代数系

鈴木　咲衣

2019 年 11 月 30 日

目次

第 1 章

イントロダクション

1.1 成績の付け方

（第一回・12/2）（第二回・12/5）

日付はただの目安です。

この列はメモ用。

講義と演義の割合７：３で成績をつける．講義の成績は試験（中間・期末）とレポートの点数でつけます．

$$\text{講義の素点} = \min\left\{70, \frac{7}{10}\left(\text{試験（100 点満点）} + \text{レポート（ひとつ 5 点満点）}\right)\right\}$$

レポート問題は冒頭に概略を完結に述べ（1 ページ以内）, 詳細はそれに続けて記述すること．練習のために概略を授業で簡潔に発表する時間も取れます．

1.2 参考文献

いろいろある．各自で自分にあった本を探すのが好ましい．以下は参考．

- 整数と郡・環・体（河田直樹）
- 環と体の理論（酒井文雄）
- 代数入門（掘田良之）
- 代数学入門（石田信）
- 代数演習（横井英夫/硲野敏博）
- 数学する身体（森田真生）
- 授業資料
  `http://http://www.is.c.titech.ac.jp/~sakie/sakietech/`

1.3 授業の概要

概要：目次で説明．（♣）は抽象代数学, （♢）は巡回群 $\mathbb{Z}_n$ を用いた具体例やウィルソンの定理にまつわる話．

1.4 授業の目標

- 素数に親しむ
- 「ウィルソンの定理」を理解する

- 巡回群 $\mathbb{Z}_m$ を「群」「環」「体」の 3 つの枠組みで理解する
- 群、環、体の枠組みの必然性や、どう自然な概念なのかを理解する
  - 群：対称性を記述する道具
  - 環：?（群の拡張だから何らかの対称性を記述するけど）
  - 体：?（いろんな視点で存在意義を言葉にできたら良い）
- ガロア理論の概観（なぜ 5 次方程式は解の公式がないのか）

このあたり授業を進めながら一緒に考える。レポートにするかも。

歴史を知るのも楽しい。

1.5　学びの進め方

ICE モデルに沿って行う（後々やりながら説明していく）.

- Ideas (基礎的知識を学習する)
- Connections (学びを繋げる)
- Extensions (広げて応用していく)

出来てしまうと意識しないことが多いと思うけど、なんとなく学ぶのではなく、それぞれの学びの段階を意識する。それを OUTPUT する。共有する。フィードバックする。

I（アイデア）のみの講義は，頑張って知識を得ても，後から振り返ると結局何だったんだろう？となりやすい．いろいろな学びにつなげて発展させていけると良い（結構頭使う）.

1.6　授業の進め方

(1) 復習 （〜15min）
(2) 資料を使ってスライドで説明する（30〜40min）
(3) 演習問題（グループワーク）（20〜30min）
(4) フィードバック（〜15min）← 配ったプリントで説明

前の大学ではみんなで散歩に行ってました。

1.7　授業の進め方の意義

- 「講義 vs ノートを取る」という構図は（私が）辛い
- グループワークで他人や自分と対話する機会を作りたい
- せっかく人が集まるんだから干渉しやすい場にしたい (無理に干渉しなくても良い)
- 代数の応用（特に情報系で）を知りたい

慣れたやり方から一回脱出してみる。→ 新たな発見があるかも。

クリエイティブな場所になるといいです。

1.8　チェックイン（グループワーク）とちょっと本論

自己紹介．この授業に期待すること.

他の科目との関係性とかも踏まえて。

1.9　フィードバック

今日したこと．感じたこと．発想.

第 2 章

整数の基本的性質

2.1 数の起こり

Henri Poincaré：水源は不明でもやはり川は流れている

河田 p4

2.2 数

あとでそれぞれを群、環、体の枠組みで捉えなおす予定。

- 自然数 $\mathbb{N} = \{1, 2, 3, \ldots\}$　（加と乗の構造）
- 整数 $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$　（加減と乗の構造）
- 正の有理数 $\mathbb{Q}_{\geq 0} = \{0, \frac{a}{b} \mid a, b \in \mathbb{N}\}$　（加と乗余の構造）
- 有理数 $\mathbb{Q} = \{0, \pm\frac{a}{b} \mid a, b \in \mathbb{N}\}$　（加減乗余の構造）
- 無理数 $\mathbb{R} \setminus \mathbb{Q}$
- 実数 $\mathbb{R} = (\mathbb{R} \setminus \mathbb{Q}) \cup \mathbb{Q}$　（加減乗余の構造）
- 複素数 $\mathbb{C}$　（加減乗余の構造）

上で自然数，整数，有理数の定義はできているが，実数と無理数は定義にはなっていない．無理数が定義できれば実数は有理数と無理数の和集合として定義できる．これは解析学のはじまりで，結構面白い．

2.3 最大公約数

ここからはしばらく整数 $\mathbb{Z}$ に注目する．

定義 2.3.1. $m, n \in \mathbb{Z} \setminus \{0\}$ を 0 でない整数とする．

- m は n を割り切る（n は m で割り切れる）とき，$m|n$ と表す．
- m と n を同時に割り切る自然数を**最大公約数**という．
- m と n を同時に割り切る最大の自然数を**最大公約数**といい，(m, n) とかく．
- m と n で同時に割り切れる自然数を**公倍数**という．
- m と n で同時に割り切れる最小の自然数を**最小公倍数**という．これは $\frac{mn}{(m,n)}$ である．
- $(m, n) = 1$ のとき，m と n は**互いに素**という．

定理 2.3.2. $m, n, q, r \in \mathbb{Z} \setminus \{0\}$ に対して

$$m = nq + r$$

が成り立つとする．このとき n と m の公約数は n と r の公約数である．また，逆も成り立つ．とくに $(m, n) = (n, r)$.

Proof. d を n と m の公約数とすると，$r = m - nq$ も d で割り切れる．よって d は n と r の公約数でもある．逆に d' を n と r の公約数とすると，$m = nq + r$ も d で割り切れる．よって d' は n と m の公約数でもある． □

2.4 ユークリッドの互除法

ユークリッドの互除法とは，定理 2.3.2 を応用した，2 つの整数の最大公約数を求めるアルゴリズムである．ユークリッドが「原論」に記した，明示的に記述された最古のアルゴリズムと言われている．

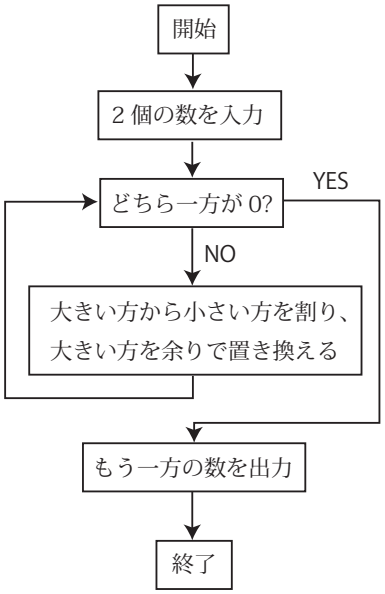
例えば 6188 と 4709 の最大公約数を求めたいとする．

1. 6188 を 4709 で割る
$$6188 = 4709 \times 1 + 1479$$
2. 4709 を 1479 で割る
$$4709 = 1479 \times 3 + 272$$
3. 1479 を 272 で割る
$$1479 = 272 \times 5 + 119$$
4. 272 を 119 で割る
$$272 = 119 \times 2 + 34$$
5. 119 を 34 で割る
$$119 = 34 \times 3 + 17$$
6. 34 を 17 で割る
$$34 = 17 \times 2 + 0$$

割り切れるところまで続ける．最後に割った数 17 が答え．つまり，

$$(6188, 4709) = (4709, 1479) = (1479, 272) = (272, 119) = (119, 34) = (34, 17) = 17.$$

アルゴリズムとしては以下のチャート．



ポイント：数が大きくなるほど，素因数分解などで最大公約数を求めるよりも効率的．

定義 2.4.1 (ランダウの記号)．$f(n) = \mathcal{O}(g(n)) \iff$ ある n_0, C が存在して $n > n_0$ なら $|f(n)| \leq C|g(n)|$．
だいたいの意味：$f(n)$ の発散のスピードは早くても $g(n)$ くらい．

定理 2.4.2. m, n, $m > n$ の最大公約数を求めるユークリッドの互除法の計算ステップ回数は $\mathcal{O}(\log_2 m)$（多項式時間）．

考察. $m, n \in \mathbb{Z}$, $m > n$, に対して $m = qn + r$ とする（$q \geq 1$, $0 \leq r < n$）．このとき $2r \leq n + r \leq m$ となるから $r \leq m/2$．よってユークリッドの互除法のステップを 2 回繰り返して $(m, n) = (n, r_1) = (r_1, r_2)$ となったとき，m, n は半分以下になる。つまりステップ回数が s 回とすると，

$$(m, n) = (n, r_1) = (r_1, r_2) = (r_2', r_3) \cdots = (r_{s-1}', r_s), \quad r_s \sim 1 \leq m/2^{\frac{s}{2}}.$$

ただし $r_i' = \min\{r_{i-1}, r_i\}$, r_{i+1} は $\max\{r_{i-1}, r_i\}$ を r_i' で割った余り．$\sim$ はだいたい．よって $\frac{s}{2} \sim \log_2 m$ となり，ステップ回数は $s = 2\log_2 m$ で抑えられる． □

一方，素因数分解を使って 1 から m まで順に試し割りをするという安直なアルゴリズムでは，ステップ数は $\mathcal{O}(m)$ になる（指数時間）．

練習 1. (m, n) のユークリッドの互除法の計算ステップ s に対して，s/m が最長になる m, n のペアはどんなものだろう．

答. フィボナッチ数 a_n の隣接二項 $(m = a_{i+1}, n = a_i)$．すなわち $a_{i+2} = a_{i+1} + a_i$, $a_0 = 0$, $a_1 = 1$.

つまりフィボナッチ数列と m, n を比較するとユークリッドの互除法の回数が上から抑えられる．

2.5　一次不定方程式（拡張ユークリッドの互除法）

拡張ユークリッドの互除法とは，ユークリッドの互除法を応用して一次不定方程式 $ax+by=c$ の解 x,y を求めるためのアルゴリズムである．

定理 2.5.1 (一次不定方程式の解の存在)．$a,b\in\mathbb{Z}\setminus\{0\}$ とする．このとき，一次不定方程式 $ax+by=c$ が解を持つための必要十分条件は $(a,b)|c$ となることである．

Proof. 4.6 章で示す． □

系 2.5.2. $a,b\in\mathbb{Z}\setminus\{0\}$ とする．このとき，一次不定方程式 $ax+by=(a,b)$ は解を持つ．

系 2.5.3. $a,b\in\mathbb{Z}\setminus\{0\}$ とする．$(a,b)=1$ のとき，一次不定方程式 $ax+by=1$ は解を持つ．

【ステップ 1】一次不定方程式 $ax+by=(a,b)$ の解をひとつ求める．

$6188x+4709y=17$ という一次不定方程式を考えよう．ユークリッドの互除法

$$\begin{aligned}6188&=4709\times1+1479,\\4709&=1479\times3+272,\\1479&=272\times5+119,\\272&=119\times2+34,\\119&=34\times3+17,\\34&=17\times2+0.\end{aligned}$$

を，最後から二番目の行から逆に辿って，

$$\begin{aligned}17&=119-34\times3\\&=119-(272-119\times2)\times3\\&=119\times7-272\times3\\&=(1479-272\times5)\times7-272\times3\\&=1479\times7-272\times38\\&=1479\times7-(4709-1479\times3)\times38\\&=1479\times121-4709\times38\\&=(6188-4709\times1)\times121-4709\times38\\&=6188\times121-4709\times159.\end{aligned}$$

よって $x=121,y=-159$ は解．

【ステップ 2】一次不定方程式 $ax+by=d(a,b)$ の解をすべて求める．

$6188x+4709y=17d$ という一次不定方程式を考えよう．ステップ 1. より，

$$6188\times121-4709\times159=17.$$

$6188x+4709y=17d$ から上の式の d 倍を引くと

$$6188(x-121d)+4709(y+159d)=0$$

両辺を 17 で割って

$$364(x-121d)+277(y+159d)=0.$$

（両辺を 6188 と 4709 の最大公約数で割った.）このとき $x-121d=277w$ とおくと，$364w+y+159d=0$ より $y=-159d-364w$. 従って一般解は

$$\begin{cases} x=121d+277w, & (277=4709/17) \\ y=-159d-364w, & (364=6188/17) \end{cases}$$

$w\in\mathbb{Z}$.

