目次

第 1 章

Group

- 測度が面積・確率の代数構造の抽出，多様体が座標の代数構造の抽出だとしたら，群は対称性の代数構造の抽出である．これは**可逆**な射ということである．ということで，群は作用（外算法）を中心に捉え，その内算法でさえ作用として捉えるのが良い．これは表現論の考え方に繋がる．
- **内算法 $G \times G \to G$ も作用と捉える視点**が肝要となる．これは currying とも呼ばれるが，ともかく直積空間ではなく同型群という関数空間を考えるのである．射が大事だという圏論的世界観で駆動するのが代数学である．
- すると，**部分群 H とは，H 自体が，左移動による H の G への作用 $H \times G \to G$ による H-軌道そのものになる場合**：$x \in H$ を上手くとれば $Hx = H$ となる，すなわち，任意の $a, b \in H$ に対して $a \in Hb \Leftrightarrow ab^{-1} \in H$ となることをいう．巡回群とは，「x を含む最小の部分群が G である」を満たす $x \in G$ が存在する群，すなわち，1 つの元からの作用 $\{x\} \times G \to G$ による $\{x\}$-軌道がすでに G 全体となるような群のことである．[†1]
- 部分群 H の左移動による作用 $H \times G \to G$ による軌道分解を剰余類という．これは，$|G| = |H\backslash G||H|$ を満たす 1.5.5. 各軌道の代表元 x に対して，H の各元を掛ける行為は，必ず違う結果を生む（群の可逆性）ので，各軌道は H と同じ個数だけある．これはまるで絶対値の性質である：$\left|\dfrac{G}{H}\right| = \dfrac{|G|}{|H|}$．ちなみに $|GH| = \dfrac{|G||H|}{|G \cap H|}$ も成り立つ．軌道を考えそう 1.7.3.
- こうして，「差を考える」ことの肝心性を，「作用」という言葉で捉えることができた．「差が H に入る」とは「同じ H-軌道に属する」ことをいうのである：$ab^{-1} \in H \Leftrightarrow a \in Hb \Leftrightarrow Ha = Hb$．**イデアルにも共通する HN などの記法は，暗黙のうちに作用を考えていたのである．**
- 各軌道 Gx は，$G/\mathrm{Stab}_G(x)$ と一対一対応する 1.5.9．x を動かさない移動を定める元が $\mathrm{Stab}_G(x)$ とあるなら，x を g と同様に動かすものは $g\mathrm{Stab}_G(x)$ だけあるためである（$g\mathrm{Stab}_G(x)$ の元は x に対する恒等変換と $g\cdot$ との合成なので結局 g 移動）．こうして，X の様子を調べる代わりに G の様子を調べれば良い．群論の結果でさえこのスキームの下にまとまる．結局はこのスキームの下で，Lagrange の定理は左移動による作用についての結果で，Sylow の定理も共役作用による結果である．
- 正則表現とは群の演算が定める作用が定める表現であるが（左移動が定めるのが左正則表現という），これは軌道がただ一つで安定化群が自明な集合上の表現として特徴付けられる[†2]．$\mathrm{Ad} : G \to \mathrm{Aut}_{\mathrm{Grp}}(G) \subset \mathrm{Aut}_{\mathrm{Set}}(G)$ と定まるのもこの場合のみだろうか．
- 中心とは左移動と右移動の合成 $\mathrm{Ad} : G \to \mathrm{Aut}(G)$ の核である．左移動と右移動だけは特別な作用で，これを 1 つにまとめた双関手的な対象が共役写像である．「迂回道がもとの道と可換か？」という問題を Adjunction というのであった．共役作用の安定化群は特に中心化群という，部分群 $\mathrm{Stab}_G(x)$ の中では x は中心となる．共役作用の定める軌道分解は共役類分解といい，各共役類の位数は中心化群の位数からわかる．**中心化群は，x と可換な元を集めた集合なので，機械的な計算で決定できる**．この手続きにしたがって，計算して得る，群の位数の共役類分解についての等式を類等式と言う．
- 類等式の考え方より，p 群の中心が自明でないことがわかる．中心の各元は単独で共役類をなす（Ad についての軌道が一見集合）から，類等式は $|G| = |Z(G)| + (p \text{ の倍数})$ という形になる．したがって，$|Z(G)| \neq 1$ である（$Z(G)$ は G の正規（特に特性）部分群であるから，位数は p の倍数である）．

[†1] 単項イデアルみたいな

[†2] https://ja.wikipedia.org/wiki/正則表現_(数学)

- 部分群のうち，共役類でもあるようなもの：$\mathrm{Ad}(G)(N) = \cup_{g\in G} gNg^{-1} = N$ を正規部分群という．この時，共役類の間に自然に演算が持ち上がる．こうして商群が定義できる．
- 部分群の正規性はコンパクト性に似ていて，核と像の両方について保たれ，商について全単射を保った対応 π^*, π_* が存在する．この点はイデアルと同様である．
- Abel 群ではない群のうち，次に扱いやすいクラスは半直積の概念で捉えられる．半直積とは，部分群 $H \subset G$ に対する系統だった可換性の破れ $\forall_{g\in G}\ hg = \varphi(g)h$ を射 $\varphi : H \to \mathrm{Aut}_{\mathrm{Set}}(G)$ として捉えることで，直積の一般化された構造 $G \rtimes_\varphi H$ を捉える概念である．これは中心拡大の例になっている．例えば，一般の対称群は $S_n = A_n \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$ で，$\varphi_\tau(\sigma) = \sigma^{n-1}$.
- ここで半直積の手法をさらに一般化することで，組成列の概念を得る（この考え方は filtration にも通じる）．こうして正規部分群から完全列へと対象が移り，Abel 圏の概念へと向かう．すると，有限群には必ず組成列が存在し，その長さは不変量で (Jordan-Hölder の定理 1.11.15)，群に「次元」の概念の萌芽が与えられる（この手法は一般の Abel 圏で通用する）．こうして対称群が明快に掴める視座まで到達する 1.11.16.
- 同様の正規鎖を用いた手法の変種を考えると，隣同士が単純群だと「部分群の構造を解明する」ための組成列の概念を得るが，隣同士を Abel 群とすると「方程式の可解性を解明する可解群」というクラスを考えられる．すると，S_n は $n \leqslant 4$ のとき可解（組成因子が全て Abel 群からなる）で，$n \geqslant 5$ のとき可解でない．
- ここで半直積の考え方に「差を捉える方法」を復活させて融合させる．$ab(ba)^{-1}$ がどんな群に入るかを見るのである．すなわち，$ab = aba^{-1}b^{-1}ba = [a,b]ba$ となるので，半直積の $\varphi : H \times G \to G$ を一般化した事になる．導来群＝交換子部分群は正規どころか特性になる．これも確実に作用的な見方があるだろうがさらに深淵で，$G^{\mathrm{Ab}} = G/[G,G]$ は G の部分群で Abel であるようなもので最大なものになる（普遍性）．この方法を使えば，導来列が有限停止するという可解群の特徴付けを得る．
- Abel 化は忘却関手 $\mathrm{Ab} \to \mathrm{Grp}$ の随伴関手となる．自由群が忘却関手 $\mathrm{Grp} \to \mathrm{Set}$ の随伴関手となるように．
- 可解群とは Abel 群の有限回の拡大によって作れる群のことをいうと捉えたら，それが特に中心拡大によるとき（自明群から初めて，拡大として G_i を挿入すると，これが出来上がった群の中で中心になる[†3]），特に冪零群という．正規鎖 (G_i) があって，どこで切っても $G_i/G_{i+1} \leqslant Z(G/G_{i+1})$ と中心に入っている「(階層さえ守れば) ほとんどアーベル群」をいう．すると p 群はここで捕まえることができる．
- すると，「中心」とは，「他の G の元全てとの可換性」だから，可解群の導来群の概念をさらに強く用いて定義される降中心列 $C^n(G) = [G, C^{n-1}(G)]$ が有限停止することとして特徴付けられる．
- Sylow の定理は本当に綺麗な消息で，群の位数の素因数分解から，群の骨格だけは定まる．その上，p-Sylow 部分群の集合への G の共役作用を考えることで，その個数についても概ね確定する．

1.1　群の圏

1.1.1　内部群

Group を Internalization の言葉で，一般の圏（ただし有限積を持つもの[a]）で定義する．群の特徴は，対合 $\mathrm{inv} : G \to G$ である．そもそも元として対消滅する組 (g, g^{-1}) を定めた時点で対合的な概念をうみ，これが対称性としての意味論に的確であり，群論独自の幾何学が始まる．[b]

[a] Any category with finite products can be considered as a cartesian monoidal category (as long as we have either (1) a specified product for each pair of objects, (2) a global axiom of choice, or (3) we allow the monoidal product to be an anafunctor).https://ncatlab.org/nlab/show/cartesian+monoidal+category

[b] 部分群の特徴付け

定義 1.1.1 (group object).

