見て, μ_j を根に持つ. すなわち, $R(f,g)$ は λ_i の多項式と見て, $\lambda_i - \mu_j$ で割り切れる. i, j は任意に取れるので, $R(f,g)$ は $\prod(\lambda_i - \mu_j)$ で割り切れる. この積の λ_i の次数は m, μ_j の次数は n なので, $R(f,g)$ の次数と一致する. よって, ある定数 C が存在して,

$$R(f,g) = C \cdot a_n^m b_m^n \prod(\lambda_i - \mu_j)$$

となる. 右辺を展開して現れる $(\mu_1 \cdots \mu_m)^n$ の項は, $g(X)$ と μ_j に対する根と係数の関係を用いると,

$$C \cdot a_n^m b_m^n ((-1)^m (\mu_1 \cdots \mu_m))^n = C \cdot a_n^m ((-1)^m b_m \mu_1 \cdots \mu_m)^n = C \cdot a_n^m b_0^n$$

となるが, 左辺の行列式で上の項が現れるのは, 対角成分の積のところで, その係数 (恒等置換の符号) は 1 である. よって, $C = 1$ となり, 証明を得る.

系 F.1　$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ とする．$f(X) = 0$ の根を $\alpha_1, \ldots, \alpha_n$ とし，f の判別式を，$D(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2$ で定義する．このとき，

$$D(f) = (-1)^{\frac{n(n-1)}{2}} R(f, f')$$

が成立する．ここで，$f'(X) = nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \cdots + a_1$ は，f の形式的な微分である．

証明.　定理 F.1 から，n 次方程式 $g(X) = 0$ の根を $\lambda_1, \ldots, \lambda_n$，$m$ 次方程式 $h(X) = 0$ の根を $\mu_1, \ldots, \mu_n$ とすると，これらの終結式は，

$$R(g, h) = a_n^n \prod_{j=1}^{n} g(\lambda_i) = (-1)^{mn} b_m^m \prod_{j=1}^{m} h(\mu_j)$$

となることに注意する．ここで，a_n，b_m はそれぞれ，g，h の最高次の係数である．

$f(X) = 0$ の根が $\alpha_1, \ldots, \alpha_n$ なので，$f(X) = \prod(X - \alpha_i)$ である．積の微分法より，

$$f'(X) = \sum_{k=1}^{n} \left(\prod_{i \neq k} (X - \alpha_i) \right)$$

となる．従って，$f'(\alpha_j) = \prod_{\substack{i=1 \\ i \neq j}}^{n} (\alpha_j - \alpha_i)$ となる．上の式を用いると，

$$R(f, f') = (-1)^{n(n-1)} \prod_{j=1}^{n-1} f'(\alpha_j) = (-1)^{n(n-1)} \prod_{j=1}^{n-1} \left(\prod_{i \neq j} (\alpha_j - \alpha_i) \right)$$

右辺の積で，$j > i$ となる組は，$\dfrac{n(n-1)}{2}$ 個あるので，符号を考えると，

$$R(f, f') = (-1)^{\frac{n(n-1)}{2}} \prod_{i<j} (\alpha_i - \alpha_j)^2$$

となり，定理を得る．

例 F.1　以下の例を見ると，3 次方程式では定義に従った素朴な計算より，行列式を用いたほうが少し易しい計算であると言える．4 次方程式では，定義に基づいた計算は大変だが，行列式では手計算ができなくもないというものになる．5 次以上になると，どちらでやっても大変である．ちなみに，Maple には，resultant という終結式の計算をする手続きが定義されている．Maple には方程式の判別式を計算する手続きもあり，discrim (discriminant の略，これも判別式と訳す) という名前である．

1. 3 次方程式 $X^3 + pX + q = 0$ の判別式は，

$$(-1)^3 \det \begin{pmatrix} 1 & 0 & p & q & 0 \\ 0 & 1 & 0 & p & q \\ 3 & 0 & p & 0 & 0 \\ 0 & 3 & 0 & p & 0 \\ 0 & 0 & 3 & 0 & p \end{pmatrix} = -(4p^3 + 27q^2)$$

2. 4 次方程式 $X^4+pX^2+qX+r=0$ の判別式は, (Maple を利用して計算すると)

$$(-1)^6\det\begin{pmatrix}1&0&p&q&r&0&0\\0&1&0&p&q&r&0\\0&0&1&0&p&q&r\\4&0&2p&q&0&0&0\\0&4&0&2p&q&0&0\\0&0&4&0&2p&q&0\\0&0&0&4&0&2p&q\end{pmatrix}=16p^4r-4p^3q^2-128p^2r^2+144pq^2r-27q^4+256r^3$$

G　不還元の場合

実際に 3 次方程式の根の公式を使うと興味深いことが起こる. 実数係数の方程式であるが, 根の計算において複素数が現れるのである. 「複素数も数である」という認識が広がった 1 つの理由でもある.