【特に $(a,b)=1$ の場合（後で素数を調べるときに重要)】

$22x+115y=1$ という一次不定方程式の解を求めよう．ステップ 1 に沿って解をひとつ求めると，

$$\begin{aligned} 115&=22\times5+5,\\ 22&=5\times4+2,\\ 5&=2\times2+1. \end{aligned}$$

の逆を辿って

$$\begin{aligned} 1&=5-2\times2\\ &=5-(22-5\times4)\times2\\ &=5\times9-22\times2\\ &=(115-22\times5)\times9-22\times2\\ &=115\times9-22\times47. \end{aligned}$$

よって $x=-47$, $y=9$ がひとつの解.

ステップ 2（$d=1$）に従って

$$22(x+47)+115(y-9)=0.$$

の解を求めると

$(22,115)=1$ より最大公約数で割るフェーズがない.

$$\begin{cases} x=-47+115w, \\ y=9-22w, \end{cases}$$

$w\in\mathbb{Z}$.

練習 2. 適当に好きな自然数のペア m,n を取ってきて以下の問いに答えよ.

(1) 最大公約数を求めよ.
(2) 最大公倍数を求めよ.
(3) 一次不定方程式 $mx+ny=(a,b)$ の解をひとつ求めよ.
(4) 一次不定方程式 $mx+ny=d(a,b)$ の一般解を求めよ.

演習 1. ユークリッドの互除法や拡張ユークリッドの互除法は，情報系のどこで使われる？どんな研究分野と繋がっている？

第 3 章

素数を拾う

3.1　素数と素因数分解

（第三回・12/9）（第四回・12/12）

定義 3.1.1 (素数)**.** 1 とその数の他に約数を持たない 2 以上の自然数を**素数**という．素数でない 2 以上の自然数を**合成数**という．

定理 3.1.2 (素因数分解の一意性)**.** 2 以上の自然数は素数の積として順序を除いて一意的に表せる．

3.2　エラトステネスの篩

エラトステネスって誰？

素数を下から列挙する方法．

1. 1 を除いた自然数から 2 を拾う．
2. 残った自然数から 2 の倍数を除く．
3. 残った数の中で一番小さい数，すなわち 3 を拾う．
4. 残った数から 3 の倍数を除く．
5. 残った数の中で一番小さい数，すなわち 5 を拾う．
6. 残った数から 5 の倍数を除く．
7. 残った数の中で一番小さい数，すなわち 7 を拾う．
8. 残った数から 7 の倍数を除く．
9. ...

3.3　素数を判定する

定理 3.3.1. 自然数 n が素数 $\iff$ $\sqrt{n}$ を超えないすべての素数で割り切れない．

（絵を描いて考えてみる．）

3.4　素数の「個数」

p を任意の素数とし，$p^!$ を p 以下の素数の積とする．

このあたり空で語れると楽しそう．

定理 3.4.1. 素数は無限個ある．

Proof.（背理法）素数が有限個であるとし，小さい方から $p_1, \ldots, p_n$ と名付ける．このとき $P = p_n^! + 1$ という正の整数を考える．場合分けで矛盾を示す．

1. P が素数だとすると，仮定から $1 \leq i \leq n$ が存在して $P = p_i$．これは $P > p_i$ に矛盾．
2. P が合成数だとすると，P は $p_1, \ldots, p_n$ のいずれかで割り切れる．これは $\frac{P}{p_i} = p_1 p_2 \cdots p_{i-1} p_{i+1} \cdots p_n + \frac{1}{p_i}$ に矛盾．

従って仮定が偽であり素数は無限個である． □

問 1；これはパッと見上の定理と矛盾しそうだけど，p_n より大きくて $p^! + 1$ より小さい素数が存在する場合があるというところがポイント．

問 1. p が素数のとき $p^! + 1$ は素数か？

答 (No!)．$p = 13$ のとき $p^! + 1 = 59 \times 509$.

問 2 (未解決問題)．$p^! + 1$ が素数になるような素数 p は有限個か？（現在見つかっている素数は 22 個...）

3.5　素数を捕まえる

定理 3.5.1 (ディリクレの素数定理)．a と d が互いに素であるとき $a + kd$ $(k \in \mathbb{N})$ という形の素数が無限個存在する。

定理 3.5.2 (ベルトラン–チェビシェフの定理)．任意の n と $2n$ の間に必ず素数が存在する。

問 3.　(1) ディリクレの素数定理やベルトラン–チェビシェフの定理の証明（部分的でも良い）を調べてみよう．

(2) ディリクレ, ベルトラン, チェビシェフはどの時代にどんな研究をした人たちか調べてみよう（プチ伝記作り）．

第 4 章

ウィルソンの定理と合同式

ここからは 2 つのストーリーを並行して進めていく（テレビドラマとかでよくある手法）．1 つは抽象代数学（♣）、もうひとつは具体例やウィルソンの定理にまつわる話（♢）．

4.1 ウィルソンの定理（♢）

ウィルソンの定理は素数を判定するための強力な定理である．そのしくみを理解することで素数に対する理解を深める．そのために群・環・体の枠組みが役に立つ．

2 以上の自然数 n に対して $E(n) = (n-1)! + 1$ と置く．

天下り的に

定義 4.1.1 (ウィルソン数)．$E(n)$ を n で割った余りを $W(n)$ と書き，**ウィルソン数**と呼ぶ．

n	$E(n)$	$W(n)$
2	2	0
3	3	0
4	7	3
5	25	0
6	121	1
7	721	0
8	5041	1
9	40321	1
10	362881	1

n	$E(n)$	$W(n)$
11	3628801	0
12	39916801	1
13	479001601	0
14	6227020801	1
15	87178291201	1
16	1307674368001	1
17	20922789888001	0
18	355687428096001	1
19	6402373705728001	0

表 4.1　ユークリッド数とウィルソン数

定理 4.1.2 (ウィルソンの定理)．2 以上の自然数 n に対して

$$n \text{ が素数} \iff W(n) = 0.$$

ウィルソン数のような「割った余り」を考えるときには次の章の合同式の枠組みが便利．

4.2　合同式（♣）

定義 4.2.1. a, b を整数，m を自然数とする．$a-b$ が m で割り切れるとき，a **と** b **は** m **を法として合同**という．またこのとき

$$a \equiv b \pmod{m}$$

と表し，このような関係式を**合同式**と呼ぶ．

例.

$$2 \equiv 4 \equiv 6 \pmod{2}$$
$$2 \equiv 5 \equiv 8 \pmod{3}$$

練習 3. 次の主張を合同式を使って表せ．

(1) x は偶数である．
(2) x は 3 で割ると 1 余る整数である．
(3)（ウィルソンの定理）自然数 n が素数であるための必要十分条件は，2 以上の自然数 n に対して $(n-1)!+1$ が n で割り切れることである．

定理 4.2.2. a, b, c を整数, m を自然数とする．

(1) $a \equiv a \pmod{m}$,
(2) $a \equiv b \pmod{m}$ ならば $b \equiv a \pmod{m}$.
(3) $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$ ならば $a \equiv c \pmod{m}$.

（すなわち，関係 $\equiv$ は**同値関係**である．次章参照.）

定理 4.2.3. a, a', b, b' を整数, m を自然数とする．$a \equiv a' \pmod{m}$, $b \equiv b' \pmod{m}$ のとき次が成り立つ．

(1) $a \pm b \equiv a' \pm b' \pmod{m}$,
(2) $ab \equiv a'b' \pmod{m}$.

練習 4.　(1) 合同数を使って見たエラトステネスの篩
(2) 合同数を使って見たウィルソンの定理：2 以上の自然数 n に対して, n が素数 $\iff$ $E(n) \equiv 0 \pmod{n}$

4.3　同値関係と商集合（♣）

上の合同式の話を一般化する．

例えば三角形の全体は「合同」という基準で分類できる．この背景には、「形」が見たいから、どこに置いてあっても同じ、という考えがある。つまり、「形」という見たいものを残して「置き場所」という情報を捨てる。現代数学でも、トポロジー（位相幾何学)、微分幾何学、複素幾何学、などは、多様体（図形）に入れる同値関係の違いで分野が分かれている。「見たいもの」によって、どの情報を捨てる（捨てた後で同じものを「同値」と

する）かが決まる。同値関係と商集合の概念は、それを考える理論的枠組みを提供してくれる。

A を集合とする．$a, b \in A$ がある基準で「関係している」とき，$a \sim b$ と書く。この「基準」をひとつ定めることは、$A \times A$ の部分集合 R をひとつ指定することと同じ操作である．すなわち

$$a \sim b \iff (a, b) \in R$$

とすればよい．

定義 4.3.1. $A \times A$ の部分集合 R を A における**関係**と呼ぶ．

$a, b \in A$ がある基準で「関係している」よりも強く、「同じである」ということを以下で定める．

定義 4.3.2 (同値関係)**.** 次を満たす関係 $\sim$ を**同値関係**という．

(1) $a \sim a$,
(2) $a \sim b$ ならば $b \sim a$.
(3) $a \sim b$, $b \sim c$ ならば $a \sim c$.

集合 A に同値関係 $\sim$ が与えられると、それによって A の元を分類することができる。すなわち、

$$R(a) = \{b \in A \mid a \sim b\}$$

とおけば、

(1) $a \in R(a)$
(2) $a \sim b \iff R(a) = R(b)$
(3) $a \not\sim b \iff R(a) \cap R(b) = \emptyset$

が成り立つ。

定義 4.3.3. $R(a)$ を a が属する**同値類**と呼び，その任意の元を同値類の**代表元**と呼ぶ．$R(a)$ の代表元 c をひとつとり，$\bar{c} = R(a)$ と書くこともある．

つまり、A はどの二つも互いに交わらない同値類の和集合として表わされる．[*1]すなわち

$$A = \sqcup \text{同値類}$$

となる。

例. (1) 同値関係 $\equiv \pmod 2$ で $\mathbb{N}$ を分類すると

$$\mathbb{N} = \{1, 3, 5, \ldots\} \sqcup \{2, 4, 6, \ldots\}.$$

(2) 同値関係 $\equiv \pmod 3$ で $\mathbb{N}$ を分類すると

$$\mathbb{N} = \{1, 4, 7, \ldots\} \sqcup \{2, 5, 8, \ldots\} \sqcup \{3, 6, 9, \ldots\}.$$

[*1] 二つの互いに交わらない部分集合の和集合のことを**直和**と呼び $\sqcup$ で表す．

練習 5.　(1) 同値関係 $\equiv \pmod 2$ で $\mathbb{N}$ を分類したとき、各同値類からひとつづつ代表元を取れ.

(2) 同値関係 $\equiv \pmod 2$ で $\mathbb{N}$ を分類したとき、ある同値類の 2 つの代表元はどんな関係にあるか答えよ.

定義 4.3.4 (商集合). 集合 A に同値関係 $\sim$ が与えられたとき、同値類全体のなす集合

$$A/\sim = \{R(a); a \in A\}$$

を A の $\sim$ による**商集合**という.

例.　(1) 同値関係 $\equiv \pmod 2$ で $\mathbb{N}$ を分類したとき、

$$\begin{aligned}\mathbb{N}/(\equiv \pmod 2) &= \{\{1,3,5,\ldots\},\{2,4,6,\ldots\}\}\\ &= \{\bar{1},\bar{2}\}\end{aligned}$$

(2) 同値関係 $\equiv \pmod 3$ で $\mathbb{N}$ を分類したとき、

$$\begin{aligned}\mathbb{N}/(\equiv \pmod 3) &= \{\{1,4,7,\ldots\},\{2,5,8,\ldots\},\{3,6,9,\ldots\}\}\\ &= \{\bar{1},\bar{2},\bar{3}\}\end{aligned}$$

定義 4.3.5. 集合 A に同値関係 $\sim$ が与えられたとき、A からの写像 $f\colon A \to G$ は $a \sim b \Rightarrow f(a) = f(b)$ のとき写像 $\bar{f}\colon A/\sim \to G$ を誘導する. このとき、写像 f は $A/\sim$ の上で**矛盾なく定義されている**（well-defined）という.

4.4　商集合 $\mathbb{Z}_m$（♢）

定義 4.4.1 ($\mathbb{Z}_m$). m を 2 以上の自然数とする. $\mathbb{Z}$ の同値関係 $\equiv \pmod m$ による商集合を $\mathbb{Z}_m$ と表す.（これは位数 m の巡回群と呼ばれるものになる. *5* 章参照.）

well-defined にならない写像の例は？

定理 7 より，$\mathbb{Z}$ の和と積は $\mathbb{Z}_m$ の上で well-defined.

練習 6. 表 *1* を埋めよ.（$m = 2,3,4,5,6$）

定理 4.4.2. p を素数とする. このとき，任意の $a \in \mathbb{Z}_p \setminus \{0\}$ は逆元をもつ. すなわち

$$ax \equiv 1 \pmod p$$

となる $x \in \mathbb{Z}_p$ が唯一つ存在する.