[†3] 後から中心拡大されて入ってきた群はさらに大きな群の中で中心になるので，昔の中心も中心のままであることに注意．

(1) 有限積を備えた圏 C について，次の 3 図式を可換にする対象 G と射 $\mathrm{mult}: G\times G\to G$, $\mathrm{inv}: G\to G$, $\mathrm{id}: 1\to G$ の組

$$\begin{array}{ccccc} G\times G & \xrightarrow{\mathrm{mult}} & G & \xleftarrow{\mathrm{inv}} & G \\ & & \uparrow{\scriptstyle \mathrm{id}} & & \\ & & 1 & & \end{array}$$

を**群対象**という．

$$\begin{array}{ccc} G\times G\times G & \xrightarrow{\mathrm{id}_{G\times G}\times \mathrm{mult}} & G\times G \\ {\scriptstyle \mathrm{mult}\times \mathrm{id}_{G\times G}}\downarrow & & \downarrow{\scriptstyle \mathrm{mult}} \\ G\times G & \xrightarrow[\mathrm{mult}]{} & G \end{array} \qquad \begin{array}{ccccc} G\times G & \xleftarrow{(\mathrm{id}_G,\mathrm{id}!)} & G & \xrightarrow{(\mathrm{id}!,\mathrm{id}_G)} & G\times G \\ & {\scriptstyle \mathrm{mult}}\searrow & \downarrow{\scriptstyle \mathrm{id}_G} & \swarrow{\scriptstyle \mathrm{mult}} & \\ & & G & & \end{array} \qquad \begin{array}{ccccc} G\times G & \xleftarrow{\Delta} & G & \xrightarrow{\Delta} & G\times G \\ {\scriptstyle \mathrm{id}_G\times \mathrm{inv}}\downarrow & & \downarrow{\scriptstyle \mathrm{id}!} & & \downarrow{\scriptstyle \mathrm{inv}\times \mathrm{id}_G} \\ G\times G & \xrightarrow{\mathrm{mult}} & G & \xleftarrow{\mathrm{mult}} & G\times G \end{array}$$

ただし，$\mathrm{id}! = \mathrm{id}\circ ! : G\to G$ とし，$\Delta = (\mathrm{id}_G, \mathrm{id}_G)$ を対角射とした．

(2) これは，反変関手 $F: C^{\mathrm{op}}\to \mathrm{Grp}$ であって，台関手 $C^{\mathrm{op}}\to \mathrm{Set}$ が表現可能であるようなものに他ならない．[†4]

注 1.1.2. このように，対角射が必要であるから，monoidal 圏の doctrine には群対象が存在するとは限らない．

定義 1.1.3 (group, Lie group, topological group, Hopf algebra).

(1) 集合の圏 Set 内の群対象を**群**という．
(2) 滑らかな多様体の圏 Diff 内の群対象を **Lie 群**という．
(3) 位相空間の圏 Top 内の群対象を**連続群**という．
(4) 可換代数の反対圏 $\mathrm{CAlg}^{\mathrm{op}}$ 内の群対象を **Hopf 代数**という．

定義 1.1.4 (monoid, semigroup, loop, quasigroup, magma, groupoid). 群 $G = (G, \mathrm{mult}, \mathrm{id}, \mathrm{inv})$ について，[†5]

(1) 射 $\mathrm{inv}: G\to G$ を除くと，これを**単系**という．さらに $\mathrm{id}: 1\to G$ の構造を除くと**半群**（結合的なマグマ）という．
(2) $\mathrm{mult}: G\times G\to G$ 結合性の条件を除くと，これを**ループ**という．さらに $\mathrm{id}: 1\to G$ の構造を除くと**擬群**という．即ち，全ての元が可逆なマグマであり，単位元が存在すればループという．
(3) 全てを除いた構造 $G = (G, \mathrm{mult})$ を，**マグマ**または二項代数系という．
(4) mult を部分写像であることを認め，小さい圏であって全ての射が可逆であるものを**亜群**という．[†6]
(5) 群 G を，一点のみを持つ groupoid $\mathcal{B}G$ だと思うことを，Homotopy theory から delooping of a group to groupoid という．

1.1.2　群の射の性質

定義 1.1.5 (group homomorphism). 写像 $f: G\to H$ であって，$\forall_{x,y\in G}\, f(x\cdot y) = f(x)\cdot f(y)$ を満たすものを群準同型という．

命題 1.1.6 (演算を保つなら単位元と逆元も保つ). $f: G\to H$ を群準同型とする．

(1) $f(e) = e'$.
(2) $f(g^{-1}) = f(g)^{-1}$.
(3) 群準同型の合成は群準同型である．

[証明].

(1) $f(1) = f(1\cdot 1) = f(1)\cdot f(1)$ である．$f(1)\in H$ の逆元 $f(1)^{-1}$ を両辺に左から掛けて，

$$1 = f(1)^{-1}(f(1)f(1)) = (f(1)^{-1}f(1))f(1) = 1\cdot f(1) = f(1).$$

[†4] 全ての公理が F から生成されるから，logic の用語では F を指標 (signature) と呼ぶ．
[†5] このような概念群を考察する試みは centipede mathematics という．Centipede mathematics in the context of foundations is often called reverse mathematics. From Mathematical Apocrypha Redux: 'You take a centipede and pull off ninety-nine of its legs and see what it can do.' 良い圏を作るのがアーベル群で，アーベル圏をなし，cohomology が展開できるが，一般の群でも何とかなる．表現としてはモノイド作用で十分でこれが代数を作るが loop だとダメである．
[†6] この観点から見れば，群とは，pointed な単一対象亜群のことである．pointed object とは，対象 X と X-値点 $!: 1\to X$ との組をいう．

(2) $1 = f(1) = f(gg^{-1}) = f(g)f(g^{-1})$ である．$f(g) \in H$ の逆元 $f(g)^{-1}$ を両辺に左から掛けて，

$$f(g)^{-1} = f(g^{-1}).$$

■

命題 1.1.7．群の射 $f : G \to G'$ が可逆であるためには，f が全単射であることが必要十分である．

[証明]．群の射 $f : G \to G'$ の逆写像 $f' : G' \to G$ が群準同型であることを示せば良い．任意の $g', h' \in G'$ について，$f(g) = g', f(h) = h'$ を満たす $h, g \in G$ が存在し，$f(gh) = f(g)f(h) = g'h'$ より，$gh = f'(g)f'(h) = f'(g'h')$. ■

命題 1.1.8 (単射性の特徴付け)．$f : G \to G'$ が単射であることと，$\mathrm{Ker}\, f = \{e\}$ であることは同値である．

[証明]．

$\Rightarrow$　$\mathrm{Ker} \neq \{e\}$ とすると，$\{e\} \subsetneq \mathrm{Ker}\, f$ である．相異なる 2 元 $x, y \in \mathrm{Ker}\, f$ について，$f(x) = f(y) = e$ が従うので単射性に矛盾．

$\Leftrightarrow$　$f(x) = f(y)$ を満たす $x \neq y \in G$ が存在するとすると，$xy^{-1} \neq e$ である．これについて $f(xy^{-1}) = f(x)f(y)^{-1} = f(y)f(y)^{-1} = e$ より，$\mathrm{Ker}\, f = \{e\}$ に矛盾．

■

1.1.3　balanced

Grp は[a]．$\mathrm{Ab} \simeq \mathrm{Mod}_{\mathbb{Z}}$.