まず, 方程式 $X^3-15X-4=0$ を根の公式を用いて解いてみる. 1.1 節の公式を適用しようとすると, $p=-15$, $q=-4$ であるので, $\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3=-121$ となる. 1.1 節の根の公式より, この 3 次方程式の根は,

$$\begin{aligned}\theta_1&=(2+11\sqrt{-1})^{\frac{1}{3}}+(2-11\sqrt{-1})^{\frac{1}{3}}\\ \theta_2&=(2+11\sqrt{-1})^{\frac{1}{3}}\left(\frac{-1+\sqrt{-3}}{2}\right)+(2-11\sqrt{-1})^{\frac{1}{3}}\left(\frac{-1-\sqrt{-3}}{2}\right)\\ \theta_3&=(2+11\sqrt{-1})^{\frac{1}{3}}\left(\frac{-1-\sqrt{-3}}{2}\right)+(2-11\sqrt{-1})^{\frac{1}{3}}\left(\frac{-1+\sqrt{-3}}{2}\right)\end{aligned}$$

となる. ここで, 立方根 $(2+11\sqrt{-1})^{\frac{1}{3}}$, $(2-11\sqrt{-1})^{\frac{1}{3}}$ がどうなるかが問題になる (複素数は, $a+b\sqrt{-1}$, $a,b\in\mathbb{R}$ の形の数全体であることに注意する). 簡単な計算で,

$$(2+\sqrt{-1})^3=2+11\sqrt{-1},\qquad (2-\sqrt{-1})^3=2-11\sqrt{-1}$$

がわかるので, これらの立方根が求まる. その結果を上に代入すると,

$$\theta_1=4,\quad \theta_2=-2-\sqrt{3},\quad \theta_3=-2+\sqrt{3}$$

であることがわかる. 実際, 元の方程式は, $X^3-15X-4=(X-4)(X^2+4X+1)$ の因数分解を利用すれば, 上の根が簡単に計算される.

問題は, 上の方程式の根はすべて実数であるのに, 根の公式を用いると途中に複素数が現れる点である. 最終的な解答が実数であるからには, 複素数を用いずに根を計算できた方が, より望ましい解法であると言える. 上の場合は, 因数分解を利用することにより, 複素数を利用せずに計算できた. しかし, 一般的にはそれが不可能であることが, 次の考察からわかる.

$f(X)\in\mathbb{Q}[X]$ を $\mathbb{Q}$ 上既約な 3 次多項式とし, $f(X)=0$ は 3 つの実根を持つとする. θ_1, θ_2, θ_3 をその根とし, $L=\mathbb{Q}(\theta_1,\theta_2,\theta_3)$ を f の分解体とする. これらの根が実数のべき根の計算だけで求まるということは, 次のような拡大体の列

$$\mathbb{Q}=K_0\subset K_1\subset\cdots\subset K_n,\qquad K_i=K_{i-1}(\sqrt[k_i]{a_i}),\quad a_i\in K_{i-1},\quad \sqrt[k_i]{a_i}\in\mathbb{R}$$

が存在して, $L\subset K_n$ となることになる. このとき特に, L は実数以外の元を含まないことに注意する.

上の拡大体の列において, 3 つの根 θ_1, θ_2, θ_3 のどれかが最初に含まれるものを, K_l とする. このとき, K_{l-1} には f のどの根も含まれない. f が 3 次式であることから, f は K_{l-1} 上既約な多項式となる (f が分解されるなら, 1 次式の因子があるので, 根を含む必要がある). 必要なら根の順番を入れ替えて, $K_l \ni \theta_1$ とする. 拡大体の列

$$K_{l-1} \subset K_{l-1}(\theta_1) \subset K_l = K_{l-1}(\sqrt[k_l]{a_l}) \subset L$$

を考えると, K_{l-1} 上の f の既約性から $[K_{l-1}(\theta_1) : K_{l-1}] = 3$ である. 従って,

$$[K_{l-1}(\sqrt[k_l]{a_l}) : K_{l-1}] = [K_l : K_{l-1}(\theta_1)][K_{l-1}(\theta_1) : K_{l-1}] = 3[K_l : K_{l-1}(\theta_1)]$$

となるので, k_l は 3 の倍数となる. $k_l = 3d$ として, $a = \sqrt[d]{a_l} \in \mathbb{R}$, $K' = K_{l-1}(a)$ とすると, $\theta \in K'(\sqrt[3]{a})$ となる. L は $\mathbb{Q}$ 上正規拡大で $K' \subset L$ なので, L/K' は正規拡大である. $\sqrt[3]{a} \in L$ であるが, ω を 1 の原始 3 乗根とすると $\sqrt[3]{a}$ の K' 上の共役元 $\sqrt[3]{a}\omega \notin \mathbb{R}$ も L の元となる. これは, 上のような実数体の部分体からなる列が取れないことを示している.