Proof.（記号を乱用し）$a \in \{1,2,\ldots,p-1\}$ とし, $i = 1,\ldots,p-1$ に対して $q_i > 0$, $r_i \in \{1,2,\ldots,p-1\}$ を

$$ai = pq_i + r_i,$$

と定める.

主張： $i \neq j$ ならば $r_i \neq r_j$, すなわち

$$\{r_1,\ldots,r_{p-1}\} = \{1,2,\ldots,p-1\}.$$

この主張の証明大事！後から同じアイデアを使う.

まず主張を示す．背理法により，$r_i = r_j$ とすると

$$ai - aj = pq_i - pq_j \equiv 0 \pmod{p} \Rightarrow a(i-j) \equiv 0 \pmod{p}$$

となり，$1 \leq i - j \leq p - 2$ より，これは $(a, p) = 1$（p は素数より）であることに矛盾．従って $i \neq j$ ならば $r_i \neq r_j$ が従う．したがって主張が示された．

これより $r_i = 1$ となる i が唯一つ存在し，

$$ai = pq_i + 1 \Rightarrow ai \equiv 1 \pmod{p}.$$

よって定理が示された．□

演習 2. 上の証明を資料を見ないで再構成できるようになろう．

定理 4.4.3 (フェルマーの小定理)．p を素数とする．任意の $a \in \mathbb{Z}_p \setminus \{0\}$ に対し

$$a^{p-1} \equiv 1 \pmod{p}$$

が成り立つ．

Proof. 定理 4.4.2 の証明と同様に，$a, 2a, 3a, \ldots, (p-1)a$ は p を法として互いに異なる．それらをすべて掛け合わせると

$$1 \cdot 2 \cdots (p-1) \equiv 1 \cdot 2 \cdots (p-1)a^{p-1} \pmod{p}.$$

$1 \cdot 2 \cdots (p-1)$ の逆元を両辺にかけると $a^{p-1} \equiv 1 \pmod{p}$ が従う．□

練習 7. フェルマーの小定理の対偶を述べよ．

4.5　フェルマーテストとカーマイケル数（♢）

命題 4.5.1 (フェルマーの小定理の対偶)．n を自然数とする．ある整数 a が存在して

$$\text{（条件 A）} (a, n) = 1 \text{ かつ } a^{n-1} \not\equiv 1 \pmod{n}$$

となるとき，n は素数ではない．

n を自然数としたとき，上の（条件 A）が成り立つか否かをチェックすることを，n の a を底とした**フェルマーテスト**という．（条件 A）が成り立たないとき n は「素数である可能性を残している」という意味において a を底とした「**フェルマーテストをパスする**」という．

定義 4.5.2.（条件 A）を満たすすべての整数 a に対してフェルマーテストにパスするのにもかかわらず素数でないような n を**カーマイケル数**と呼ぶ．

定理 4.5.3.
- 1 から 100 万までのカーマイケル数は 43 個$(561, 1105, 1729, 2465, \ldots)$.
- カーマイケル数は無限個（*Alford, Granville, Pomerance, 1994.*）
- n がカーマイケル数であることの必要十分条件は以下の 2 つの条件を満たすことである．
  1. n を割り切る任意の素数 p に対して $p - 1 | n - 1$.
  2. n は平方因子を持たない．
- カーマイケル数は、少なくとも 3 個以上の異なる素数の積である．

4.6　一次不定方程式の証明（♣）

定理（再掲） (定理 2.5.1)．$a, b \in \mathbb{Z} \setminus \{0\}$ とする．このとき，一次不定方程式 $ax + by = c$ が解を持つための必要十分条件は $(a, b)|c$ となることである．

Proof. まず $c = 1$ とする．
(⇒) $(a, b) = d \neq 1$ とすると，$ax + by$ は d で割り切れるはずだから $ax + by = 1$ は解を持たない．よって $(a, b) = 1$.
(⇐) 定理 4.4.2 の証明とほぼ同様（p を b とする．）
　次に $c \neq 1$ とする．
(⇒) $(a, b) \not| c$ とすると，$ax + by$ は (a, b) で割り切れるはずだから $ax + by = c$ は解を持たない．よって $(a, b)|c$.
(⇐) $a = p(a, b)$, $b = q(a, b)$ とおく．ここで $(p, q) = 1$ とする．$px + qy = 1$ は整数解を持つので，両辺を (a, b) 倍して，$ax + by = (a, b)$ も同じ整数解を持つ．$c = d(a, b)$ とすると $axd + byd = c$ となるので，$px + qy = 1$ の解をそれぞれ d 倍した整数が解になる．
□

4.7　ウィルソンの定理の証明（♢）

（復習）$W(n)$：$E(n) = (n - 1)! + 1$ を n で割った余り．

定理（再掲） (定理 4.1.2; ウィルソンの定理)．2 以上の自然数 n に対して

$$n \text{ が素数} \iff W(n) = 0.$$

Proof.（⇒ の証明）$n = 2, 3$ のとき $W(2) = W(3) = 0$. p を 5 以上の素数とする．定理 4.4.2 より任意の $a \in \mathbb{Z} \setminus \{0\}$ は逆元を持つ．1 と $p - 1$（のみ）がそれ自身を逆元にもつことに注意すると，

$$1 \cdot 1 \equiv 1 \tag{4.1}$$
$$2 \cdot i_2 \equiv 1 \tag{4.2}$$
$$\vdots$$
$$(p-2) \cdot i_{p-2} \equiv 1 \tag{p-2}$$
$$(p-1)(p-1) \equiv 1 \tag{p-1}$$

ただし $\{i_2, \ldots, i_{p-2}\} = \{2, \ldots, p - 2\}$.

> **主張**：合同式 (2)$\cdots$(p-2) から，積をとった結果が $(p - 2)!$ になるよう $\frac{p-3}{2}$ 個の合同式をとれる．

主張にある $\frac{p-3}{2}$ 個の合同式と合同式 (p-1) をかけると

$$(p - 1)! \cdot (p - 1) \equiv 1 \pmod{p}.$$

この両辺に $(p-1)$ をかけると

$$(p-1)! \equiv p-1 \equiv -1 \pmod{p}.$$

（⇐ の証明）$W(n)=0$ とする．背理法で n が素数であることを示す．n を合成数とすると，$1<d<n$ かつ $d|n$ となる d が存在する．このとき $d|(n-1)!$ より $d \nmid ((n-1)!+1)$. すなわち $n \nmid ((n-1)!+1)$. これは $W(n)=0$ に反するため n は素数.

□

演習 3. 上の主張を示せ.

問 4. ウィルソンの定理にまつわる歴史を調べてみよう.

第 5 章

群という見方

（第五回・12/16）（第六回・12/19）（第七回：中間試験もしくは休講・12/23）

逆元の存在がポイント.

5.1 半群、モノイド、群（♣）

集合 A とその上の二項演算 $\_\cdot\_\colon A\times A\to A$ が与えられているとする.

- 任意の $a,b,c\in A$ に対して以下が成り立つとき二項演算 $\cdot$ は**結合法則**を満たすという.

$$(a\cdot b)\cdot c=a\cdot(b\cdot c)$$

- 任意の $a\in A$ に対して以下を満たす $e\in A$ を**単位元**と呼ぶ.

$$e\cdot a=a=a\cdot e$$

- $a\in A$ に対して以下を満たす $a'\in A$ を a の**逆元**と呼ぶ. 逆元を持つ A の元を**単元**という.

$$a\cdot a'=e=a'\cdot a$$

定義 5.1.1 (半群、モノイド、群). 集合 A とその上の二項演算 $\_\cdot\_\colon A\times A\to A$ の組 $(A,\cdot)$ を考える.

- $(A,\cdot)$ は (1) 結合法則を満たすとき**半群**と呼ばれる.
- $(A,\cdot)$ は (1) 結合法則を満たし (2) 単位元を持つとき**モノイド**と呼ばれる.
- $(A,\cdot)$ は (1) 結合法則を満たし (2) 単位元を持ち (3) 任意の元に逆元が存在するとき**群**と呼ばれる.

例.

- 自然数 $\mathbb{N}=\{1,2,3,\dots\}$ （加と乗の構造）
  $\Rightarrow$ $(\mathbb{N},$加$)$: 半群、$(\mathbb{N},$乗$)$: モノイド
- 整数 $\mathbb{Z}=\{0,\pm1,\pm2,\pm3,\dots\}$ （加減と乗の構造）
  $\Rightarrow$ $(\mathbb{Z},$加$)$: 群、$(\mathbb{Z}\setminus\{0\},$乗$)$: モノイド
- 正の有理数 $\mathbb{Q}_{\geq 0}=\{0,\frac{a}{b}\mid a,b\in\mathbb{N}\}$ （加と乗余の構造）
  $\Rightarrow$ $(\mathbb{Q}_{\geq 0},$加$)$: 半群、$(\mathbb{Q}_{\geq 0}\setminus\{0\},$乗$)$: 群

– 有理数 $\mathbb{Q} = \{0, \pm\frac{a}{b} \mid a, b \in \mathbb{N}\}$　（加減乗余の構造）
⇒ $(\mathbb{Q}, 加)$: 群、$(\mathbb{Q} \setminus \{0\}, 乗)$: 群

練習 8.　(1) $(\mathbb{N}, +)$ と $(\mathbb{N}, \times)$ はどちらも群にならないことを示せ.
(2) $(\mathbb{Z}, +)$ は群になり，$(\mathbb{Z} \setminus \{0\}, \times)$ は群にならないことを示せ.
(3) $(\mathbb{Q}_{\geq 0}, +)$ は群にならず，$(\mathbb{Q}_{\geq 0} \setminus \{0\}, \times)$ は群になることを示せ.
(4) $(\mathbb{Q}, +)$ と $(\mathbb{Q} \setminus \{0\}, \times)$ はどちらも群になることを示せ.

5.2　群の生成元（♣）

定義 5.2.1. G を群とする.

– G の元の個数を G の**位数**といい，$|G|$ で表す.
– G の演算について群になる部分集合 $H \subset G$ を G の**部分群**という.（部分集合 $H \subset G$ は，任意の $a, b \in H$ に対して $a \cdot b \in H$ かつ $a^{-1} \in H$ が成り立つとき**部分群**という.）
– G の任意の元が G の部分集合 S の元の積と逆元を有限回とることで得られるとき，群 G は部分集合 S で**生成される**という．このとき，S を G の**生成元集合**と呼び，S の元を G の**生成元**という．生成元 $s_1, \ldots, s_r$ が有限個のとき，$G = \langle s_1, \ldots, s_r \rangle$ と書く.

「引き算で閉じるように $\mathbb{N}$ から $\mathbb{Z}$ をつくる」などの操作の数学的定式化.

練習 9.　(1) 群 $(\mathbb{Q}, +)$ の中で次の部分集合により生成される群を示せ.
(i) $\mathbb{N}$
(ii) $\mathbb{Q}_{\geq 0}$
(2) 群 $(\mathbb{Q} \setminus \{0\}, \times)$ の中で次の部分集合により生成される群を示せ.
(i) $\mathbb{N}$
(ii) $\mathbb{Z} \setminus \{0\}$
(3) 次の群の（それ自身でない）生成元集合をひとつ求めよ.
(i) $(\mathbb{Q}, +)$
(ii) $(\mathbb{Q}_{\geq 0} \setminus \{0\}, \times)$
(iii) $(\mathbb{Q} \setminus \{0\}, \times)$

定義 5.2.2. G を群とする.

– G は要素が有限個のとき**有限群**と呼ばれる.
– G は一つの元で生成されるとき**巡回群**と呼ばれる.
（$\iff$ ある $a \in G$ が存在し $G = \langle a \rangle$ となるとき）.
– G は有限集合で生成されるとき**有限生成**であるという.
（$\iff$ ある $a_1, \ldots, a_m \in G$ が存在し $G = \langle a_1, \ldots, a_m \rangle$ となるとき）.
– $a \in G$ で生成される巡回群の位数 $|\langle a \rangle|$ を a の**位数**という.
（位数は $a^n = e$ となる最小の n と一致する.）

練習 10. $(\mathbb{Z}, +)$ が巡回群であることを示せ.

5.3 $\mathbb{Z}_m$ の場合（♢）

練習 11. (1) $(\mathbb{Z}_m, +)$ が有限群かつ巡回群であることを示せ.
(2) p を素数とすると, $(\mathbb{Z}_p \setminus \{0\}, \times)$ が群になることを示せ.
ヒント：フェルマーの小定理（定理 *4.4.3*）
(3) $\bar{a} \in (\mathbb{Z}_m \setminus \{0\}, \times)$ が単元であることの必要十分条件は $(a, m) = 1$ であることを示せ.
ヒント：一次不定方程式（定理 *2.5.1*）

定理 5.3.1. 自然数 m が素数 $\iff$ $(\mathbb{Z}_m \setminus \{0\}, \times)$ が群

練習 12. 定理 *5.3.1* とウィルソンの定理との関係は？つまり自然数 m に対して
$W(m) = 0 \iff (\mathbb{Z}_m \setminus \{0\}, \times)$ が群
を直接証明してみよう.