[a] https://ncatlab.org/nlab/show/Grp

命題 1.1.9．任意のモノ射は等化子である．

系 1.1.10．任意の epic mono は可逆である．

系 1.1.11．任意のエピ射は余等化子である．

1.2　群の例

- 強い可逆性：群の集合論的使用感の特徴は，mult と inv の組み合わせにより，自由に「移項」出来る点にある．mult, inv が Set で奏でる協奏曲は部分群の特徴づけ（命題 1.3.4）などで現れ，特に作用が軌道分解を定める直接の理由になっている．
- 可逆性とそれの高階化による弱化が代数学の道具だと思えば，category と groupoid が 2 つの基本的な概念の両極であることが容易に想像がつく．モノイドと群はその退化した形である．
- pointed category：Grp, Ab, Vect（いずれもアーベル圏）には零対象 0 が存在する．ただの終対象 1 があるならば，それは global point として使えるが，その役割は $\mathbb{Z}$ が担い，[a]実際 Ring では 2 つは分離し，$\mathbb{Z}$ は始対象，零環 0 が終対象となる．

[a] この場合 $\mathbb{Z}$ は終対象ではないので，global point という用語法は nLab では避けるように言われている．

1.2.1　より大きな代数的構造の単位として

より高級な代数系では，剰余を取る際に正規部分群だとかの議論が必要ないことも多い．

例 1.2.1 (環の部分代数：addiitive group, group of unit).

(1) 環 R は加法について可換群になる．これを**体の加法群**と呼ぶ．
(2) $R\backslash\{0\}$ は乗法について可換群である．これを**体の乗法群**と呼び，$(R\backslash\{0\},\cdot)=R^\times$ または $\mathrm{GL}_1(R)$ と表す．
(3) 一般に単元＝可逆元のみを選び出すことによって，環から乗法群を抽出できる：$^\times:\mathrm{Ring}\to\mathrm{Grp}$.

□

例 1.2.2 (整数環の部分群)**.** 整数環の部分群は特徴付けられる 1.3.16. □

1.2.2　有限群

例 1.2.3 (zero object)**.** 自明群 $\{e\}=\mathbb{Z}_1=\mathcal{F}_1=1$ は零対象である．[†7]アーベル群の圏，環上の加群の圏，体上の線型空間の圏と同様の消息である．終対象であるだけでなく，始対象である，その理由はただ一つの射 $e:\{e\}\to G$ が出るからである． □

例 1.2.4 (cyclic group)**.** 一番単純な対象が巡回群で，簡明な分類ができる（定理 1.7.7）． □

例 1.2.5. 有限群の分類は，位数によっては Abel 群の構造定理を用いてできるが，少し技巧的 1.9.20．または Sylow の定理によっても出来る．p,q を $p<q$ かつ $q\not\equiv 1 \mod p$ を満たす素数とする．このとき，位数 pq の群（15, 33 など）G は $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z}$ と同型な Abel 群である（命題 1.13.9）．位数 $2p$ の群 G は次のいずれかである（命題 1.13.10）．

(1) 巡回群 $G\simeq\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\simeq\mathbb{Z}/2p\mathbb{Z}$.
(2) 二面体群 $G\simeq D_p$.

□

例 1.2.6 (the group of order two)**.** 位数 2 の群は同型を除いて一意である． 2 倍写像 $\cdot 2:\mathbb{Z}\to\mathbb{Z}$ の余核（像による商）であるため，$\mathbb{Z}/2\mathbb{Z}$ と表す．$\mathcal{F}_2$ とも表す． □

例 1.2.7 (the groups of order four)**.** 位数 4 の群は，巡回群 $C_4=\mathbb{Z}/4\mathbb{Z}$ と，Klein 群 1.4.12$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ の 2 つである．Klein の 4 群の直積による表示は $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$1.10.10 となる．これは 2 次元の $\mathbb{F}_2$-線型空間とみなせるから，$\mathrm{Aut}(V)=M_2(\mathbb{F}_2)$．長方形の変換群など，作用としての理解もできる 1.4.12．これより，$S_4/V\simeq S_3$ も分かる． □

1.2.3　有限生成群：群の位数と捩れ

1.2.3.1　ねじれ群

ねじれ群は有限群の拡張概念であり，有限生成というクラスに繋がる．有限生成なねじれ群は有限群であるか？という問題は Burnside の問題と呼ばれ 1902 に提起された．これは 1964 に反例となる p-群が構成された．

定義 1.2.8 (order, torsion subgroup / periodic group, torsion-free).

(1) 群の位数：群の台集合の濃度を位数と呼ぶ．
(2) 元の位数：群の元 $g\in G$ について，$\exists_{n\in\mathbb{N}}\ g^n=e$ を満たす最小の自然数を**元の位数**という．位数が存在する元を位数有限，または捩れ元と呼び，位数が存在しない元を位数無限という．
(3) ある群 G の中で，位数有限な元は部分群 $T(G)$ をなす．これを**捩れ部分群**といい，これが自明である群をねじれがない群という．
(4) 任意の元が有限位数であるような群を一般に**捩れ群**または**周期群**と呼ぶ．
(5) ねじれ群は有限群とは限らないが，任意の有限群は捩れ群である．
(6) ねじれ群とその群準同型は群 Tor をなす．[†8]

注 1.2.9 (元の位数と群の位数)**.** 元の位数は内部自己同型によって保存される．なぜなら圏論的な不変量だからである．元の位数は

[†7] Abel 群として見た時の自明群は $0=\{0\}$ と書くこともある．
[†8] 基礎論の結果「アーベル群の言語 $\{+,-,0\}$ 上の有限個の閉論理式が全てのねじれがないアーベル群で正しければ，それらの閉論理式は，ねじれのあるアーベル群でも正しい．」

Ker $g : \mathbb{Z} \to G$ の位数を介して定義できる（命題 1.3.17）．n 次巡回群からの射を使えば，位数 n の元を観測できる（系 1.6.10）．

注 1.2.10 (Abel 圏でのねじれ群)**.** 特に Abel 群に対して，ねじれ部分群の対応 $T : \mathrm{Ab} \to \mathrm{Tor}$ は実は関手的である．また $T(G) \lhd G$ は特性部分群である．圏 Ab を捩れ群とねじれのない群とに分けて研究する理論を torsion theory と言う．

定義 1.2.11 (exponent). ねじれ群について，その元の位数の全ての最小公倍数を，存在すれば**冪数**という．

例 1.2.12 (非有限なねじれ群)**.** 群の全ての元は有限位数を持つが，群としては位数有限でない例がある．

(1) 回転群 $\mathbb{Q}/\mathbb{Z}$（例 1.7.2）．
(2) 有限体上の多項式の加法群．
(3) 全ての二面体群の合併．
(4) Prüfer の p-群（例 1.2.33）．

□

注 1.2.13. ねじれ群の興味深い性質の一つは、それが一階述語論理で定式化できないことである。

1.2.3.2　p-群

p-群と Abel 群が，群の分類で中心となる．p-群は捩れ群であるが，有限群とは限らない．

定義 1.2.14 (p-primary group / p-group / primary group).

(1) 群 G の任意の元 $g \in G$ が，位数 $p^{n(g)}$ を持つとき，これを **p-群**または **p-準素群**という．$n : G \to \mathbb{N}$ が有界とは限らないことに注意．
(2) 群 G が有限群であるとき，冪数が存在するから，群の位数 $|G|$ が p の冪であることと，G が p-群であることは同値．

要諦 1.2.15.