H　円分多項式 (4.8 節の補足)

この節では, 標数 0 の素体 $\mathbb{Q}$ で考える. $m \in \mathbb{N}$ として, $\zeta_m \in \overline{\mathbb{Q}}$ を 1 の原始 m 乗根の 1 つとする. (例えば, $\zeta_m = e^{\frac{2\pi i}{m}}$) このとき, 1 の m 乗根の集合は, $\mu_m = \{1, \zeta_m, \ldots, \zeta_m^{m-1}\}$ で与えられる. 1 の原始 m 乗根の集合を μ_m^{pr} と書くことにすると, $\mu_m^{\mathrm{pr}} = \left\{ \zeta_m^i \mid (m,i) = 1,\ 1 \leqq i < m \right\}$ となる. 1 の原始 m 乗根全体を根に持つ多項式,

$$\Phi_m(X) = \prod_{\zeta \in \mu_m^{\mathrm{pr}}} (X - \zeta) = \prod_{(m,d)=1} (X - \zeta_m^d)$$

が円分多項式である.

r を m の約数とする. $d = \dfrac{m}{r}$ とすると, ζ_m^d は 1 の原始 r 乗根になる. 1 の原始 r 乗根の集合は, ζ_m を用いて次のように与えられる.

$$\mu_r^{\mathrm{pr}} = \left\{ (\zeta_m)^{dk} \mid 1 \leqq k < r,\, (r,k) = 1 \right\} = \left\{ \zeta_m^i \mid 1 \leqq i < m,\, (m,i) = d \right\}$$

r が m の約数全体を動けば, $d = \dfrac{m}{r}$ も m の約数全体を動くので, μ_m の集合としての次の直和分解を得る.

$$\mu_m = \coprod_{d|m} \mu_d^{\mathrm{pr}}$$

したがって, Φ_m の定義から,

$$X^m - 1 = \prod_{d|m} \Phi_d(X)$$

が成立する.

定理 H.1　$\Phi_m(X) \in \mathbb{Z}[X]$ であり, $\mathbb{Q}$ 上既約である. 特に, $\Phi_m(X)$ は ζ_m の $\mathbb{Q}$ 上の最小多項式である.

証明.　$\Phi_m(X) \in \mathbb{Z}[X]$ は, m に関する帰納法で証明される. $m = 1$ のときは, $\Phi_1(X) = X - 1$ で成立する. $m - 1$ まで成立するとする. 仮定より, 因数分解

$$X^m - 1 = \Phi_m(X) \left(\prod_{d|m,\ d<m} \Phi_d(X) \right)$$

において, $\prod_{d|m,\ d<m} \Phi_d(X) \in \mathbb{Z}[X]$ である. 多項式の積の定義から, $\Phi_m(X) \in \mathbb{Q}[X]$ がわかる. このとき, 注意 3.7.1, 1. より, $\Phi_m(X) \in \mathbb{Z}[X]$ である.

次に, $\Phi_m(X)$ が $\mathbb{Z}[X]$ で規約であることを示す. $f(X)$ を ζ_m の $\mathbb{Q}$ 上の最小多項式とすると, $\Phi_m(\zeta_m) = 0$ より, $f(X) \,|\, \Phi_m(X)$ である. したがって, 上の証明で用いたことと同じ理由で $f(X) \in \mathbb{Z}[X]$ とでき, $\Phi_m(X) = f(X)g(X)$, $g(X) \in \mathbb{Z}[X]$ となる. $g(X)$ の取り方から, $f(X)$ と $g(X)$ の最大公約因子は, 1 である.