定義 5.3.2.
- $\bar{a} \in \mathbb{Z}_m$ は $(a, m) = 1$ であるとき**既約剰余類**と呼ばれる.
- $\mathbb{Z}_m$ の既約剰余類（すなわち単元；練習 *11(3)*）を集めた集合を

$$(\mathbb{Z}_m)^\times = \{\bar{a} \in \mathbb{Z}_m \mid (a, m) = 1\}$$

と置き，$((\mathbb{Z}_m)^\times, \times)$ を $\mathbb{Z}_m$ の**既約剰余類群**と呼ぶ.

練習 13. (1) 表 *1* において $(\mathbb{Z}_m)^\times$ の行と列をマークせよ.

命題 5.3.3. p が素数のとき,

(1) $(\mathbb{Z}_p)^\times = \mathbb{Z}_p \setminus \{0\}$.
(2) $(\mathbb{Z}_p)^\times = \{a^k \mid k = 1, \ldots, p-1\}$ となる a が存在する.（すなわち $(\mathbb{Z}_p)^\times$ は巡回群.）

Proof. (1) 省略. (2) $\bar{a} \in (\mathbb{Z}_p)^\times$ で位数が $p-1$ のものがとれる $\to$ 7 章. □

演習 4. (1) $((\mathbb{Z}_4)^\times, \times)$ が $\bar{3}$ で生成されることを示せ.
(2) $((\mathbb{Z}_{11})^\times, \times)$ の巡回群としての生成元をすべて求めよ.

5.4 群の左剰余類，正規部分群と剰余群（♣）

定義 5.4.1 (左剰余類). G を群とする.

- G の部分群 H が与えられたとき，G の元の同値関係 $a \sim b$ を関係 $a^{-1}b \in H$ で定義する．この同値関係による同値類を G の H による**左剰余類**という.
- 左剰余類の集合を G/H で表す.
- G/H の元の個数を G における H の**指数**とよび $[G : H]$ で表す.

練習 14. G を群，H をその部分群とする.

(1) $a \sim b$ が同値関係であることを示せ．
酒井 p9
(2) G の元 a の H による左剰余類 $\bar{a}$ は $aH = \{a\eta \mid \eta \in H\}$ に一致することを示せ．

定理 5.4.2 (ラグランジュ（Lagrange）の定理)**.** G を有限群とし，H をその部分群とする．このとき H の位数は G の位数の約数であり，$[G : H] = |G|/|H|$ が成立する．

Proof. 上の同値関係において，$\sigma \in G$ に同値な元（同じ左剰余類に属する元）は一意的に $\sigma\eta, \eta \in H$ と表される．よって，同じ左剰余類に属する元は $|H|$ 個である．従って（G の元の個数）＝（左剰余類の個数）×（H の元の個数）．すなわち $|G| = [G : H]|H|$．　□

練習 15. 巡回群 $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ とその部分群 $\mathbb{Z}_6^{\mathrm{ev}} = \{\bar{0}, \bar{2}, \bar{4}\}$ を考える．

(1) $\mathbb{Z}_6/\mathbb{Z}_6^{\mathrm{ev}}$ と $[\mathbb{Z}_6 : \mathbb{Z}_6^{\mathrm{ev}}]$ を求めよ．
(2) $\mathbb{Z}_6$ と $\mathbb{Z}_6^{\mathrm{ev}}$ でラグランジュの定理を確認せよ．

定義 5.4.3 (正規部分群と剰余群)**.**
- H を G の部分群とする．すべての $h \in H$ とすべての $g \in G$ について，$ghg^{-1} \in H$ が成り立つとき，H は G の**正規部分群**という．このとき $H \triangleleft G$ と表す．
- H が G の正規部分群のとき，左剰余集合 G/H は積 $\bar{a} \cdot \bar{b} = \overline{ab}$ で群になる．この群を G の H による**剰余群**という．

練習 16. H が G の正規部分群のとき，左剰余集合 G/H は積 $\bar{a} \cdot \bar{b} = \overline{ab}$ で群になることを示せ．（逆に H が正規部分群でないとき，上の積が *well-defined* になるとは限らないことを確認せよ．）

定義 5.4.4. 群 G は積が可換（$ab = ba$）のとき**アーベル群**と呼ばれる．

練習 17. アーベル群の部分群は正規部分群であることを示せ．

演習 5. 一般線型群 $GL(n;\mathbb{C})$ とは可逆な 2×2 行列のなす集合を行列の積で群とみなしたものである．このとき特殊線型群

$$SL_n = \{A \in M(n;\mathbb{C}) \mid \det(A) = 1\}$$

が正規部分群になることを示せ．$GL(n;\mathbb{C})$ の正規部分群には他にどんなものがあるだろう？

5.5　群の準同型（♣）

定義 5.5.1 (群の準同型)**.** G と H を群とする．

- 写像 $\phi\colon G \to H$ で，任意の $a, b \in G$ に対して $\phi(ab) = \phi(a)\phi(b)$ となるものを**準同型写像**という．
- 全単射準同型写像を**同型写像**とよび，同型写像 $\phi\colon G \to H$ が存在するとき G と H は**同型**という．
- $\mathrm{Im}(\phi) = \{\phi(a) \mid a \in G\} \subset H$ を ϕ の**像**とよび，$\mathrm{Ker}(\phi) = \{a \in G \mid \phi(a) = e\} \subset G$ を ϕ の**核**とよぶ．

練習 18. $\phi\colon G \to H$ を群の準同型写像とする．次を示せ．

(1) $\phi(1) = 1$, および $\phi(a^{-1}) = \phi(a)^{-1}$.
(2) $\mathrm{Im}(\phi)$ は H の部分群であり，$\mathrm{Ker}(\phi)$ は G の正規部分群である．
(3) ϕ が単射 $\iff \mathrm{Ker}(\phi) = \{e\}$
(4) 群の同型は同値関係である．

定理 5.5.2 (群の準同型定理)**.** 群の準同型写像 $\phi\colon G \to H$ が与えられたとき，群の同型 $G/\mathrm{Ker}(\phi) \cong \mathrm{Im}(\phi)$ が成立する．

Proof. 写像 $\phi\colon G \to H$ は $G/\mathrm{Ker}(\phi)$ の上で well-defined で，これが同型写像になる．

□ 酒井 p12

練習 19. 加法群 $\mathbb{Z}$ の部分群 $m\mathbb{Z}$ による剰余群は $(\mathbb{Z}_m, +)$ と同型であることを示せ．

練習 20. 任意の部分群 H に対して環の準同型写像 $\phi\colon G \to S$ であって $\mathrm{Ker}(\phi) = H$ となるものが存在することを示せ．

5.6 直積群と有限アーベル群の基本定理（♣）

定義 5.6.1 (直積群)**.** 群 $G_1, \cdots, G_r$ の**直積群**とは，直積集合 $G = G_1 \times \cdots \times G_r$ に積を

$$(a_1, \ldots, a_r) \cdot (b_1, \ldots, b_r) = (a_1 \cdot b_1, \ldots, a_r \cdot b_r)$$

で定義した群である．単位元は $(e, \ldots, e)$ であり，$(a_1, \ldots, a_r)$ の逆元は $(a_1, \ldots, a_r)^{-1} = (a_1^{-1}, \ldots, a_r^{-1})$ である．

定理 5.6.2. m と n が互いに素な自然数のとき，$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ が成り立つ．

酒井 p13

定理 5.6.3 (有限アーベル群の基本定理)**.** 有限アーベル群 G は巡回群の直積に同型である．より詳しくは，$n_i | n_{i+1}$ を満たす自然数の組 $(n_1, \ldots, n_r)$ が一意的に存在して，

$$G \sim \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$$

が成立する．

m と n が互いに素じゃないときはどうなる？

第 6 章

環と体という見方

（第八回・12/26）（第九回・1/6）

和と積を同時に考える枠組み.

6.1 環と体（♣）

定義 6.1.1 (環). 加法（和）$+$ および乗法（積）$\cdot$ のふたつの二項演算をもつ集合 R は以下の条件を満たすとき**環**であるという.

(1) 加法 $+$ についてアーベル群になる.
(2) 乗法 $\cdot$ についてモノイドになる.
(3) 分配法則

$$a(b+c) = ab + ac, \quad (b+c)a = ba + ca$$

が成り立つ.

加法に関する単位元を**零元**と呼び 0 で表す. 乗法に対する単位元を e と書き，逆元をもつ R の元を R の**単元**という.

命題 6.1.2 (単位元の一意性). 単位元は一意的である.

練習 21. (1) $(\mathbb{Z}, +, \times)$ と $(\mathbb{Q}, +, \times)$ が環になることを示せ.
(2) $(\mathbb{Z}_m, +, \times)$ が環になることを示せ.

定義 6.1.3 (可換環と整域).
- 乗法について可換な環を**可換環**という.
- 可換環 R の元 a は，$ab = 0$ となる $b \neq 0$ があるとき**零因子**と呼ばれる.
- 可換環 R は 0 以外の零因子を持たないとき**整域**と呼ばれる.

定義 6.1.4 (体). 可換環 R において，0 以外の元が存在し，それらが全て乗法に関する逆元をもつとき R を**体**という.

練習 22. (1) 体は整域であることを示せ.
(2) $(\mathbb{Q}, +, \times)$ が体になることを示せ.
(3) 素数 p に対して $(\mathbb{Z}_p, +, \times)$ が体になることを示せ.（実は逆も成り立つ.）

つまり $(\mathbb{Z}_p, +, \times)$ は整域.

6.2　イデアルと剰余環（♣）

定義 6.2.1 (部分環)**.** 環 R の e を含む部分集合 S で，R の加法と乗法に関してそれ自身が環になっているものを**部分環**という.

定義 6.2.2 (イデアル)**.** 環 R において，次の性質を満たす空でない部分集合 I を**イデアル**と呼ぶ.

(1) R の加法について，I は群になる.
(2) 任意の $a \in I$ と $c \in R$ について，$ca \in I$, $ac \in I$.

イデアルは部分環の特別なものです.

R 自身，および $\{0\}$ は明らかにイデアルである．これらを**自明なイデアル**という.

練習 23. 体には自明なイデアルしかないことを示せ.

定義 6.2.3. R を可換環とし，I をイデアルとする.

- $a_1, \ldots, a_r \in R$ について $I = \{c_1a_1 + c_2a_2 + \cdots c_ra_r \mid c_i \in R\}$ となるとする．このとき $I = (a_1, \ldots, a_r)$ と書き，$A = \{a_1, \ldots, a_r\}$ を I の**生成系**，$a_1, \ldots, a_r$ を I の**生成元**という.
- 一つの元で生成されるイデアルを**単項イデアル**と呼ぶ.

アーベル群の部分群は正規部分群でした（練習 17）．つまり剰余環の加法だけ考えると…

定義 6.2.4 (剰余環)**.** I を環 R のイデアルとする．R に同値関係を次のように定める.

$$a \sim b \quad \Longleftrightarrow \quad a - b \in I.$$

この同値関係による同値類 $R/\sim$ を R/I で表し，a の属する同値類を $\bar{a}$ と表す．R/I は加法と乗法を $\bar{a} + \bar{b} = \overline{a+b}$, $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$ で定義すると環になる．この環を R の I による**剰余環**または商環という.

練習 24:これがわかるとイデアルの定義の意味がわかる.

練習 24. 剰余環 R/I の加法と乗法が矛盾なく定義されていることを示せ.

練習 25. 剰余群の定義と剰余環の定義を見比べて，それらがどう自然なのか考えてみよう.

6.3　環の準同型（♣）

定義 6.3.1 (環の準同型)**.** R と S を環とする.

- 写像 $\phi\colon R \to S$ であって，次の条件を満たすものを**準同型写像**という.
  (1) 任意の $a, b \in R$ について，$\phi(a+b) = \phi(a) + \phi(b)$.
  (2) 任意の $a, b \in R$ について，$\phi(ab) = \phi(a)\phi(b)$.
  (3) $\phi(e_R) = e_S$.
  ただし e_R, e_S はそれぞれ R,S の積に対する単位元.
- 全単射準同型写像を**同型写像**とよび，同型写像 $\phi\colon R \to S$ が存在するとき R と S は**同型**という.
- $\mathrm{Im}(\phi) = \{\phi(a) \mid a \in G\}$ を ϕ の**像**とよび，$\mathrm{Ker}(\phi) = \{a \in G \mid \phi(a) = 0\}$ を ϕ の

核とよぶ.