(1) 任意の有限 Abel 群は，その p-群の直和に分解できる（有限 Abel 群の構造定理 1.9.1）．これを p-準素成分／部分 (p-primary parts / components) などという．
(2) 任意の有限 p-群は，非自明な中心を持つ（命題 1.5.22）．
(3) したがって，次のように構成した p-群 G の昇中心列 $(Z^n(G))$ は G で有限停止するから，p-群は冪零である．
   (i) $Z^0(G) = \{e\}$.
   (ii) $\pi : G \twoheadrightarrow G/Z^{n-1}(G)$ について，$Z^n(G) := \pi^{-1}(Z(G/Z^{n-1}(G)))$．これを n 次の中心という．

注 1.2.16 (基本アーベル群)**.** 基本アーベル群 1.9.15 は p-群の特別な場合である．Klein の四元群は特別な位置を占め，位数 p^2 の Abel 群は $p = 2$ の場合と同じ要領で 2 つに分類できる 1.9.16.

1.2.4　対称群

対称群＝順序数の変換群

群の例のほとんどが，同型群であるが，集合の同型群を対称群といい，その部分群を置換群という．

例 1.2.17 (symmetric group, permutation group, cyclic permutation)**.**

(1) 集合 X に対し，$\mathrm{Aut}_{\mathrm{Set}}(X) =: \mathrm{Aut}(X)$ は群となる．この部分群を**置換群**という．
(2) $X = [n]$ の時，$\mathrm{Aut}([n])$ を n 次**対称群**と呼び，$\mathfrak{S}_n$ で表す．$n \geqslant 3$ において，可換でなく，中心は自明である．$m \geqslant 5$ において，可解でない．$S_n \simeq \mathrm{GL}_n(\mathcal{F}_1)$.
(3) 射 $\mathrm{sgn} : S_n \to \{\pm 1\}$ の核 A_n を n 次**交代群**と呼ぶ．これは対称群の交換子部分群に一致する 1.12.9．また，$[A_n, A_n] = A_n$ $(n \geqslant 5), [A_4, A_4] = V$.

(4) S_4, S_5 の 2-Sylow 部分群は位数 8 で，二面体群 D_4 である．
(5) S_n の元を交わりのない巡回置換の積に分解したとき，長さ l の巡回置換が現れる回数 k_l を用いて，組 $(k_1, \cdots, k_n)$ を**型**という．型は共役類を定める．

□

例 1.2.18 (S_3)**.** S_3 の表示 1.8.1：$\tau\sigma\tau = \sigma^2$．中心の様子 1.5.21．正規部分群 1.6.6．類等式 1.5.18．半直積による表示は $S_n \simeq A_n \rtimes C_2$1.10.7．二面体群に極めて似ているが，「ねじれ方」が違う．つまり，組成因子は同じ 1.11.16．A_n $(n \geqslant 5)$ は単純である 1.11.3．組成列は 1.11.9．□

例 1.2.19 (S_4)**.** $S_4/V \simeq S_3$ で，これは分裂し，$S_4 \simeq V \rtimes S_3$1.10.12．□

例 1.2.20 (平面の変換群：dihedral group)**.** 正 n 角形の頂点集合は

$$T_n := \left\{ \left(\cos\frac{2k\pi}{n}, \sin\frac{2k\pi}{n} \right) \in \mathbb{R}^2 \;\middle|\; k \in n \right\}$$

と表せる．

$$D_n := \{ g \in O_2(\mathbb{R}) \mid g(T_n) = T_n \}$$

を**二面体群**と言う．[†9]二面体群は S_n の部分群である 1.13.11．

(1) 回転 σ と鏡映 τ の 2 つへの標準分解が存在し，回転は巡回群 $C_n = \langle \sigma \rangle$ を作るから，$D_n = C_n + \tau C_n$ より，位数は $2n$ となる．
(2) これは典型的な半直積の例となっている：$D_{2n} = C_n \rtimes_\phi C_2$1.10.4．ただし，$\phi : C_2 \to \mathrm{Aut}(C_n)$ は，$\rho(1) = -^{-1}$ とする．
(3) 交換法則は $\tau\sigma = \sigma^{-1}\tau$ より，D_n の中心は n が奇数のとき自明で，n が偶数のときは $\sigma^{n/2}$ も含んだ位数 2 の部分群となる．

正多角形の中心を座標平面の原点に置けば、それを不変とする合同変換は線型写像と見なせる。これによって、D_n の各々の元は、行列で表すことができ、変換の合成は行列の積に対応する。これは、群の**忠実表現**の一例である。□

例 1.2.21 (立体の変換群：tetrahedral, octahedral, icosahedral group)**.** $T \subset \mathbb{R}^3$ を四面体とすると，$T := \{ g \in O_3(\mathbb{R}) \mid g(T) = T \}$ は四面体群である．同様にして，八面体群 O，二十面体群 I も定義できる．□

1.2.5　行列の群

やはり順序数の変換群と思うより，幾何学的対象の変換群と思う方が構造がわかる．

例 1.2.22 (general linear group)**.**

(1) $\mathrm{GL}_n(K)$ の元と K^n の基底は一対一に対応する．よって，$\mathrm{GL}_n(\mathcal{F}_p)$ の位数がわかる．
(2) $\mathrm{GL}_n(K) = \mathrm{SL}_n(K) \rtimes K^\times$．$[\mathrm{GL}_n(K), \mathrm{GL}_n(K)] = \mathrm{SL}_n(K)$ である 1.12.9．
(3) $Z(\mathrm{GL}_n(K)) \simeq K^\times$．

□

例 1.2.23 (Lie 群の例：orthogonal group, unitary group)**.**

(1) 行列 A の余因子行列を $\Delta(A)$ とすると，これは A の成分の多項式であるから，写像

$$\begin{array}{ccc} {}^{-1} : \mathrm{GL}(n,\mathbb{R}) & \longrightarrow & M(n,\mathbb{R}) \\ \cup & & \cup \\ A & \longmapsto & (\det A)^{-1}\Delta(A) \end{array}$$

は連続である．また転置 ${}^t : M(n,\mathbb{R}) \to M(n,\mathbb{R})$ も連続である．従って，直交群 $O(n,\mathbb{R}) := \{ A \in \mathrm{GL}(n,\mathbb{R}) \mid A^t A = 1 \}$ は $M(n,\mathbb{R})$-閉集合，特殊直交群 $SO(n,\mathbb{R}) := O(n,\mathbb{R}) \cap \mathrm{SL}(n,\mathbb{R})$ も $M(n,\mathbb{R})$-閉集合である．

[†9] Dynkin 図形と区別するために，nLab では D_{2n} と表される．

(2) $M(m,n;\mathbb{C}) \simeq \mathbb{C}^{mn}$ での標準内積は $\mathrm{Tr}({}^t X\overline{Y})$ と表せる．一般線型群は $M(n,\mathbb{C})$-開集合，特殊線型群は $M(n,\mathbb{C})$-閉集合である．ユニタリ群 $U(n) := \{A \in \mathrm{GL}(n,\mathbb{C}) \mid A^*A = 1\}$ も，特殊ユニタリ群 $SU(n) := U(n) \cap \mathrm{SL}(n,\mathbb{C})$ も $M(n,\mathbb{C})$-閉集合である．

□

例 1.2.24 (上三角行列の空間)**.** 可逆な上三角行列全体は部分 Lie 群をなす．半直積による表示は，(2,2)-行列の場合だと $G \simeq \mathbb{C} \rtimes_\phi (\mathbb{C}^\times \times \mathbb{C}^\times)$1.10.16．冪単な行列の集合 U が正規部分群をなし，あとは固有値について回転する．一般に，可逆な上三角行列の集合 B は，冪単行列がなす部分集合 U と対角行列 T を用いて $B = U \rtimes T$ と表せる 1.10.4．なお，U は $\mathrm{GL}_n(\mathbb{F}_p)$ の p-Sylow 部分群になる 1.13.3．また U は冪零度 $n-1$ の冪零群である 1.12.23．冪零度と Jordan 分解は絶対対応していると思うが，まだ見えない．□