$\deg g \geqq 1$ と仮定して矛盾を導く. $g(X) = 0$ の ($\overline{\mathbb{Q}}$ での) 根も, 1 の原始 m 乗根なので, ζ_m^d, $(m, d) = 1$ の形である. ζ_m は $f(X) = 0$ の根なので, $d > 1$ である. このような最小の d を取り, p を d の約数となる素数とする. $\zeta' = \zeta_m^{\frac{d}{p}}$ とおく. $(m, d) = 1$ なので, $(m, p) = 1$ で, ζ' も 1 の原始 m 乗根である. d の取り方から, $f(\zeta') = 0$ となる. f の既約性から, $f(X)$ は ζ' の $\mathbb{Q}$ 上の最小多項式になる. $g(\zeta'^p) = g(\zeta_m^d) = 0$ なので, $g(X^p)$ は ζ' を根に持つ $\mathbb{Z}[X]$ の元である. よって, $g(X^p) = f(X)h(X)$, $h(X) \in \mathbb{Z}[X]$ と因数分解される.

ここで, 整数係数多項式の係数を mod p で考えて, $\mathbb{Z}/p\mathbb{Z}$ 係数の多項式と考え, その多項式を, 元の多項式に $\bar{}$ をつけて表すことにする. 上に述べたことから,

$$\overline{f}(X)\overline{h}(X) \equiv \overline{g}(X^p) \equiv (\overline{g}(X))^p \pmod{p}$$

が成立する. f はモニック (最高次の係数が 1) なので, $\deg \overline{f} > 0$ である. 上の式より, $\mathbb{Z}/p\mathbb{Z}$ の代数閉包の中で, $\overline{g}(X) = 0$ と $\overline{f}(X) = 0$ は共通根を持つ. 一方, $f(X)g(X) \,|\, (X^m - 1)$ と $(m, p) = 1$ より, $\overline{f}(X)\overline{g}(X) \,|\, (X^m - 1) \pmod{p}$ である. したがって, $\overline{g}(X) = 0$ と $\overline{f}(X) = 0$ は共通根は, $X^m - 1 = 0$ の $\mathbb{Z}/p\mathbb{Z}$ の代数閉包の中での重根になる. しかし, $(p, m) = 1$ なので, $X^m - 1 = 0$ は $\mathbb{Z}/p\mathbb{Z}$ では分離的な多項式となり, 重根は持たず, 矛盾する.

系 H.1 $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$

証明. 上のことから, $\mathbb{Q}(\zeta_m)$ は $\mathbb{Q}$ 上既約な方程式 $\Phi_m(X) = 0$ の分解体であり, $\mathbb{Q}$ 上の Galois 拡大になる. よって, $|\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})| = [\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \deg \Phi_m = \varphi(m)$ となる. 定理 4.8.1 より, $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ は, $(\mathbb{Z}/m\mathbb{Z})^\times$ の部分群と同型であるが, 位数を考えて, $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$

問 H.1 (問 4.8.1) 自然数 n に対して, n の Möbius (メビウス) 関数 $\mu(n)$ を次で定義する.

$$\mu(n) = \begin{cases} 1 & n = 1 \\ (-1)^m & n = p_1 \cdots p_m \ (n \text{ の素因数分解}, p_i \neq p_j) \\ 0 & \text{それ以外 (1 以外の平方数を因子に持つ).} \end{cases}$$

すなわち, $\mu(n)$ は n を素因数分解したとき, 平方数を因子に持てば 0 で, そうでなければ, 素因数の個数だけ -1 を乗じたものとして定義する. このとき,

$$\Phi_m(X) = \prod_{d|m} (X^d - 1)^{\mu(\frac{m}{d})}$$

が成立することを示せ. (考え方は, 問 1.2.3, 2. と同じ.)

I 有限体

この節では有限個の元からなる体を考える. 有限体は, 情報通信の分野で符号理論や暗号理論に利用されており, 現実世界で利用されているものである. これがなければ, 音楽 CD や情報通信機器は作ることができないものである.

K を有限体とする．$\mathrm{char}(K) = 0$ なら，$K \supset \mathbb{Q}$ となるので，K は有限体ではない．従って，$\mathrm{char}(K) = p > 0$ である．K の素体を $\mathbb{F}_p = \{0, 1, \ldots, p-1\} \cong \mathbb{Z}/p\mathbb{Z}$ と書くことにする．K は $\mathbb{F}_p$ 上の有限次元ベクトル空間なので，$[K : \mathbb{F}_p] = n$ とすると，$|K| = p^n$ である．