練習 26. (1) $\phi(0)=0$, $\phi(-a)=-\phi(a)$, および $\phi(a^{-1})=\phi(a)^{-1}$ を確かめよ.
(2) $\mathrm{Im}(\phi)$ は S の部分環であり，$\mathrm{Ker}(\phi)$ は R のイデアルである.
(3) ϕ が単射 $\iff$ $\mathrm{Ker}(\phi)=\{0\}$
(4) 環の同型は同値関係である.

定義 6.3.2 (環の準同型定理). 環の準同型写像 $\phi\colon R\to S$ が与えられたとき，群の同型 $R/\mathrm{Ker}(\phi)\cong\mathrm{Im}(\phi)$ が成立する.

Proof. 写像 $\phi\colon R\to S$ は $R/\mathrm{Ker}(\phi)$ の上で well-defined で，これが同型写像になる. □

練習 27. 環 $(\mathbb{Z}_m,+,\times)$ は環 $\mathbb{Z}$ のイデアル (m) による剰余環と同型であることを示せ.

練習 28. (1) 任意のイデアル I に対して環の準同型写像 $\phi\colon R\to S$ であって $\mathrm{Ker}(\phi)=I$ となるものが存在することを示せ.
(2) 体 K から環 R への零写像でない準同型写像は単射であることを示せ.

6.4 剰余環 $\mathbb{Z}_m$ と体（♢）

定理 6.4.1. 自然数 m が素数 $\iff$ 剰余環 $(\mathbb{Z}_m,+,\times)$ が体.

定理 4.1.2, 定理 5.3.1 に引き続き 3 つめの素数の特徴付け.

Proof. ($\Rightarrow$) はすでに示した (練習 22). ここでは ($\Leftarrow$) を背理法で示す.
自然数 m に対して $(\mathbb{Z}_m,+,\times)$ が体であるとする. m が素数でないとすると，$1<n<m$ なる m の約数 n が存在する. このとき m と n は互いに素でないので $nx+my=1$ を満たす x,y は存在しない（一次不定方程式の解の存在）. すなわち $\bar{n}\cdot\bar{x}=\bar{1}\in\mathbb{Z}_m$ なる $\bar{x}$ が存在しないので，$\bar{n}$ は単元にならない. これは $(\mathbb{Z}_m,+,\times)$ が体であることに矛盾. 従って m は素数でなければならない. □

演習 6. 定理 *6.4.1* の証明を初めから最後まで再構成してみよう.

命題 6.4.2. m を 2 以上の自然数とし，$\mathbb{Z}_m$ を m に関する $\mathbb{Z}$ の剰余環とする. $\bar{a}$ について,

(1) a と m が互いに素であれば，$\bar{a}$ は $\mathbb{Z}_m$ の単元である.
(2) a と m が互いに素でなければ，$\bar{a}$ は $\mathbb{Z}_m$ の零因子である.

Proof. (1) は一次不定方程式の解の存在と同等. (2) を示す. a と m が最大公約数 $d>1$ を持つとする. すなわち

$$a=da',\quad m=dm',\quad (a',m')=1.$$

すると

$$am'=da'm'=ma'\equiv 0 \pmod{m}.$$

したがって $\bar{m}'\neq\bar{0}$ に対して $\bar{a}\cdot\bar{m}'=\bar{0}$ となり，$\bar{a}$ は $\mathbb{Z}_m$ の零因子である. □

河田 6.2 章（p67）

6.5　ウィルソンの定理再訪（♢）

補題 6.5.1. p を素数とする．$\bar{x} \in \mathbb{Z}_p$ に対して

$$\bar{x}^2 = \bar{1} \Rightarrow \bar{x} = \overline{p-1} \text{または} \bar{x} = \bar{1}.$$

Proof. $\bar{x}^2 = \bar{1}$ より

$$\bar{x}^2 - \bar{1} = \bar{0} \Rightarrow (\bar{x}+1)(\bar{x}-1) = \bar{0}.$$

$\mathbb{Z}_p$ は整域だから

$$(\bar{x}+1) = \bar{0} \text{または} (\bar{x}-1) = \bar{0}.$$

したがって

$$\bar{x} = \overline{-1} = \overline{p-1} \text{または} \bar{x} = \bar{1}.$$

□

定理（再掲） (ウィルソンの定理)．自然数 n が素数 $\iff$ 2 以上の自然数 n に対して $E(n) = (n-1)! + 1$ を n で割った余り $W(n) = 0$.

定理（再掲） (定理 4.1.2; ウィルソンの定理 $\mathbb{Z}_p$ver.)．p を素数とする．このとき $\mathbb{Z}_p$ において

$$\bar{1} \cdot \bar{2} \cdots \overline{(p-2)(p-1)} = \overline{-1}.$$

Proof. 補題 6.5.1 より $\mathbb{Z}_p$ の元で $\bar{x}^2 = 1$ となるものは $\bar{x} = \bar{1}, \overline{(p-1)}$ のみである．そのほかの元 $\{\bar{2}, \bar{3}, \ldots, \overline{(p-2)}\}$ は，$\mathbb{Z}_p$ が体であることによりそれぞれの逆元がまたこの中に入っていて，しかも一意である．すなわち

$$\bar{2} \cdot \bar{3} \cdots \overline{(p-2)} = \bar{1}.$$

これより

$$\bar{1}\bar{2} \cdot \bar{3} \cdots \overline{(p-2)} \cdots \overline{(p-1)} = \overline{(p-1)} = \overline{-1}.$$

□

第 7 章

まとめともろもろ

（自習）

さて．振り返ります．

7.1 素数の特徴付け：集合・群・環・体それぞれからの見方

自然数 m が素数であることの 3 つの特徴付け：

定理（再掲） (定理 4.1.2)．自然数 m が素数 $\iff$ 2 以上の自然数 m に対して $W(m) = 0$ $\iff$ $(m-1)! + 1 \equiv 0 \pmod{m}$ $\iff$ $\overline{(m-1)!} + \bar{1} = \bar{0} \in \mathbb{Z}_m$

定理（再掲） (定理 5.3.1)．自然数 m が素数 $\iff$ $(\mathbb{Z}_m \setminus \{0\}, \times)$ が群

定理（再掲） (定理 6.4.1)．自然数 m が素数 $\iff$ 剰余環 $(\mathbb{Z}_m, +, \times)$ が体

上の特徴付けたちの背後にある素数の性質：

定理（再掲） (定理 4.4.2)．p を素数とする．このとき，任意の $a \in \mathbb{Z}_p \setminus \{0\}$ は逆元をもつ．すなわち

$$ax \equiv 1 \pmod{p}$$

となる $x \in \mathbb{Z}_p$ が唯一つ存在する．

7.2 オイラーの定理とフェルマーの小定理（◇）

石田 p61-(2–4 章) 参照

定義（再掲） (既約剰余類群)．m を自然数とする．$(m, n) = 1$ となる n に対して $\bar{n} \in \mathbb{Z}_m$ を $\mathbb{Z}_m$ の**既約剰余類**と呼ぶ．既約剰余類は単元であり，その全体からなる $\mathbb{Z}_m$ の部分集合 Γ_m は乗法に関して群になる．これを $\mathbb{Z}_m$ の**既約剰余類群**という．

練習 29. 表 *2–5* を埋めよ．

定義 7.2.1. m を自然数とする．m 以下の自然数 $\{1, 2, \ldots, m\}$ の中で m と互いに素なものの個数を $\varphi(m)$ と書き，**オイラー関数**と呼ぶ．

練習 30. $\bar{x}$ を $\mathbb{Z}_m$ の単元とすると，$\bar{x}^{\varphi(m)} = \bar{1}$ を示せ．
（ヒント：$\varphi(m)$ は $\mathbb{Z}_m$ の既約剰余類群の位数に等しい．既約剰余類群の部分群で $\bar{x}$ の生成する巡回群を考える．＋ ラグランジュの定理:定理 *5.4.2*）

石田 p62

定理 7.2.2 (オイラーの定理)**.** m を 2 以上の自然数，x を整数とする．このとき

$$(x, m) = 1 \quad \Rightarrow \quad m|(x^{\varphi(m)} - 1).$$

とくに $m = p$ が素数であれば

$$p \not| x \to m|(x^{p-1} - 1).$$

いろんな道から同じ頂上にたどり着く様は面白いですね.

となりフェルマーの小定理（定理 4.4.3：$x^{p-1} \equiv 1 \pmod{p}$）が従う．

Proof. 練習 30 の言い換え．
$\bar{x}$ が $\mathbb{Z}_m$ の単元 $\iff$ $(x, m) = 1 \Rightarrow \bar{x}^{\varphi(m)} = \bar{1}$ $\iff$ $m|(x^{\varphi(m)} - 1)$ □

7.3 メビウスの関数（♢）

$\varphi(m)$ を計算する公式を与える．
一般に，自然数に対して定義された複素数値関数 f を考え，$m \in \mathbb{N}$ に対して

$$\sum_{d|m} f(d)$$

で m のすべての正の約数 d についての $f(d)$ の和を表すことにする．

練習 31. $\sum_{d|m} f(d) = \sum_{d|m} f(\frac{m}{d})$ を示せ．
（ヒント： m の正の約数の集合を S とする．このとき $g\colon S \to S,\ d \mapsto \frac{m}{d}$ は全単射を与える．）

定義 7.3.1 (メビウス（Möbius）の関数)**.**

$$\mu(m) = \begin{cases} 1, & m = 1 \text{ のとき}, \\ 0, & \text{ある素数 } p \text{ に対し } p^2|m, \text{のとき}. \\ (-1)^k & m = p_1 \cdots p_k (p_k \text{ は相異なる素数}) \text{ のとき}. \end{cases}$$

練習 32. $(m, n) = 1$ であれば $\mu(mn) = \mu(m)\mu(n)$ となることを示せ．（ヒント：$\mu(m)$ と $\mu(n)$ の値で場合分けして一つづつ考える．）

定理 7.3.2. 以下の等式が成り立つ．

$$\sum_{d|m} \mu(d) = \begin{cases} 1 \ \textit{if } m = 1, \\ 0 \ \textit{if } m \neq 1 \end{cases}$$

Proof. $m = p_1^{e_1} \cdots p_s^{e_s}$, $d = p_1^{g_1} \cdots p_s^{g_s}$ と置いて計算してみる．二項定理を使う． □

定理 7.3.3 (メビウス関数の反転公式)**.** f を自然数上の関数とし，$F(m) = \sum_{d|m} f(d)$ とおく．このとき次が成り立つ．

$$f(m) = \sum_{d|m} \mu(d) F\left(\frac{m}{d}\right) = \sum_{d|m} \mu\left(\frac{m}{d}\right) F(d).$$

考察. 2 つめの等式は練習 31 より．1 つめの等式を小さい方から確かめていく．$m = 1$ のとき

$$\mu(1)F(1) = f(1)$$

$m = p$ (p:素数) のとき

$$\begin{aligned}\mu(1)F(p) + \mu(p)F(1) &= \mu(1)\{f(1) + f(p)\} + \mu(p)f(1)\\ &= \{\mu(1) + \mu(p)\} f(1) + \mu(1)f(p)\\ &= f(p)\end{aligned}$$

$m = p^2$ (p:素数) のとき

$$\begin{aligned}\mu(1)F(p^2) + \mu(p)F(p) + \mu(p^2)F(1) &= \mu(1)\left\{f(1) + f(p) + f(p^2)\right\} + \mu(p)\{f(1) + f(p)\} + \mu(p^2)f(1)\\ &= \left\{\mu(1) + \mu(p) + \mu(p^2)\right\} f(1) + \{\mu(1) + \mu(p)\} f(p) + +\mu(1)f(p^2)\\ &= f(p^2)\end{aligned}$$

$m = p_1p_2$ (p_1, p_2:素数) のとき

$$\begin{aligned}&\mu(1)F(p_1p_2) + \mu(p_1)F(p_2) + \mu(p_2)F(p_1) + \mu(p_1p_2)F(1)\\ &\quad= \mu(1)\{f(1) + f(p_1) + f(p_2) + f(p_1p_2)\} + \mu(p_1)\{f(1) + f(p_2)\} + \mu(p_2)\{f(1) + f(p_1)\} + \mu(p_1p_2)f(1)\\ &\quad= \{\mu(1) + \mu(p_1) + \mu(p_2) + \mu(p_1p_2)\} f(1) + \{\mu(1) + \mu(p_1)\} f(p_2) + \{\mu(1) + \mu(p_2)\} f(p_1) + \mu(1)f(p_1p_2)\\ &\quad= f(p_1p_2)\end{aligned}$$

いずれも最後の等式は定理 7.3.2 を使った. □

練習 33. 定理 *7.3.3* を示せ.