例 1.2.25 (quaternion group)**.** 四元数群は，生成元 $1, i, j, k$ と関係式 $i^2 = j^2 = k^2 = ijk = -1$ が定める群である．この群を規定として生成される 4 次元の実線型空間の元を四元数 $\mathbb{H}$ という．これは斜体をなす．$\mathbb{R}$ を真の部分環に持つ斜体は $\mathbb{C}$ と $\mathbb{H}$ のみである (Frobenius の定理)．三次元球面 S^3 上に群構造を入れたものとみなせ，$\mathbb{H} \simeq \mathrm{SU}_2 \simeq S^3$ は $2D_4$ と同型．これらは general dicyclic groups の系列の一部である．$Z(Q_8) = \pm 1$．また，最小の非 Abel な p-群であり，冪零度 2 の冪零群である 1.12.23．□

例 1.2.26 (Klein group)**.** Klein の四元群 1.4.12 は，正方形でない長方形の変換群である．□

1.2.6　Lie 群

特に豊かな変換群が Lie 群である．Lie 群の作用の軌道・安定化群定理は等質空間の理論にあたる．

例 1.2.27 (affine 空間)**.** affine 変換群 $\mathrm{Aff}_n(\mathbb{R})$ は局所コンパクトで，n 次元空間 A^n の推移的な位相変換群である．原点 0 における等方部分群は $\mathrm{GL}_n(\mathbb{R})$ に等しいから，$\mathrm{Aff}_n(\mathbb{R})/\mathrm{GL}_n(\mathbb{R}) \simeq A^n$ が成り立つ．この分母を払うと，$\mathrm{Aff}_n(\mathbb{R}) \simeq A^n \rtimes \mathrm{GL}_n(\mathbb{R})$ の構造になっている 1.10.4．$\mathrm{Aff}(\mathbb{R}^n)$ の積は $(A_1, b_1) \cdot (A_2, b_2) = (A_1A_2, A_1b_2 + b_1)$ で定まるからである．□

例 1.2.28 (直交群の等質空間としての単位球面)**.** $O(n) \subset \mathrm{GL}_n(\mathbb{R})$ はコンパクト部分群である．列ベクトルの空間として，$U_1(0) \subset \mathbb{R}^n$ を n 次元開球とすると，$O(n) \subset \overline{(U_1(0))}^n$ より．ここで，$\|Ax\| = \|x\|$ を満たすから，$O(n)$ の作用は連続写像 $S^{n-1} \to S^{n-1}$ を誘導する．また，$O(n)$ は推移的に S^{n-1} に作用する．したがって，S^{n-1} は $O(n)$ の等質空間である．点 $e_1 \in S^{n-1}$ における等方部分群は

$$H := \left\{ \begin{pmatrix} 1 & 0 \\ 0 & B \end{pmatrix} \,\middle|\, B \in O(n-1) \right\}$$

より，軌道と安定化群との関係から，$O(n)/H \simeq O(n)/O(n-1) \simeq S^{n-1}$ である．

全く同様の議論で，$SO(n)/SO(n-1) \simeq S^{n-1}$ も成り立つ．

$SO(n)$ は $O(n)$ の正規部分群であるだけでなく，単位元を含む連結部分となる．□

1.2.7　対称群の分類

注 1.2.29 (ADE classification)**.** Dynkin 図形によって分類される．A は交代群，D は二面体群，E は多面体群である．

命題 1.2.30 .

(1) Klein の四元群について，$D_4 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.
(2) $D_6 \simeq S_3$.
(3) $T_4 \simeq S_4 \simeq O \cap \mathrm{SO}_3$.（向きを保つ四面体群の部分群）
(4) orientation-preserving な対称変換への制限 $T \cap \mathrm{SO}_3$ は A_4 に同型.

命題 1.2.31 (cycle decomposition)． 任意の置換 $\sigma \in S_n$ は巡回置換の積に分解できる．

[証明]． $[n]$ は σ-軌道に分解でき，それぞれの中での巡回置換を $\tau_1, \cdots, \tau_r$ とすると，$\sigma = \tau_1 \cdots \tau_r$ である．■

問 1.2.32. 全ての無限群は，無限の正規部分群を持つか？

反例 1.2.33 (Prüfer p-group)**.** **ブリューファー p 群**とは，次のように定義できる．

$$\mathbb{Z}(p^\infty) = \left\{ \exp\left(\frac{2\pi i m}{p^n}\right) \,\middle|\, n, m \in \mathbb{N} \right\}$$

または p 進数の加法群 $\mathbb{Q}_p$ と p 進整数からなる部分群 $\mathbb{Z}_p$ を用いて，$\mathbb{Z}(p^\infty) = \mathbb{Q}_p/\mathbb{Z}_p$ と表せる．この p^∞ 群または p 準巡回群の部分群は包含関係によって全順序づけられる唯一の無限群の系列である（素数 p の取り方だけ違う）．

反例 1.2.34 (Tarski Monster group)**.** Tarski Monster group は全ての部分群に対して素数 p が存在して位数 p の巡回群に同型になる無限群である．

1.2.8　群環

多項式環の拡張となるより構造豊かな加群を考える．R が体であるとき，これは線型空間になる．畳み込み積は，四元数のように，基底（G の元）同士にも演算が存在するような線型空間である．したがって代数の例である．

定義 1.2.35 (group ring / group algebra). 群 G と環 R について，群 R-代数，または，群環 $R[G]$ とは，G 上の自由 R-加群 $U(R[G]) = \mathrm{Hom}_{\mathrm{Set}}^{\text{fin supp}}(U(G), U(R))$ 上に，畳み込み積 (convolution product)

$$(f_1 * f_2)(g) = \sum_{h \in G} f_1(gh^{-1}) f_2(h) \qquad (g_1, g_2 : G \to R)$$

を定めたものである．

注 1.2.36. 基本的には $\{\chi_g : U(G) \to U(R)\}_{g \in G}$ を基底とした自由加群である．各元は写像 $r_{(-)} : U(G) \to U(R)$ とみなせる．groupoid algebra, category algebra として一般化される．Hopf 代数であり，graded algebra でもある，結合代数のクラスである．

1.2.9　群の構成

定義 1.2.37 (direct sum). アーベル群の族 $(M_\lambda)_{\lambda \in \Lambda}$ に対して，

$$\bigoplus_{\lambda \in \Lambda} M_\lambda = \{(m_\lambda)_{\lambda \in \Lambda} \mid m_\lambda = 0 \ \text{ f.e.}\}$$

に，$(m_\lambda)_{\lambda \in \Lambda} = (m'_\lambda)_{\lambda \in \Lambda} = (m_\lambda + m'_\lambda)_{\lambda \in \Lambda}$ によって加法を定義したものは Abel 群になる．

1.2.10　群の射の例

群の射あるところに準同型定理あり．

例 1.2.38 (行列式と特殊線型群)**.**

(1) 可換環 A に対して，$\det : \mathrm{GL}_n(A) \twoheadrightarrow A^\times$ は群の全射準同型である．
(2) $\mathrm{SL}_n(A) := \mathrm{Ker}\ \det$ である．
(3) 準同型定理より，$\mathrm{GL}_n(A)/\mathrm{SL}_n(A) \simeq A^*$ となる．$U(2)/SU(2) \simeq S^1$ はその制限なのかもしれない．

□

例 1.2.39 (置換の符号と交代群)**.** 置換の符号

$$\begin{array}{ccc} \mathrm{sgn} : S_n & \longrightarrow & \{\pm 1\} \\ \cup & & \cup \\ \sigma & \longmapsto & \displaystyle\prod_{1\leqslant i<j\leqslant n} \frac{\sigma(i)-\sigma(j)}{i-j} \end{array}$$

は次の群準同型 $P : S_n \to \mathrm{GL}_n(K)$ を用いて行列式で定義することができる.

(1)

$$\begin{array}{ccc} P : S_n & \longrightarrow & \mathrm{GL}_n(K) \\ \cup & & \cup \\ \sigma & \longmapsto & P(\sigma) := (e_{\sigma(1)} \cdots e_{\sigma(n)}) \end{array}$$

は単射な準同型である.