まずは，有限体は常に可換体になるという，有名な Wedderburn の定理を示す．

定理 I.1（Wedderburn）　非可換な有限体は存在しない．

証明.　K を有限体とし，非可換であるとする．$Z = \{a \in K \mid ax = xa,\ \forall x \in K\}$ を K の中心とする．Z は K の可換な部分体になる．よって，$|Z| = p^l$ である．$|Z| = q$ とする．K は Z 上の有限次元ベクトル空間であるので，$|K| = q^m$ となる．$m = 1$ なら，$K = Z$ となるので，K は可換体になる．$m > 1$ として，矛盾を導く．$K^\times = K \setminus \{0\}$ の乗法群の類等式を考える．

$$q^m - 1 = q - 1 + \sum_x |C_x|$$

ここで，$q - 1 = |Z \setminus \{0\}|$ であり，C_x は x の共役類である．$|C_x| = \dfrac{|K \setminus \{0\}|}{|C_{K\setminus\{0\}}(x)|}$ となるが，$C_K(x) = \{a \in K \mid ax = xa\}$ が Z を含む部分体，すなわち，Z の拡大体になることが容易にわかるので，自然数 $\delta(x)$ が存在して，$|C_{K\setminus\{0\}}(x)| = q^{\delta(x)} - 1$ となる．従って上の類等式は，

$$q^m - 1 = q - 1 + \sum_x \frac{q^m - 1}{q^{\delta(x)} - 1}$$

となる．ここで，$\Phi_m(X)$ を m 次の ($\mathbb{Q}$ 上の) 円分多項式とすると，左辺の $q^m - 1$ および右辺の和の各成分 $\dfrac{q^m - 1}{q^{\delta(x)} - 1}$ は $\Phi_m(q)$ の倍数である．実際，$m > \delta(x)$ なので，分母 $q^{\delta(x)} - 1$ は q の多項式と見て 1 の原始 m 乗根を根に持たないことに注意すれば良い．よって特に，$q - 1$ は $\Phi_m(q)$ の倍数となる．ここで，$\Phi_m(X) \in \mathbb{Z}[X]$(定理 H.1) なので，$\Phi_m(q) \in \mathbb{Z}$ に注意する．一方，$\zeta_m \in \mathbb{C}$ を 1 の原始 m 乗根とすると，$\Phi_m(X) = \displaystyle\prod_{(d,m)=1} (X - \zeta_m^d)$ であり，$|\zeta_m| = 1$, $q \geqq 2$ より，$|q - \zeta_m^d| > q - 1 \geqq 1$ となり，

$$|\Phi_m(q)| = \prod_{(n,d)=1} |q - \zeta_m^d| > (q-1)^{\varphi(n)} \geqq q - 1$$

となる．これは，$q - 1$ が $\Phi_m(q)$ の倍数であることに矛盾する．

$q = p^n$ とし，K を q 個の元からなる有限体とする．このとき，$K^\times = K \setminus \{0\}$ は，体の有限乗法群なので，位数 $q - 1$ の巡回群となる (系 4.8.1)．特に，$x \in K \setminus \{0\}$ とすると，$x^{q-1} = 1$ が成立する．よって K の元は，方程式 $X^q - X = 0$ の根の集合となる．

$\overline{\mathbb{F}}_p$ を $\mathbb{F}_p$ の代数的閉包とする．上のことから，

$$K = \{x \in \overline{\mathbb{F}}_p \mid x^q - x = 0\}$$

が成立する．特に，K は $\overline{\mathbb{F}}_p$ の方程式 $X^q - X = 0$ の分解体であり，この方程式は重根を持っていないので，$K/\mathbb{F}_p$ は分離拡大であることもわかる．すなわち，$K/\mathbb{F}_p$ は，Galois 拡大である．

$$\sigma : \overline{F}_p \to \overline{F}_p\,, \quad \sigma(x) = x^p$$

とすると，σ は $\overline{\mathbb{F}}_p$ の自己同型写像であり，$\sigma_{|\mathbb{F}_p} = \mathrm{id}_{\mathbb{F}_p}$, $\sigma(K) = K$ が成立する．すなわち，$\sigma \in \mathrm{Gal}(K/\mathbb{F}_p)$ である．また，$x \in K$ に対して，$\sigma^n(x) = x^{p^n} = x^q = x$ であるので，$\sigma^n_{|K} = \mathrm{id}_K$ である．$k = 1, \ldots, n-1$ に対して，

$\sigma^k(x) = x$ は, 方程式 $x^{p^k} = x$ の根と同値なので, 根の個数を数えることにより, $\sigma^k_{|K} \neq \mathrm{id}_K$, $k = 1, \ldots, n-1$ である. $|\mathrm{Gal}(K/\mathbb{F}_p)| = [K : \mathbb{F}_p] = n$ なので, $\mathrm{Gal}(K/\mathbb{F}_p)$ は, σ から生成される位数 n の巡回群となる.

以上をまとめて, 次を得る.

定理 I.2 p を素数, K を $q = p^n$ 個の元からなる有限体とする. このとき, 次が成立する.