7.3.1 メビウス関数とオイラー関数

定理 7.3.4. 以下の等式が成り立つ.

$$\sum_{d|n} \frac{\mu(d)}{d} = \begin{cases}1, & m = 1 \text{ のとき},\\ \prod_{i=1}^{s}\left(1 - \frac{1}{p_i}\right), & m = p_1^{e_1}p_2^{e_2}\cdots p_s^{e_s} \text{のとき}.\end{cases}$$

Proof. 定理 7.3.2 と同様に $m = p_1^{e_1}\cdots p_s^{e_s}$, $d = p_1^{g_1}\cdots p_s^{g_s}$ と置いて計算してみる. □

補題 7.3.5. 自然数 m に対して次が成り立つ.

$$m = \sum_{d|m} \varphi\left(\frac{m}{d}\right) = \sum_{d|m} \varphi(d)$$

Proof. $x = 1, \ldots, m$ とする. x と m の最大公約数は m の約数である.

主張：m の約数 d に対し，$(m, x) = d$ となるような x の数は $\varphi(\frac{m}{d})$ である.

上の主張を仮定すると，$1, \ldots, m$ を m との約数で分類して，その数を約数ごとに足しあげることで $m = \sum_{d|m} \varphi\left(\frac{m}{d}\right)$ が従う.

上の主張を示す. $(m, x) = d$ となる x は $x = dn$, $(n, \frac{m}{d}) = 1$ である. このような n の個数はオイラー関数 $\varphi(\frac{m}{d})$ より主張が従う. □

系 7.3.6.

$$\varphi(m) = \begin{cases}1, & m = 1 \text{ のとき},\\ m\prod_{i=1}^{s}\left(1 - \frac{1}{p_i}\right), & m = p_1^{e_1}p_2^{e_2}\cdots p_s^{e_s} \text{のとき}.\end{cases}$$

特に $(m, n) = 1$ ならば $\varphi(mn) = \varphi(m)\varphi(n)$ が従う.

Proof. 補題 7.3.5 の等式

$$m = \sum_{d|m} \varphi\left(\frac{m}{d}\right) = \sum_{d|m} \varphi(d)$$

に反転公式を使うと

$$\varphi(m) = \sum_{d|m} \mu(d)\frac{m}{d} = m\sum_{d|m} \frac{\mu(d)}{d}.$$

定理 7.3.4 より系の主張が従う． □

練習 34. p を素数とすると $\varphi(p^e) = p^e - p^{e-1}$ となることを示せ．

7.3.2　メビウス関数とエラトステネスの篩

エラトステネスの篩は，知っている素数で割れる自然数を篩にかけて自然数の集合から除いていく方法であった．言い換えると，知っている素数で割れない自然数を残す方法とも言える．自然数をひとつ取ったとき，知っている素数で割れるか割れないかを判定する写像（指示関数）はメビウス関数で得られる．

メビウス関数での定式化は言い換えであって，アルゴリズムとしては等価．つまり，知っている素数で割るか割れないかをひとつづつ判定するという方法は変わらない．

定義 7.3.7. 集合 X とその部分集合 A が与えられたとき，写像

$$\chi_A\colon X \to \{0,1\}, \quad \chi_A(x) = \begin{cases} 1 \ if\, x \in A, \\ 0 \ if\, x \notin A \end{cases}$$

を X の A による**指示関数**と呼ぶ．

帰納的に，$p_1, \ldots, p_k$ を知っている素数とし，$P = p_1, \ldots, p_k$ とおく．自然数 n が $p_1 \ldots, p_k$ のどれかで割れることと，$(n, P) > 1$ であることは同値である．素数 $p_1, \ldots, p_k$ のいずれでも割れない自然数の部分集合を A_k とおくと，以下が成り立つ．

系 7.3.8.

$$\chi_{A_k}(n) = \sum_{d|(n,P)} \mu(d).$$

Proof. 定理 7.3.2 より． □

7.4　命題 5.3.3 (2)：$(\mathbb{Z}_p)^\times$ が巡回群であることの証明

補題 7.4.1. G を位数 n の群とする．すべての $a \in G$ について a の位数は n の約数である．

とくに $\mathbb{Z}_m$ の既約剰余類群を考えるとオイラーの定理が従う．

Proof. 練習 30 の一般化．G と，a で生成される部分群 $\langle a \rangle$ に対してラグランジュの定理を使う． □

補題 7.4.2. p を素数とすると $\mathbb{Z}_p^\times$ の位数 d の個数は 0 またはオイラー関数 $\varphi(d)$ である．

Proof. 以下を認める：

$\mathbb{Z}_p$ 上の n 次多項式 $f(x)$ の根の個数は n 以下である（$\Leftarrow$ 定理 9.1.6）.

$(\mathbb{Z}_p)^\times$ に位数 d の元 a が存在するとする．このとき $\bar{x}^d - \bar{1} = \bar{0}$ の解の集合は $\{a, a^2, \ldots, a^d\}$ である．この中から位数 d の元を拾う．a^k の位数を d_k とする．このとき

$$d_k = d \quad \Longleftrightarrow \quad (d, k) = 1$$

より位数 d の個数はオイラー関数 $\varphi(d)$ になる． □

補題（再掲） (補題 7.3.5)**.** 自然数 m に対して次が成り立つ.

$$m = \sum_{d|m} \varphi(d)$$

練習 35. 補題 *7.3.5,7.4.1,7.4.2* を用いて，素数 p に対して $(\mathbb{Z}_p)^\times$ が巡回群になることを証明せよ.

第 8 章

群と対称性

（第十回・1/9）

群は対称性を記述するための言語である．
推奨動画：東京大学 2006 年度 数学公開講座 『対称性と群』
(https://www.ms.u-tokyo.ac.jp/video/open/2006koukai-kouza/index.html)

8.1 群の作用（♣）

酒井 p14-

定義 8.1.1 (群の作用)．– 群 G の集合 X への**作用**とは，写像

$$G \times X \to X, \quad (g, u) \mapsto gu,$$

であって，すべての $u \in X$ と $a, b \in G$ に対して
(1) $eu = u$,
(2) $(ab)u = a(bu)$
が成り立つものをいう．

– 任意の $u, v \in X$ に対して $a \in G$ が存在して $v = au$ となるとき，G は X に**推移的**に作用するという．

– $u \in X$ をひとつとる．群 G が X に作用しているとき，集合 $\mathrm{Orb}(u) = \{\sigma u \mid \sigma \in G\} \subset X$ を u の**軌道**（*Orbit*）という．

– $u \in X$ に対して $G_u = \{\sigma \in G \mid \sigma u = u\} \subset G$ とおくと，G_u は G の部分群になる．G_u を u の**固定群**と呼ぶ．

練習 36. (1) $u, v \in X$ に対して $u \sim v \iff v \in \mathrm{Orb}(u)$ すると, $\sim$ は同値関係を定めることを示せ．
(2) G_u が部分群になることを示せ．

練習 37. $|\mathrm{Orb}(u)| = [G : G_u]$ となることを示せ．
ヒント：全単射 $\mathrm{Orb}(u) \to G/G_u$ をつくる．

酒井, 補題 1.12

演習候補

8.2 巡回群 $\mathbb{Z}_m$ の作用（♢）

$X_0 = \{x_1, \ldots, x_m\}$ を位数 m の集合とすると，巡回群 $\mathbb{Z}_m$ は以下で X_0 に作用する．

$$m_0 \colon \mathbb{Z}_m \times X_0 \to X_0, \quad (\bar{n}, x_i) \mapsto x_{i+n},$$

ただし $x_{i+m} = x_i$ とおく．

練習 38.　(1) 写像 m_0 が作用になっていることを確認せよ．
(2) m_0 は推移的な作用であることを示せ．
(3) x_i の固定群 $(\mathbb{Z}_m)_{x_i}$ を求めよ．

X_1 を複素数平面の中心に埋め込まれた正 m 角形（内部は含まない）とすると，巡回群 $\mathbb{Z}_m$ は回転として X_1 に作用する．

$$m_1 \colon \mathbb{Z}_m \times X_1 \to X_1, \quad (\bar{n}, x+yi) \mapsto e^{\frac{2\pi i n}{m}}(x+yi).$$

練習 39.　(1) 写像 m_1 が作用になっていることを確認し，正 m 角形の頂点集合への作用が m_0 と等しいことを確認せよ．
(2) m_1 は推移的な作用で**ない**ことを示せ．
(3) $u \sim v \iff v \in \mathrm{Orb}(u)$ で定まる同値関係による商集合 $X_1/\sim$ をとる．$X_1/\sim$ の代表元の集合で複素平面内で連結なものをひとつ求めよ．

X_2 を複素数平面の中心に埋め込まれた正 m 角形（内部を含む）とすると，巡回群 $\mathbb{Z}_m$ は回転として X_2 に作用する．

$$m_2 \colon \mathbb{Z}_m \times X_2 \to X_2, \quad (\bar{n}, x+yi) \mapsto e^{\frac{2\pi i n}{m}}(x+yi).$$

絵を描いて考えてみる．

練習 40.　(1) 原点 0 の固定群を求めよ．
(2) $u \sim v \iff v \in \mathrm{Orb}(u)$ で定まる同値関係による商集合 $X_2/\sim$ をとる．$X_1/\sim$ の代表元の集合で複素平面内で連結なものをひとつ求めよ．

8.3　対称群（♢）

横井/硲野 p29

定義 8.3.1. 集合 X から X 自身への全単射写像全体からなる集合 $S(X)$ は写像の合成に関して群になる．

- $S(X)$ を X 上の**対称群**といい，$S(X)$ の元を**置換**という．
- とくに X が有限集合 $\{1,\dots,n\}$ のとき，$S(X) = S_n$ と表し，n **次対称群**という．ひとつの置換 δ は $(1,2,\dots,n)$ を上段に，その像 $(\delta(1),\delta(2),\dots,\delta(n))$ を下段に書いて

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \delta(1) & \delta(2) & \cdots & \delta(n) \end{pmatrix}$$

と表す．

練習 41.　(1) 群 S_n は位数 $n!$ で，$n \geq 3$ に対して非可換な群になることを示せ．
(2) 定義 *8.3.1* の記法に基づいて S_3 の元を全て挙げよ．

定義 8.3.2.　- S_n の元で，部分集合 $\{i_1,\dots,i_r\}$, $1 \leq r \leq n$, を巡回的にうつす元

$$\begin{cases} \sigma(i_1) = i_2,\ \sigma(i_2) = i_3,\ \dots,\ \sigma(i_{r-1}) = i_r,\ \sigma(i_r) = i_1, \\ \sigma(j) = j, (j \neq i_1,\dots,i_r) \end{cases}$$

を**長さ r の巡回置換**といい，$(i_1,\dots,i_r)$ で表す．長さ 2 の巡回置換を**互換**という．

– 2 つの巡回置換 $(i_1,\dots,i_r)$ と $(j_1,\dots,j_s)$ は，2 つの部分集合として共通部分がないとき**互いに素**であるという．

定理 8.3.3. (1) S_n の任意の元は互いに素な幾つかの巡回置換の積で一意的に表される．
(2) S_n の任意の元はいくつかの互換の積で表される．このとき互換の積の個数の偶奇は一意的である．

横井/硲野 p57, 定理 9, 10

ビデオ参照

定義 8.3.4.
– 偶数個の互換の積で表される S_n の元を**偶置換**，奇数個の互換の積で表される S_n の元を**奇置換**という．
– S_n の元 σ の**符号**を，偶置換のとき $\mathrm{sgn}(\sigma)=1$, 奇置換のとき $\mathrm{sgn}(\sigma)=-1$ と定める．
– S_n の偶置換の全体を A_n と書き，n **次交代群**と呼ぶ．

練習 42. A_n は長さ 3 の全ての巡回置換で生成されることを示せ．

酒井, 例題 1.7

定理 8.3.5. G を位数 n の有限群とする．このとき S_n のある部分群で G と同型になるものが存在する．

横井/硲野 p59, 例題 16

Proof. $G=\{a_1,a_2,\dots,a_n\}$ とおく．定義より S_n は G 上の対称群である．一方，G の元 a をとると，G 上の全単射写像 $T_a\colon G\to G$ が a の左からの積 $T_a(g)=ag$ で定まる（全単射であることを確認せよ）．これは写像

$$T\colon G\to S_n,\quad a\mapsto T_a$$

を定める．T が群の単射準同型であることを示せば主張が従う．
$a,b\in G$, $x\in G$ に対して

$$T_{ab}(x)=(ab)x=a(bx)=T_a(bx)=T_a(T_b(x))=(T_a\cdot T_b)(x)$$

となるから T は群の準同型である．$T_a=T_b$ とすると

$$a=T_a(e)=T_b(e)=b$$

となるから T は単射である． □

演習 7. $\mathbb{R}^3$ の中の正四面体をそれ自身に重ねる回転のつくる群（正四面体群）は 4 次の交代群 A_4 になることを示せ．
ヒント：頂点への作用を考えると S_4 の部分群になる．