(2) K の標数が 2 でなければ，次の準同型 $\mathrm{sgn} : S_n \to \{\pm 1\}$ が引き起こされる.

$$\begin{array}{ccccc} S_n & \xrightarrow{P} & \mathrm{GL}_n(K) & \xrightarrow{\det} & K^\times \\ & \searrow^{\mathrm{sgn}} & & & \uparrow{\scriptstyle i} \\ & & & & \{\pm 1\} \end{array}$$

偶置換を集めた群 $A_n := \mathrm{Ker}\ \mathrm{sgn}$ を交代群という.[†10] よって $A_n \lhd S_n$. 準同型定理より，$S_n/A_n \simeq \{\pm 1\}$. □

例 1.2.40 (指数表示という群準同型)**.** 指数を帰納的に定める．次は群準同型である．像は巡回群 $\langle g \rangle$ である．この関手性を**指数法則**という.

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & G \\ \cup & & \cup \\ n & \longmapsto & g^n \end{array}$$

□

例 1.2.41 (対数という群準同型)**.** $\log : \mathbb{R}_{>0} \xrightarrow{\sim} \mathbb{R}$ は乗法群と加法群の間の同型を与えている. □

例 1.2.42 (回転という群準同型)**.**

$$\begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathrm{GL}_2(\mathbb{R}) \\ \cup & & \cup \\ t & \longmapsto & \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix} \end{array}$$

□

1.2.11　群の同型の例

内部自己同型が一番わからない．$G/Z(G)$ と同型であるようだ 1.5.20.

例 1.2.43 (inner automorphism：共役という標準的な自己同型)**.** 2 変数写像

$$\begin{array}{ccc} \mathrm{Ad} : G \times G & \longrightarrow & G \\ \cup & & \cup \\ (h, g) & \longmapsto & ghg^{-1} \end{array} \qquad \begin{array}{ccc} G & \longrightarrow & \mathrm{Aut}(G) \\ \cup & & \cup \\ g & \longmapsto & \mathrm{Ad}(g) \end{array}$$

[†10] Boole 代数みを感じる．環論も感じる.

の currying $\mathrm{Ad}(g) : G \to G$ は群同型であり，逆射は $\mathrm{Ad}(g^{-1})$ である．名前の由来は随伴 (adjunct) だからである．[†11]

$$\begin{array}{ccc} G & \xrightarrow{g} & G \\ {\scriptstyle h}\downarrow & & \downarrow{\scriptstyle h} \\ G & \xleftarrow{g^{-1}} & G \end{array}$$

自己同型のうち，共役として得られるもの $\mathrm{Im}\,\mathrm{Ad} =: I(G) \subset \mathrm{Aut}(G)$ を**内部自己同型**という．$\mathrm{Ker}\,\mathrm{Ad} \subset G$ は群の中心 $Z(G)$ である．よって $\mathrm{Ad} : G \twoheadrightarrow I(G) \hookrightarrow \mathrm{Aut}(G)$ についての準同型定理より，$G/Z(G) \simeq I(G)$ □

要諦 1.2.44 (内部自己同型とは，G の自己同型への埋め込み)**.** 群作用 $G \to \mathrm{Aut}(G)$ のうち，g^* と g_* を合わせたものが共役という考え方だ．Awodey では，ここから任意の圏はある具体圏と同型であるという証明をパラレルに描き出した．

1.2.12　Cayley の定理

半直積と同様，自己言及という構造

群論の目標は

(1) 全ての群を分類する．
(2) 全ての群の作用を分類する．群の作用は $G \to \mathrm{Aut}_{\_}(\Gamma)$ というときの $\_$ に入る圏の定め方，あるいは $\mathrm{Aut}_{\mathrm{Set}}(G)$ の部分群の定め方が肝となるが，特に，集合への作用である**置換表現**，そして線型空間への作用である**線型表現**である．[α]

群の公理が，対象の対称性を表しているかは応用者によるが，Cayley の定理が一つ別個の回答を与える．群は必ず自身の対称群の部分群となっている．こうして Grp は数学の中で欠かせない役割を担うことになる．
この証明は，左移動と右移動として知られる群作用の，線型表現である**正則表現**を構成することで行われる．これは群 G 上で自由生成された K-線型空間を考えることにあたる．

[α] これはグラフ理論で行列が出てくるような理由と同じであるか．

1.3　部分群

包含写像が定める構成

最も簡単な構成法は自身の内部を省みる，部分群である．これは群を定める 3 つの射が自然に部分射を定めるような包含写像 $H \to G$ を部分群という．部分作用 $\rho : H \times H \to G$ が $\mathrm{Im}\,\rho \subset H$ を満たすことと同値．

1.3.1　定義と特徴付け：部分作用という見方

mult と inv が Set で奏でる協奏曲：差が H に入ることが H を特徴付ける

$ab^{-1} \in H$ は mult, inv の閉性の両方を含意している．**同伴性**のように（注 2.8.13），差に注目する技法である．これは軌道の同値性 $aH = bH \iff ab^{-1} \in H$ 1.4.16 の特殊な場合である．そう，「差が等しい」とは同じ軌道に属することをいう．そして部分群 H とは，演算 $G \times G \to G$ を作用と捉えると，H が自分に作用することと捉えらえる．

記法 1.3.1 (部分群の積：実はこれは部分群のなす束の結びの演算となっている)**.** 群 G の部分集合 $S, T \subset G$ と元 $a, b \in S$ に対して，群を

$$ST = \{st \mid s \in S, t \in T\} \qquad S^{-1} = \{s^{-1} \mid s \in S\}$$

[†11] The process of currying is an instance of passage to adjuncts, specialized to the tensor-hom adjunction of a closed monoidal category. fiber にも見えるし，座標変換にも見える．これが可換になるとは，Abel 群ということでもある．

$$aS = \{ax \mid x \in S\}^{\dagger 12} \qquad Sb = \{xb \mid x \in S\} \qquad aSb = \{axb \mid x \in S\}$$

と定義する．また，帰納的に

$$S^0 = \{e\} \qquad S^{-1} = \{x^{-1} \mid x \in S\} \qquad S^{m+1} = S^m S$$

という記法も定める．

注 1.3.2 (coset group)**.** この記法は方程式的に使う時に重宝する．群の本質は方程式の解の一意性＝乗法 $\cdot : G \times G \to G$ の currying が全単射であることにある．$a^{-1}Na \subset N \Leftrightarrow N \subset aNa^{-1}$．すると，この構造上に群構造が入りそうである．これが剰余群である．

定義 1.3.3 (subgroup). 群 $(G, \cdot, e, {}^{-1})$ の部分集合 $H \subset G$ が部分群であるとは，

(1) $e \in H$,
(2) $\forall_{x,y \in G}\ xy \in H$,
(3) $\forall_{x \in G}\ x^{-1} \in H$,

を満たすことをいう．

$$\begin{array}{ccccc} G \times G & \xrightarrow{\text{mult}} & G & \xleftarrow{\text{inv}} & G \\ & & \uparrow{\scriptstyle \text{id}} & & \\ & & 1 & & \end{array}$$

命題 1.3.4 (部分群の特徴付け). G を群，$H \subset G$ を空でない部分集合とする．次の 3 条件は同値である．

(1) H は群である．
(2) $H^2 \subset H \wedge H^{-1} \subset H$.[†13]
(3) $H^{-1}H \subset H$.[†14]

[証明]. (1)⇒(2)⇒(3) は論理的帰結である．(3)⇒(1) を示す．群の演算の制限 $\cdot|_{H \times H}$ の値域が H に含まれること：$\forall_{a,b \in H}\ ab \in H$ を示せば良い．

1. $H \neq \varnothing$ より，$a \in H$ が取れる．
2. (3) より，$a^{-1}a = e \in H$ である．[†15]
3. (3) より，$a^{-1}e = a^{-1} \in H$ である．
4. 以上より，任意の $a, b \in H$ について，$a^{-1} \in H$ もわかったから，(3) より，$(a^{-1})^{-1}b = ab \in H$.