1. $\overline{\mathbb{F}}_p$ を K の素体 $\mathbb{F}_p$ の代数的閉包とすると, $K = \{x \in \overline{\mathbb{F}}_p \mid x^q - x = 0\}$ である. 特に, q 個の元を持つ有限体は, 同型を除いて一意的に存在する.
2. $K/\mathbb{F}_p$ は Galois 拡大であり, $\mathrm{Gal}(K/\mathbb{F}_p) =< \sigma >$ は位数 n の巡回群である. ここで, σ は $\sigma(x) = x^p$ で定まる K の自己同型写像である.

上の定理から, q 個の元を持つ有限体は同型を除いて一意的に定まるので, それを $\mathbb{F}_q$ と書いたり (数学系業界) $\mathrm{GF}(q)$ と書いたり (情報系業界, GF は Galois field の略) する.

$\mathbb{F}_q$ の有限次拡大体も有限体になる. 上の考察と全く同様にして, 次のことが証明される.

定理 I.3 $\mathbb{F}_q$ を q 個の元からなる有限体とする. $n \in \mathbb{N}$ に対して, $\mathbb{F}_{q^n}$ は $\mathbb{F}_q$ の n 次の Galois 拡大体であり, $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) =< \sigma_q >$ は, 位数 n の巡回群となる. ここで, $\sigma_q(x) = x^q$, $x \in \mathbb{F}_{q^n}$ である.

問 I.1 上の定理の証明を書け.

J $\mathbb{Q}(\zeta_p)$ と Gauss 和

素数 p に対して, ζ_p を 1 の原始 p 乗根とする. $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ が成立するのは, 上で見たとおり (系 H.1) である. $\mathbb{Z}/p\mathbb{Z}$ は体なので, $(\mathbb{Z}/p\mathbb{Z})^\times$ は位数 $p-1$ の巡回群である. $p \geqq 3$ とすると, $(\mathbb{Z}/p\mathbb{Z})^\times$ には指数 2(i.e. 位数 $\dfrac{p-1}{2}$) の部分群 H がただひとつ存在する. この部分群 H に対する固定体 $\mathbb{Q}(\zeta_p)^H$ を確定させるのが, この節の内容である. すなわち, 例 4.8.2 の前半部分を一般の素数で考える. 例 4.8.2 では, 直接計算によって不変体を求めたが, 場合分けの煩雑さを避けるため, ここでは Gauss 和を利用する.

1 の p 乗根 $\zeta_p (\neq 1)$ をひとつ取って固定する. $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ の $\mathbb{Q}(\zeta_p)$ への Galois 群としての作用は, $\zeta_p \to \zeta_p^a$ で与えられる. 乗法群の生成元 (原始根と呼ばれる) $r \in (\mathbb{Z}/p\mathbb{Z})^\times$ をひとつ取って固定する[*10]. このとき, $(\mathbb{Z}/p\mathbb{Z})^\times = \{1, r, r^2, \ldots, r^{p-2}\}$ である. この群の指数 2 の部分群は,

$$H =< r^2 >= \{1, r^2, r^4, \ldots, r^{p-3}\}$$

である. $H \lhd (\mathbb{Z}/p\mathbb{Z})^\times$ なので, Galois の基本定理より, $\mathbb{Q}(\zeta_p)^H/\mathbb{Q}$ は Galois 拡大で, $\mathrm{Gal}(\mathbb{Q}(\zeta_p)^H/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times/H \cong \mathbb{Z}/2\mathbb{Z}$ となり, $\mathbb{Q}(\zeta_p)^H$ は $\mathbb{Q}$ の 2 次拡大である.

$$\alpha = \zeta_p^r + \zeta_p^{r^3} + \cdots + \zeta_p^{r^{p-2}} = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times \setminus H} \zeta_p^a$$
$$\beta = \zeta_p + \zeta_p^{r^2} + \cdots + \zeta_p^{r^{p-3}} = \sum_{a \in H} \zeta_p^a$$

とおくと, r の Galois 群の元としての作用は, α, β の互換を与える. よって, α, β は r^2 の作用で不変となり, $\alpha, \beta \in \mathbb{Q}(\zeta_p)^H$ である. さらに, $\alpha + \beta$, $\alpha\beta$ は r の作用で不変であり, r は Galois 群を生成するから,

[*10] 原始根の取り方は, $\varphi(p-1)$ 通りある. ここで, φ は Euler の関数である.