横井/硲野 p60, 例題 18

8.4 可解群（♢）

「多項式 $f(x)$ がベキ根によって解けるための必要十分条件は $f(x)$ のガロア群が可解群であることである」–10 章参照

定義 8.4.1. G を群とする．$a,b\in G$ に対し $[a,b]=aba^{-1}b^{-1}$ とおき，a,b の**交換子**と呼ぶ．G のすべての交換子で生成された部分群を G の**交換子群**と呼び，$[G,G]$ とかく．

練習 43. G を群とする．

(1) $[G,G]=\{1\}$ の必要十分条件は G がアーベル群であることである．これを示せ．
(2) $[G,G]$ が正規部分群であることを示せ．

定理 8.4.2. G を群とし，H をその正規部分群とする．G/H がアーベル群である必要十分条件は $H \supset [G,G]$ となることである．とくに $G/[G,G]$ はアーベル群になり，これを G の**アーベル化群**と呼ぶ．

酒井 p17, 命題 1.16

定義 8.4.3. G を群とする．

- G が**可解群**であるとは，正規部分群の列

$$G = G_0 \triangleright \cdots \triangleright G_{l-1} \triangleright G_l = \{1\}$$

が存在して各剰余群 G_{i-1}/G_i がアーベル群になることをいう．
- $G^{(0)} = G$ とおき，帰納的に $G^{(i+1)} = [G^{(i)}, G^{(i)}]$ と定義する．この正規部分群の列

$$G = G^{(0)} \triangleright G^{(1)} \triangleright G^{(2)} \triangleright \cdots$$

を G の**交換子群列**という．

酒井 p18–19, 命題 1.17–1.20

命題 8.4.4. G が可解群 $\iff$ ある r が存在して $G^{(r)} = \{1\}$.

命題 8.4.5. 可解群の部分群および準同型写像の像は再び可解群である．

命題 8.4.6. 群 G とその部分群 H が与えられているとき，H と G/H が可解群であれば G も可解群である．

定理 8.4.7. 対称群 S_n は $n \leq 4$ のときは可解であるが，$n \geq 5$ のときは可解でない．

演習 8. 定理 *8.4.7* の証明に挑戦してみよう．$n = 1, 2$ は明らか．$n = 3, 4$ は具体的に考える．$n \geq 5$ は $n = 3, 4$ の場合を参考にして考える．

第 9 章

多項式と環

9.1 多項式環（♣）

（第十一回・1/24）（第十二回・1/28）

定義 9.1.1. – 環 R 上の**多項式**とは，文字 x による形式的な有限和

酒井 2 章, p28–

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \quad (a_i \in R)$$

のことをいう．文字 x を**不定元**あるいは**変数**とよぶ．

– 環 R 上の多項式全体の集合を $R[x]$ で表し，**加法**と**乗法**を次のように定義する．

$$\sum_i a_ix^i + \sum_j b_jx^j = \sum_k (a_k + b_k)x^k,$$

$$\left(\sum_i a_ix^i\right) \cdot \left(\sum_j b_jx^j\right) = \sum_k \left(\sum_{i+j=k} a_i \cdot b_j\right) x^k,$$

この加法と乗法により $R[x]$ は環になる．R が可換環のとき，$R[x]$ も可換環である．

– 多項式

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n, a_n \neq 0$$

について，n を $f(x)$ の**次数**とよび，$\deg f$ で表す．

練習 44. R を可換環とし，f, g を R 上の多項式とする．

(1) $\deg(f+g) \leq \max\{\deg f, \deg g\}$

(2) $\deg(fg) \leq \deg f + \deg g$．もし f, g のどちらかの最高次の係数が零因子でなければ，等号が成立する．

酒井 p29, 補題 2.2

Proof.

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m, a_m \neq 0,$$
$$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n, b_n \neq 0$$

と置いて和と積を考える．(1) は明らか．(2) で fg の最高次の係数 a_mb_n が 0 となるのは a_m, b_n のどちらも零因子のときである． □

系 9.1.2. R が整域であれば R 上の多項式環は整域である．

練習 45. 整域 R 上の多項式環 $R[x]$ の単元は，R の単元と一致することを示せ．

定理 9.1.3 (除法定理)**.** R を可換環とし，$f, g \in R[x]$ をとる．このとき，g の最高次の係数が単元であれば，$q, r \in R[x]$ が存在して

$$f = qg + r, \quad \deg r < \deg g$$

が成立する．さらに商 q と剰余 r は f, g によって一意的に定まる．

定義 9.1.4. R を可換環とし，R 上の (零多項式でない) 多項式 $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in R[x]$ をひとつとる．

- R の元 $b \in R$ に対して

$$f(b) = a_0 + a_1b + a_2b^2 + \cdots + a_nb^n \in R$$

と定義し，f **の** b **における値**という．
- R の元 b は $f(b) = 0$ となるとき多項式 $f(x)$ の**根**という．
- 一般に $f, g \in R[x]$ について，$f = gh$ となる $h \in R[x]$ が存在するとき，g は f の**因子**であるという．このとき $g|f$ と表す．

定理 9.1.5 (剰余定理)**.** 可換環 R の元 a が R 上の多項式 $f(x)$ の根である必要十分条件は $(x - a)$ が f の因子になることである．

酒井 p30–p31

Proof. f を $(x - a)$ で割り算して $q(x - a) + r$ と表す．このとき $r = f(a)$ であるから主張が従う． □

定理 9.1.6. n を自然数とする．整域 R 上の n 次多項式 $f(x)$ の根の個数は n 以下である．

Proof. f の次数に関する帰納法で示す．$n = 0$ のとき $f(x)$ は根をもたないから主張は正しい．$n > 1$ とする．f が R に根をもたないときは根の個数は 0 より主張は正しい．f が根 $a \in R$ を持つとする．このとき定理 9.1.5 により $f(x) = (x - a)g(x)$, g は $n - 1$ 次多項式, と表される．f に別の根 $b \in R$ があるとき，$f(b) = (b - a)g(b) = 0$ であり, R は整域で , $(b - a) \neq 0$ だから $g(b) = 0$. $g(b)$ は $n - 1$ 次多項式だから，帰納法の仮定より根の個数は $n - 1$ 以下である．したがって f の根の個数は n 以下． □

練習 46 (R が整域でない場合)**.** $\mathbb{Z}_8$ 上の多項式 $x^2 - \bar{1}$ は 4 個の根を持つことを確かめよ．

根の数が次数より多い例

系 9.1.7. 整域 R が無限個の元を含むとする．多項式 $f(x) \in R[x]$ について，関数 $R \to R, a \mapsto f(a)$ が零関数であれば，多項式として $f = 0$ が従う．

Proof. $f \neq 0$ とし，$\deg f = n$ とおく．R から $n + 1$ 個の異なる元 $a_1, \ldots, a_{n+1}$ をとる．関数 $R \to R, a \mapsto f(a)$ が零関数であれば $a_1, \ldots, a_{n+1}$ は f の根であり，これは定理 9.1.6 に矛盾する． □

練習 47 (有限個の元しかない場合)**.** 多項式 $f(x) = x^p - x \in \mathbb{Z}_p$ は零多項式ではないが，$\mathbb{Z}_p$ 上の関数として考えると零関数になる．

零多項式ではないが零関数になる例

9.2 ユークリッド整域, 単項イデアル整域, 一意分解整域（♣）

体 K 上の多項式環 $K[x]$ の性質は，ユークリッド整域として一般化することができる．

定義 9.2.1 (ユークリッド整域)．R を整域とする．$R \setminus \{0\}$ の自然数値関数 v（ノルム）が存在して，任意の $f, g \in R,\ g \neq 0$ について

$$f = qg + r, \quad q, r \in R, \quad v(r) < v(g)$$

と表されるという条件を満たすとき，R は**ユークリッド整域**という．ただし $v(0) = -\infty$ とする．

練習 48. 体 K 上の多項式環 $K[x]$ はユークリッド整域であることを示せ．（ノルム v を指定せよ．）

定義 9.2.2 (単項イデアル整域)．可換環 R のすべてのイデアルが単項イデアルであるとき，R は**単項イデアル整域**であるという．

酒井 p47

練習 49. (1) 整数環 $\mathbb{Z}$ は単項イデアル整域であることを示せ．
ヒント：$g = \min\{|a| \mid a \in I \setminus \{0\}\}$ とおくと，$I \subset (g)$ となることを示す．
(2) $\mathbb{Z}[x]$ のイデアル $(2, x)$ は単項イデアルでないことを示せ．

定義 9.2.3 (既約元と素元)．
– 整域 R の 0 でも単元でもない元 a について，分解 $a = bc$ があれば b または c が単元になるとき，a は**既約元**であるという．
– 整域 R の 0 でも単元でもない元 a について，$a|bc$ があれば $a|b$ または $a|c$ となるとき，a は**素元**であるという．

定義 9.2.4 (一意分解整域)．整域 R が次の性質を満たすとき，R は**一意分解整域**であるという．

酒井 p40, 定義 2.21

(1) 0 でも単元でもない任意の元 $a \in R$ は既約分解をもつ．すなわち，有限個の既約元 $a_1, \ldots, a_r$ が存在して

$$a = a_1 \cdots a_r$$

と表される．
(2) 上のような分解は順序と単元の積とを除いて一意的である．すなわち，既約元 $a_1, \ldots, a_r$ と既約元 $b_1, \ldots, b_s$ について $a_1 \cdots a_r = b_1 \cdots b_s$ であれば $r = s$ であり，番号を付け替えればすべての a_i と b_i が単元の積を除いて等しい．

練習 50. (1) $\mathbb{Z}$ は一意分解整域であることを示せ（既約元は何か？）．
(2) $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ は一意分解整域でないことを示せ．

命題 9.2.5. 整域 R が以下の性質を満たせば R は一意分解整域である．

酒井 p41, 命題 2.26

(1) 0 でも単元でもない元は既約分解を持つ．
(2) 既約元は素元である．

Proof. 条件 (1) は同じなので，分解の一意性を示せば十分．R の既約元（従って素元）

$a_1,\dots,a_r$, $b_1,\dots,b_s$ が $a_1\cdots a_r = b_1\cdots b_s$ を満たすとする．$a_1|b_1\cdots b_s$ だからある b_i が存在して $a_1|b_i$. b の添字を適当に付け替えて $i=1$ とする．a_1 と b_1 はどちらも既約元だから単元 u_1 が存在して $b_1 = u_1a_1$ と表される．このとき $a_1\cdots a_r = u_1a_1\cdots b_s$ が成り立ち，R は整域より $a_2\cdots a_r = b_2\cdots b_s$. これを繰り返すと $s\geq r$ が従い, かつ $i\leq r$ について単元 u_i が存在し $b_i = u_ia_i$ となる．逆に b_i で割ることから始めると $r\geq s$ が従い, かつ $i\leq s$ について単元 u_i が存在し $a_i = u_ib_i$ となり，分解の一意性が成り立つ． □

酒井 p47, 系 2.39

酒井 p49, 命題 2.42

定理 9.2.6. ユークリッド整域は単項イデアル整域である．単項イデアル整域は一意分解整域である．

Proof. 前半を示す．R をユークリッド整域とする．$I\subset R$ をイデアルとする．$I=\{0\}$ は単項イデアルである．$I\neq\{0\}$ のとき，I に含まれる 0 でない元でノルム v が最小のものをひとつとり g とおく．$I=(g)$ を示す．$I\supset(g)$ は明らか．I の任意の元 f をとり g で割って $f = qg+r$, $q,r\in R, v(r)<v(g)$. このとき $r\in I$ となるから g の最小性より $r=0$ である．したがって $f\in(g)$, すなわち $I\subset(g)$ が成り立つ.

後半を示す．R を単項イデアル整域とする．命題 9.2.5 より，R の 0 でも単元でもない元の既約分解の存在と，既約元が素元であることを示せば十分．R の 0 でも単元でもない元 a_0 が既約分解を持たないとする．このとき a_0 自身既約でないので，分解 $a=bc$ と b も c 単元でないが存在して, しかも b と c のどちらかは既約分解を持たない．その既約分解を持たない方を a_1 とすると，$(a_0)\subsetneq(a_1)$. このような操作を繰り返すとイデアルの無限列

$$(a)\subsetneq(a_1)\subsetneq(a_2)\subsetneq(a_3)\cdots$$

が得られる．このとき，$\tilde{I}=\cup_{i=0}^{\infty}$ とおくと $\tilde{I}$ はイデアルであり，仮定より $b\in R$ が存在し $\tilde{I}=(b)$ となる．しかし b はある i に対して $b\in(a_i)$ であるから，$\tilde{I}=(a_i)=(a_{i+1})=\cdots$ が成り立ち，これは $(a_i)\subsetneq(a_{i+1})$ に矛盾． □

第 10 章

体とガロア理論

（第十三回・1/31）

代数学の金字塔.