■

要諦 1.3.5 (internalization で考えると，今回示すべき事柄と群の公理のズレがわかりやすい)**.** 要は，群の公理のうち，射の性質に当たるものは今回は示す必要がなく，可換図式から射が誘導されるための条件のみを示せば良い．安定性：$\mathrm{Im}\,(\cdot|_{H \times H}) \subset H$ が成り立てば良い．具体的に言えば，結合性と単位元の中立性と存在，逆元の吸収性と存在のうち，前者は演算の閉性のみが大事で（じゃないと G を H に書き換えた図式に可換な射が引き起こされない），後 2 者は存在のみが大事である（これは $\mathrm{Im\ inv} \subset H, \mathrm{Im\ id} \subset H$ という閉性のことである）．図式の言葉で考えれば，全てが統一的に見れる．

系 1.3.6 (部分群の共通部分に関する閉性：実はこれは部分群のなす束についての交わりの演算となる). $H_1, H_2 \subset G$ を G の部分群とする．$H_1 \cap H_2$ も部分群である．

[証明]. 群の特徴付け（命題 1.3.4）より，任意の $a, b \in H_1 \cap H_2$ について，$a^{-1}b \in H_1 \cap H_2$ だから，$H_1 \cap H_2$ も群である．■

[†13] $\forall_{a,b \in H}\ (ab \in H) \wedge (a^{-1} \in H)$.
[†14] $\forall_{a,b \in H}\ a^{-1}b \in H$.
[†15] $a = e$ でも構わない．

1.3.2　生成と巡回群

1 元から生成される群を巡回群という．巡回群はアーベル群である．巡回群は結局，自由群 $\mathbb{Z}/n\mathbb{Z}$ $(n=0,1,2,\cdots)$ で尽くされる．

補題 1.3.7 (生成される群). 群 G の部分集合 $S\subset G$ に対して，S を含む最小の部分群が存在する．これを S **から生成される部分群**といい，$\langle S\rangle$ で表す．

[証明]. これは次のように構成される：$(G_\lambda)_{\lambda\in\Lambda}$ を S を含む G-部分群全体からなる族として，$\langle S\rangle=\bigcap_{\lambda\in\Lambda}G_\lambda$．また，$\langle S\rangle=\{s_1^{n_1}\cdots s_r^{n_r}\in G\mid a_i\in S,n_i\in\mathbb{Z},r\in\mathbb{N}_{>0},i\in[r]\}$ などがある． ■

補題 1.3.8 (1 元生成群が巡回群である). $g\in G$ に対し，$\langle g\rangle=\{g^n\in G\mid n\in\mathbb{Z}\}$．これを巡回群と呼ぶ．

[証明].

$\langle g\rangle$ 部分群である　任意の元 $g^n,g^m\in\langle g\rangle$ について，$g^n(g^m)^{-1}=g^{m-n}\in\langle g\rangle$ より，部分群の特徴付け 1.3.4 から部分群である．

最小性：無限降下法　ある部分集合 $\{e\}\subsetneq H\subsetneq\langle g\rangle$ が $H=\langle g\rangle$ であるとする．すると $\exists_{n\in\mathbb{N}}\ g^n\notin H$ であるが，このためには $g^{n-1}\notin H$ が必要．これを繰り返すと $g\notin H$ となり，矛盾．

■

補題 1.3.9 . 巡回群は Abel 群である．

[証明]. 指数において，整数加法が可換であることによる． ■

補題 1.3.10 . 元 $g\in G$ が位数有限であることと，群 $\langle g\rangle$ が位数有限であることは同値で，その位数は一致する．

[証明].

$\Rightarrow$　g の位数を $n\in\mathbb{N}$ として，$\langle g\rangle=\{e,g,g^2,\cdots,g^n\}$ であることを示す．任意に $m\in\mathbb{Z}$ をとり，$g^m\in\{e,g,g^2,\cdots,g^n\}$ を示せば良い．$m=nk+r$ $(0\leqslant r<n)$ と表せるが，$g^m=(g^n)^kr=r\in\{e,g,g^2,\cdots,g^n\}$ が従う．

$\Leftrightarrow$　$\langle g\rangle$ が位数有限より，$\exists_{m,n\in\mathbb{Z}}\ m\neq n\wedge g^m=g^n$ を満たす．よって，$g^{m-n}=e$.

■

1.3.3　射と部分群

命題 1.3.11 (kernel, image). 群準同型 $f:G\to G'$ について，

(1) $\operatorname{Ker}f=\{g\in G\mid f(g)=e'\}$ は G-部分群である．なお，一般に部分群 $H'\subset G'$ に対して，その逆像 $f^{-1}(H')$ は部分群である．
(2) $\operatorname{Im}f=\{f(g)\mid g\in G\}$ は G'-部分群である．

[証明].

(1) $g_1,g_2\in f^{-1}(H')$ を任意に取る．
  1. $f(g_1g_2)=f(g_1)f(g_2)\in H'$ より，$g_1g_2\in f^{-1}(H')$.
  2. $f(g_1^{-1})=f(g_1)^{-1}\in H'$ より，$g_1^{-1}\in f^{-1}(H')$.
  3. $f(e)=e_{G'}\in H'$ より，$e\in f^{-1}(H')$.

■

1.3.4　中心：共役作用の核

可換性 $gh = gh$ を，「g による左作用と右作用が同じ結果を生む」ことだと思うと，左移動と右移動の合成たる共役作用が恒等になることとして中心が捉えられる．すると，中心は $\mathrm{Ad} : G \to \mathrm{Aut}(G)$ の核であるから正規である．

定義 1.3.12 (center / zentrum). 群 G に対して，$Z(G) := \{g \in G \mid \forall_{h \in G}\ gh = hg\}$ は部分群となり，これを**中心群**という．

補題 1.3.13 . 共役作用 $\mathrm{Ad} : G \to \mathrm{Aut}_{\mathrm{Grp}}(G)$ に対して，$Z(G) = \mathrm{Ker}\ \mathrm{Ad}$.

[証明]. $g \in G$ が $\forall_{h \in G}\ gh = hg$ を満たすことと，$\forall_{h \in G}\ ghg^{-1} = h$ を満たすこと，すなわち $\mathrm{Ad}(g) = \mathrm{id}_G$ より $g \in \mathrm{Ker}\ \mathrm{Ad}$ であることは同値である． ■

1.3.5　部分群の束

部分群の束の，meet, join，束の間の対応を使いこなせるようになりたい．

補題 1.3.14 . $N \lhd G$ として，$\pi : G \to G/N$ を考える．任意の部分群 $H \overset{\mathrm{subgrp}}{\subset} G$ について，$\pi^{-1}(\pi(H)) = HN = NH$．正規部分群の対応 1.6.11 参照．$NH$ が正規とは限らない（第二同型定理 1.7.3）．

[証明]. N で剰余を取るとは，任意の $h \in H, n \in N$ について，$\pi(h) = \pi(hn)$，すなわち，$\pi(H) = \pi(HN)$ ということであるから． ■

補題 1.3.15 . G と部分群 H, H' について，次の 2 条件は同値．

(1) HH' も部分群である．
(2) $HH' = H'H$.