$\alpha+\beta, \alpha\beta \in \mathbb{Q}$ である. すなわち, $\mathbb{Q}(\zeta_p)^H$ は, $X^2-(\alpha+\beta)X+\alpha\beta \in \mathbb{Q}[X]$ の分解体である.

$$\alpha+\beta = \sum_{a\in(\mathbb{Z}/p\mathbb{Z})^\times} \zeta_p^a = \zeta_p+\zeta_p^2+\cdots+\zeta_p^{p-1} = -1$$

は容易にわかる. 例 4.8.2 では, $\alpha\beta$ を本質的に直接計算しているが, 一般的な場合を扱うには, 判別式 $(\beta-\alpha)^2$ の方が計算がしやすいので, それを紹介する.

判別式の平方根

$$G_p = \beta-\alpha = \sum_{a\in H} \zeta_p^a - \sum_{a\in(\mathbb{Z}/p\mathbb{Z})^\times\setminus H} \zeta_p^a$$

は, Gauss 和と呼ばれている. 判別式 (Gauss 和の 2 乗) を計算するために, 平方剰余記号 (Legendre (ルジャンドル) の記号) を導入する. (乗法) 群の準同型写像,

$$(\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm1\}, \quad (\mathbb{Z}/p\mathbb{Z})^\times \ni a \mapsto \left(\frac{a}{p}\right) \in \{\pm1\}$$

を, $\left(\dfrac{r}{p}\right) = -1$ で定める. $\left(\dfrac{a}{p}\right)$ を平方剰余記号という. $\left(\dfrac{0}{p}\right) = 0$ として, $\mathbb{Z}/p\mathbb{Z}$ 上に拡張しておく. H の決め方から, $\left(\dfrac{a}{p}\right) = 1 \Leftrightarrow a \in H$ (i.e H はこの準同型写像の核) である.

定義から, 次が直ちにわかる.

命題 J.1 1. $\left(\dfrac{ab}{p}\right) = \left(\dfrac{a}{p}\right)\left(\dfrac{b}{p}\right), \quad a,\ b \in (\mathbb{Z}/p\mathbb{Z})^\times$

2. $\displaystyle\sum_{a=1}^{p-1}\left(\frac{a}{p}\right) = 0$

3. $\left(\dfrac{a}{p}\right) = 1 \Longleftrightarrow a \neq 0$ かつ $x^2 \equiv a \pmod p$ は解を持つ.

証明. 1. は準同型写像という定義そのものである.

2. は, H が指数 2 の部分群であることから従う.

3. $\left(\dfrac{a}{p}\right) = 1$ なら $a \in H$ なので, 原始根 r と非負整数 k を用いて, $a = r^{2k}$ となる. よって, $x = \pm r^k$ は $x^2 \equiv a \pmod p$ の解である. 逆に $x^2 \equiv a \pmod p$ の解を $x = r^k$ とすると, $a = r^{2k} \in H$ となり, $a \in H$ で $\left(\dfrac{a}{p}\right) = 1$ である.

Fermat の小定理から, $(a,p) = 1$ のとき $a^{p-1} \equiv 1 \pmod p$ が成立する. 両辺の平方根をとると, $a^{\frac{p-1}{2}} \equiv \pm1 \pmod p$ を得る. 実際には, 右辺は平方剰余と合同である.

補題 J.1 (Euler(オイラー) の基準)

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$$

証明. $a \equiv 0 \pmod p$ のとき, 両辺は 0 なので明らかに成立する.

原始根 r に対して, $r^{\frac{p-1}{2}} \equiv -1 \pmod p$ である. 実際, $r^{p-1} \equiv 1 \pmod p$ だから, $r^{\frac{p-1}{2}} \equiv \pm1 \pmod p$ であるが, $r^{\frac{p-1}{2}} \equiv 1 \pmod p$ は原始根の定義に矛盾する. $a = r^k$ とすると,

$$\left(\frac{a}{p}\right) = (-1)^k \equiv r^{\frac{p-1}{2}k} = \left(r^k\right)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \pmod p$$

上の証明から次がわかる.

命題 J.2（第一補充法則）

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

証明. 原始根 r を用いると, $-1 \equiv r^{\frac{p-1}{2}} \pmod{p}$ なので, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

補題 J.2 1 の原始 n 乗根 μ と $a \in \mathbb{Z}$ に対して,

$$\sum_{k=1}^{n-1} \mu^{ak} = \begin{cases} n-1 & a \equiv 0 \pmod{n} \\ -1 & a \not\equiv 0 \pmod{n} \end{cases}$$

証明. $a \equiv 0 \pmod{n}$ なら, $\mu^{ak} = 1$, $k = 1, \ldots, n-1$ なので. 上の式は成立する. $a \not\equiv 0 \pmod{n}$ のときは, $\mu^a \neq 1$ なので, 等比数列の和の公式より,

$$\sum_{k=1}^{n-1} \mu^{ak} = \frac{\mu^a(1-\mu^{a(n-1)})}{1-\mu^a} = \frac{\mu^a - 1}{1-\mu^a} = -1$$