定義 10.0.1 (標数)**.** 可換環 R とその乗法の単位元 e において $n \cdot e = e + \cdots + e = 0$ となる最小の自然数 n のことを**標数**といい，$\mathrm{char}(R)$ で表す．そのような n が存在しないときは標数は 0 と定義する.

例.
(1) $\mathrm{char}(\mathbb{Z}) = 0, \mathrm{char}(\mathbb{Z}_m) = m$.
(2) $\mathrm{char} = n$ のとき，$m \cdot e = 0 \iff m$ は n の倍数.

10.1 体の拡大（♣）

定義 10.1.1 (拡大体と中間体)**.**
- 体 E の部分集合 F が E と同じ演算で体になるとき，F を E の**部分体**, E を F の**拡大体**であるといい，E/F で表す.
- E の部分体であり F の拡大体であるような体 K を**中間体**という.

定義 10.1.2 (単純拡大と原始元)**.** E を体, F を E の部分体とする.

- E の部分集合 S をとり，F と S を含む最小の部分体を F **に** S **を添加した体**と呼び，$F(S) \subset E$ で表す.
- $E = F(a_1, \ldots, a_n)$ となる $a_1, \ldots, a_n \in E$ が存在するとき，E は F 上**有限生成**であるという.
- 特に $E = F(a)$ となる $a \in E$ が存在するとき，E は F 上**単純拡大**であるといい，a を拡大 $F(a)$ の**原始元**という.

定義 10.1.3 (有限次拡大と無限次拡大)**.** 拡大体 E/F において，E は F 上のベクトル空間とみることができる.

- E が F 上のベクトル空間として有限次元であるとき，E/F は**有限次拡大**であるという．その次元を**拡大次数**といい，$[E : F]$ で表す．また，E/F のベクトル空間としての基底を E **の** F **上の基底**という.
- E が F 上のベクトル空間として有限次元でないとき，E/F は**無限次拡大**であるといい，$[E : F] = \infty$ で表す.

例.　(1) 複素数体 $\mathbb{C}$ は実数体 $\mathbb{R}$ 上の有限拡大で，$[\mathbb{C},\mathbb{R}]=2$ となる．例えば $\{1, i=\sqrt{-1}\}$ は $\mathbb{C}$ の $\mathbb{R}$ 上の基底をなす．
(2) 実数体 $\mathbb{R}$ は有理数体 $\mathbb{Q}$ 上の無限次拡大である．

酒井 p107, 定理 4.24

定理 10.1.4. F を標数 0 の体とする．F の任意の有限次拡大 E は単純拡大である．

練習 51. $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$ を示せ．

定義 10.1.5.
– 拡大体 E/F において，E の元 α を根にもつような F 係数の多項式が存在するとき，α は F 上**代数的**であるという．また，そのような多項式が存在しないとき，α は F 上**超越的**であるという．
– E のすべての元が F 上代数的であるとき，E/F は**代数拡大**であるという．

例. 複素数体 $\mathbb{C}$ は実数体 $\mathbb{R}$ 上の代数拡大であるが，実数体 $\mathbb{R}$ は有理数体 $\mathbb{Q}$ 上の代数拡大でない．

定義 10.1.6 (最小多項式)**.** 拡大体 E/F において，E の元 α が F 上代数的であるとき，α を根にもつ F 上の多項式の中で次数が最小なものを，α の**最小多項式**という．最小多項式は F の定数倍を除いて一意的に定まり，F 上既約である．最小多項式の次数を α の F 上の**次数**と呼ぶ．

例. 虚数単位 $i=\sqrt{-1}$ は，実数体 $\mathbb{R}$ 上の既約多項式 x^2+1 の根である．従って i は $\mathbb{R}$ 上 2 次の代数的元であり，x^2+1 が i の最小多項式である．

10.2　代数学の基本定理と分解体（♣）

酒井 p103-

実はここから全ての根が K の元であることが従う

定義 10.2.1. 体 K 上の任意の定数でない任意の多項式 $f(x)\in K[x]$ が K 内に少なくとも一つの根をもつとき，K は**代数的閉体**という．

定理 10.2.2 (代数学の基本定理)**.** 複素数体 $\mathbb{C}$ は代数的閉体である．

一般に代数的閉体とは限らない体 K の多項式の根を考察するときは，次のような，「多項式の根を含む最小の拡大体」を考える．

定義 10.2.3. 多項式 $f(x)\in K[x]$ に対して，次の性質を満たす K の拡大体 L を $f(x)$ の**分解体**という．

(1) $L[x]$ において $f(x)$ は一次式に分解する．つまり $f(x)=a\prod_{i=1}^{n}(x-\alpha_i)$.
(2) $L=K(\alpha_1,\ldots,\alpha_n)$.

定義 10.2.4. 次の性質を満たす体 K の拡大体 L を K の**代数的閉包**という．

(1) L は代数的閉体である．
(2) $L\supset K$ は代数拡大である．

定義 10.2.5. 体 K の拡大体 L,L' に体の同型写像 $\sigma\colon L\to L'$ が存在し，かつその K への制限が恒等写像になるとき ($\sigma|_K=\mathrm{id}_K$)，σ を K**-同型写像**という．このような K-同型写像が存在するとき L と L' は K**-同型**という．

定理 10.2.6. 多項式 $f(x) \in K[x]$ の分解体や K の代数的閉包は K-同型を除いて一意的に存在する.

なにかが存在してそれが一意的であるというのは数学でよく出てくる大事な考え方.

10.3 ガロア群（♣）

酒井 p108-

定義 10.3.1 (ガロア群). K を体, L を K の代数的拡大とする.

- L の自己同型写像 $\sigma\colon L \to L$ が K-同型写像になるとき，σ を L の K-**自己同型写像**という.
- L の K-自己同型写像全体は，合成で積を入れることにより群になる．この群を拡大 $L \supset K$ の**ガロア群**と呼び，$\mathrm{Gal}(L/K)$ で表す.

どの定義を定理環境に入れてどれを平文に入れるかを考えて分けたほうが解りやすい資料になるのかな？（いまさら）

練習 52. (1) 複素数体 $\mathbb{C}$ の複素共役写像 $\sigma\colon z \to \bar{z}$ を考える．このとき $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{1, \sigma\}$ となることを示せ.
ヒント：$\phi \in \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ をとると，$\phi(i)^2 = \phi(i^2) = \phi(-1) = -1$. つまり $\phi(i)$ は i もしくは $-i$.

(2) $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ を求めよ.

定義 10.3.2 (ガロア拡大).

- 体 L の自己同型群の部分群 G に対して, G のすべての元で動かないような L の元の集合を L の G による**固定体**と呼び, L^G で表す. すなわち

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

- K を体, L を K の代数的拡大とする．$L^{\mathrm{Gal}(L/K)} = K$ となるとき L は**ガロア拡大**と呼ばれる.

例. (1) $\mathbb{C} \supset \mathbb{R}$ はガロア拡大.
(2) $\mathbb{Q}(\sqrt[3]{2})$ はガロア拡大ではない.

$\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{1\}$ になって $\sqrt[3]{2}$ も固定される.

定理 10.3.3 (ガロア拡大と分解体). K を標数 0 の体, L を K の代数的拡大とする．次の条件は同値である.

(i) L を K のガロア拡大である.
(ii) $|\mathrm{Gal}(L/K)| = [L : K]$
(iii) L はある多項式 $f(x) \in K[x]$ の K 上の分解体である.

定理 10.3.4 (ガロア理論の基本定理). K を標数 0 の体, L を K の有限ガロア拡大（有限次拡大かつガロア拡大）とする．このとき，$L \supset K$ の中間体 M とガロア群 $\mathrm{Gal}(L/K)$ の部分群 H とは次の全単射写像で一対一に対応する.

$$\phi\colon M \mapsto \mathrm{Gal}(L/M),$$
$$\psi\colon H \mapsto L^H.$$

さらに, 拡大 $M \supset K$ がガロア拡大であるための必要十分条件は $\mathrm{Gal}(L/M)$ が $\mathrm{Gal}(L/K)$

の正規部分群になることであり，このとき群の同型

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

が従う．

定義 10.3.5. K を標数 0 の体, $f(x)$ を K 上の多項式とする．L を $f(x)$ の K 上の分解体とするとき，ガロア群 $\mathrm{Gal}(L/K)$ を K 上の**多項式 f のガロア群**と呼び，$\mathrm{Gal}_K(f)$ と書く．

10.4　代数方程式（♣）

酒井 p132-, 石田 p169-

横井/硲野 p208-

定義 10.4.1 (方程式の解の公式とは)**.** 標数 0 の体 F の元を係数とする多項式

$$f(x) = a_0 + a_1x^1 + \cdots + a_{n-1}x^{n-1} + a_nx^n$$

に対して，代数方程式 $f(x) = 0$ の根がすべて，方程式の係数 $a_0, \ldots, a_n$ から加減剰余とべき乗根を付け加える操作を有限回施すことによって書き表されるとき，方程式 $f(x)$ は**代数的に解ける**という．

例. 2 次方程式 $ax^2 + bx + c = 0$,$(a \neq 0)$ の解は

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

定義 10.4.2 (べき根拡大)**.** 標数 0 の体 K の拡大体 L に対して，中間体の列

$$K = L_0 \subset L_1 \subset \cdots \subset L_r = L,$$
$$L_{i+1} = L_i(\alpha_i) \quad (\alpha_i^{n_i} \in L_i, 0 \leq i \leq r-1)$$

が存在するとき，L を K の**べき根拡大**という．

定理 10.4.3. K 係数の代数方程式 $f(x) = 0$ が代数的に解ける．$\iff$ $f(x)$ の K 上の最小分解体が K のべき根拡大である．

定理 10.4.4. K 係数の代数方程式 $f(x) = 0$ が代数的に解ける．$\iff$ $f(x)$ の K 上のガロア群が可解群になる．

定義 10.4.5 (一般多項式)**.** 標数 0 の体 K に n 個の独立変数 $x_1, \ldots, x_n$ を添加して得られる体を $L = K(x_1, \ldots, x_n)$ とするとき，L 係数の方程式

$$g(X) = X^n - x_1X^{n-1} + \cdots + (-1)^n x_n = 0$$

を n 次の一般多項式という．

定理 10.4.6. n 次の一般方程式のガロア群は，n 次の対称群 S_n に同型である．

定理 10.4.7. n 次の一般方程式が代数的に解けるためには $n \leq 4$ であることが必要十分である．

10.5　円分多項式（♢）

定義 10.5.1.　– 自然数 m に対して，多項式 x^m-1 の根を 1 **の** m **乗根**という．1 の m 乗根全体は，乗法に関して位数 m の巡回群をなす．
– 1 の m 乗根全体のなす巡回群における生成元を 1 **の原始** m **乗根**という．
– 1 の原始 m 乗根 ζ_m を根とする多項式

$$\Phi_m(x)=\prod_{\zeta_m}(x-\zeta_m)$$

を**円分多項式**という．

定理 10.5.2. $\varphi(m)$ をオイラー関数とする．1 の原始 m 乗根は $\varphi(m)$ 個存在し，円分多項式 $\Phi(m)$ は $\varphi(m)$ 次の多項式である．

定理 10.5.3. $\mu(d)$ をメビウス関数とするとき，次が成り立つ．

$$\Phi(m)=\prod_{d|m}(x^{m/d}-1)^{\mu(d)}.$$

定理 10.5.4. 体 F の標数が 0 のとき，任意の自然数 $m>1$ に対して，円分多項式 $\Phi(m)$ は有理数体 $\mathbb{Q}$ 上既約である．

定義 10.5.5. 体 F 上の x^m-1 の最小分解体 $F(\zeta_m)$ を F 上の m 次の**円分体**という．

定理 10.5.6. 1 の原始 m 乗根 ζ_m に対して次が成り立つ．

$$[\mathbb{Q}(\zeta_m):\mathbb{Q}]=\varphi(m).$$

このとき $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})\cong\mathbb{Z}_m^\times$ となる．

系 10.5.7. 任意の自然数 m について 1 の原始 m 乗根はべき根によって解ける．

$\mathbb{Z}_n^\times$ は可換群より可解群であるから