定理 J.1

$$G_p^2 = \left(\frac{-1}{p}\right) p = (-1)^{\frac{p-1}{2}} p$$

証明. 右側の等号は, 第一補充法則なので, 左側の等号を示す.

$$G_p^2 = \left(\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta_p^a\right) \left(\sum_{b=1}^{p-1} \left(\frac{b}{p}\right) \zeta_p^b\right) = \sum_{a,\,b=1}^{p-1} \left(\frac{ab}{p}\right) \zeta_p^{a+b}$$

である. ここで, $b = ac$ (i.e. $c \equiv a^{-1}b \pmod{p}$) で c を定めると, b が 1 から $p-1$ まで動くとき, c は, $\pmod{p}$ で 1 から $p-1$ を動く. ζ_p^k は $k \pmod{p}$ で値が定まるので, 平方剰余記号の性質を利用すると, 上の右辺は次のようになる.

$$G_p^2 = \sum_{a,\,c=1}^{p-1} \left(\frac{a^2c}{p}\right) \zeta_p^{a(1+c)} = \sum_{a,\,c=1}^{p-1} \left(\frac{a}{p}\right)^2 \left(\frac{c}{p}\right) \zeta_p^{a(1+c)} = \sum_{c=1}^{p-1} \left(\frac{c}{p}\right) \sum_{a=1}^{p-1} \zeta_p^{a(1+c)}$$

ここで, 右側の和に補題 J.2 を利用し, $c = p-1$ とそれ以外の部分に和を分けて考える. さらに命題 J.1 2. を利用すると ($p-1 \equiv -1 \pmod{p}$ に注意する),

$$G_p^2 = -\sum_{c=1}^{p-2} \left(\frac{c}{p}\right) + (p-1)\left(\frac{p-1}{p}\right) = \left(\frac{p-1}{p}\right) + (p-1)\left(\frac{p-1}{p}\right) = \left(\frac{-1}{p}\right) p$$

上の定理から, α, β を解とする 2 次方程式の判別式が計算された. よって, α, β は次で与えられる.

$$\frac{1}{2}(\alpha + \beta \pm \sqrt{G_p^2}) = \frac{-1 \pm \sqrt{(-1)^{\frac{p-1}{2}} p}}{2}$$

$\mathbb{Q}(\zeta_p)^H = \mathbb{Q}(\alpha)$ なので, 次を得る.

系 J.1 $\mathbb{Q}(\zeta_p)^H = \mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}}p}\right)$

注意 J.1 Gauss 和に関しては, 平方剰余の相互法則とともに述べられている書籍が沢山あるので, 興味のある人は, そちらを参考にして欲しい. 例えば, [3] には, 平方剰余の相互法則や, $\zeta_p = e^{\frac{2\pi i}{p}} \in \mathbb{C}$ としたときの Gauss 和の値の決定が書いてある. G_p^2 は上のように計算できるが, その平方根の符号を決定するのは, 難しいことが知られている.

参考文献

[1] 足立恒雄, ガロア理論講義, 日本評論社

[2] デイヴィッド A. コックス 著, 梶原健訳, ガロワ理論 (上, 下), 日本評論社 (原著, David A. Cox, Galois Theory, John Wiey & Sons)

[3] 藤崎源二郎, 体とガロア理論, 岩波基礎数学講座, 岩波書店

[4] 堀田良之, 代数入門 —群と加群—, 数学シリーズ, 裳華房

[5] 堀田良之, 可換環と体, 岩波書店

[6] 桂利行, 代数学 I 群と体, 東京大学出版会

[7] 桂利行, 代数学 II 環上の加群, 東京大学出版会

[8] 桂利行, 代数学 III 体とガロア理論, 東京大学出版会

[9] 森田康夫, 代数概論, 数学選書 9, 裳華房

[10] 佐武一郎, 線型代数学, 数学選書 1, 裳華房

[11] 鈴木通夫, 群論 (上, 下), 岩波書店

[12] 鈴木通夫, 有限単純群, 紀伊国屋書店

[13] 雪江明彦, 代数学 1 群論入門, 日本評論社

[14] 雪江明彦, 代数学 2 環と体とガロア理論, 日本評論社

[15] 上野健爾, 代数入門, 岩波書店

この講義ノートを作るにあたって参考にした書籍, および本文内で参照した書籍である. これら以外にも, 良書は沢山ある.