1.3.6　整数環の部分群の分類

$\mathbb{Z}$ は Ring の始対象になる．実際，$\mathbb{Z}$-値点 $\mathbb{Z} \to G$ は，G の元を一つ選ぶことに等しい．

命題 1.3.16 . 整数 $n \geqslant 0$ に対し，$n\mathbb{Z}$ は $\mathbb{Z}$ の部分群であり，$\mathbb{Z}$ の部分群はこの形のものに尽きる．

[証明]. $n\mathbb{Z}$ が $\mathbb{Z}$ の部分群であることは，整数加法の代数法則から従う．

■

命題 1.3.17 (終対象ではないが，大域点として使える). 任意の群 $G \in \mathrm{Grp}$ について，$\mathrm{Hom}_{\mathrm{Grp}}(\mathbb{Z}, G) \simeq U(G)$ である．

[証明].

$$\begin{array}{ccc} F : \mathrm{Hom}_{\mathrm{Grp}}(\mathbb{Z}, G) & \longrightarrow & U(G) \\ \cup & & \cup \\ f & \longmapsto & f(1) \end{array}$$

が集合の同型になっている．逆写像は

$$\begin{array}{ccc} G : U(G) & \longrightarrow & \mathrm{Hom}_{\mathrm{Grp}}(\mathbb{Z}, G) \\ \cup & & \cup \\ g & \longmapsto & f_g : m \mapsto g^m \end{array}$$

である． ■

要諦 1.3.18. これは，自由関手 $F : \mathrm{Set} \to \mathrm{Grp}$ が，Set の終対象 $1 \in \mathrm{Set}$ を Grp に持ち上げているのか？ Grp の終対象は $1 = \{e\}$ なのに．

1.4　群作用と軌道分解：外算法の定める標準分解

一般に群はある自由群からの全射準同型像なので必ず表示を持つが，それは一意的ではない．線型空間の理論と同様，「関係 R」さえ，群としての表現：正規閉包を持つ．線型空間については，関係 R は余核として定めた．これはいずれも Set の直交分解系 (orthogonal factorization system) に由来するためである．
正規部分群を内算法による軌道分解で定義したが，これを圏論的精神で一般化すると，核という概念は必然的に正規部分群の例となる．実際，正規部分群の逆像は正規部分群である．

1.4.1　作用の定義

定義 1.4.1 (action of a group). 集合 X への群 G の作用とは，X 上での表現 $\mathrm{act} : G \to \mathrm{Aut}_{\mathrm{Grp}}(X)$ をいう．あるいは Set 特有の定式化としては[†16]，この currying を直して，

(1) 写像 $* : G \times X \to X$ が次の 2 条件を満たす時，これを**左作用**という．
  (a) $\forall_{x\in X}\ e * x = x$.
  (b) $\forall_{g,h\in G}\ \forall_{x\in X}\ g * (h * x) = (gh) * x$.
(2) 写像 $\star : X \times G \to X$ が次の 2 条件を満たす時，これを**右作用**という．[†17]
  (a) $\forall_{x\in X}\ x \star e = x$.
  (b) $\forall_{g,h\in G}\ \forall_{x\in X}\ (x \star g) \star h = x \star (gh)$.

補題 1.4.2 (右作用を左作用に変換する反変対応).

(1) 任意の $g \in G$ について，左移動 $g_* : X \to X$ は全単射である．すなわち，群準同型 $\overline{\mathrm{act}} : G \to \mathrm{Aut}(X)$ が定まる．
(2) 右作用 $\star : X \times G \to X$ に対して，$g * x = x \star g^{-1}$ と置くと，$* : G \times X \to X$ は左作用を定める．

[証明].

(1) $(g^{-1})_* : G \to G$ が逆射である．
(2) 群作用の 2 公理 1.4.1 を満たす：
  (a) $e * x = x \star e^{-1} = x$.
  (b) $g * (h * x) = g * (x \star h^{-1}) = x \star h^{-1} \star g^{-1} = x \star (gh)^{-1} = (gh) * x$.

■

1.4.2　群作用の性質

群の乗法は正則な自己作用として特徴付けられる

固定 pr_2 と群作用による移動 ρ とを比べる機構が剪断写像である．群作用の性質はこの写像の性質で特徴付けられる．

定義 1.4.3 (shear map). 群作用 $\rho : G \times X \to X$ に対して，群の射

$$\begin{array}{ccc} (\rho, \mathrm{pr}_2) : G \times X & \longrightarrow & X \times X \\ \cup & & \cup \\ (g, x) & \longmapsto & (\rho(g)(x), x) \end{array}$$

を**剪断写像**という．

定義 1.4.4 (proper, transitive, free, regular, faithful / effective). 群作用 $\rho : G \times X \to X$ について，

[†16] 圏論的には，共役 $\mathrm{Ad} : G \to \mathrm{Aut}(G)$ や Cayley 表現同様に，表現で考える．群 G の作用とは，群 G の X 上での表現 $\rho : G \to \mathrm{Aut}(X)$ のことである．すなわち関手 $\rho : \mathcal{B}G \to C$ のことであるが，特に $C = \mathrm{Set}$ では写像 $G \times X \to X$ であって，関手性を満たすもののことをいう．
[†17] Richard Borcherds は $((s)(gh)) = ((s)g)h$ と書いている．関数とは左作用なのであり，いつしか統一が図られたのみである．

(1) 位相群の作用が**固有**であるとは，shear map $G \times X \to X \times X$ が proper であることをいう．すなわち，全てのコンパクト集合の逆像はコンパクトである．
(2) $X \neq \varnothing$ で軌道を 1 つしか持たないとき，すなわち $\forall_{x,y\in X}\ \exists_{g\in G}\ gx = y$ を満たすとき，**推移的**であるという．すなわち，shear map が全射である．
(3) $k \in \mathbb{N}$ について，群作用が定める作用 $G \times X^k \to X^k$ が推移的であるとき，k-推移的であるという．
(4) $\forall_{x\in X}\ gx = x \Rightarrow g = e$ が成り立つとき，**自由**であるという．すなわち，shear map が単射である．
(5) 推移的かつ自由な群作用を**正則**という：$\forall_{x,y\in X}\ \exists!_{g\in G}\ gx = y$．すなわち，shear map が全単射である．この時集合 X を G-torser または主等質空間 (principal homogeneous space)[†18] という．
(6) E 上の G-主束または E 上の G-torsor とは，束 $X \to E$ のファイバー X に G が正則に作用している時をいう．
(7) 置換表現 $\tilde{\rho} : G \to \mathrm{Aut}(X)$ が**忠実**であるとは，$\forall_{g,h\in G}\ g \neq h \Rightarrow [\exists_{x\in X}\ gx \neq hx]$．すなわち，置換表現 $\tilde{\rho} : G \to \mathrm{Aut}(X)$ が単射であることをいう．このとき，作用は**効果的**であるという．

例 1.4.5.

(1) $\mathrm{PSL}_2(\mathbb{C})$ の $\hat{\mathbb{C}}$ への作用は 3-transitive である．
(2) 群の乗法 $G \times G \to G$ は正則で，G の正則表現という．つまり，群の乗法は正則な群作用として特徴付けられる．
(3) Hopf fibration $S^1 \hookrightarrow S^3 \twoheadrightarrow S^2$ にて，$p \in S^2$ の各 fiber は大円になる．

□

1.4.3　作用の定める表現 (currying)

群準同型 $G \to S_n = \mathrm{Aut}([n])$ を作るには，$G \times [n] \to [n]$ を作れば良い，これは線型空間の基底のようである．実際，群作用 $G \times G \to G$ は集合上の表現（置換表現とも言うらしい）$G \to \mathrm{Aut}_{\mathrm{Set}}(G)$ を定める 1.4.2．置換表現といってもこのとき実は，基底の行き先が定まっていると見れば，G から k 上自由生成される k-線型空間 V_G 上の線型写像も一つ定まっている．ということで，一般に「表現」と言った時は線型空間上のものを考えるのである．こうして，正規表現を加群とみなし，既約表現への分解の理論ができる．正則表現とは群の演算が定める作用が定める表現であるが，これは軌道がただ一つで安定化群が自明な集合上の表現として特徴付けられる．[a]

[a] https://ja.wikipedia.org/wiki/正則表現_(数学)

命題 1.4.6 (群作用の定める準同型).

(1) g に左作用を対応させる写像

$$\begin{array}{ccc} \rho : G & \longrightarrow & \mathrm{Aut}(X) \\ \cup & & \cup \\ g & \longmapsto & g_* \end{array}$$

は準同型である．
(2) 準同型 $\pi : G \to \mathrm{Aut}(X)$ に対して，群作用を $(g, x) \mapsto \pi(g)(x)$ と定めると，これは左作用である．
(3) $\mathrm{act}(G \times X, X) \simeq \mathrm{Hom}_{\mathrm{Grp}}(G, \mathrm{Aut}(X))$

[証明].

(1) 補題 1.4.2 より，確かに $g_* \in \mathrm{Aut}(G)$ であることに注意．X の自己全単射として，$\rho(gh) = \rho(g) \circ \rho(h) \in \mathrm{Aut}(X)$ より．
(2) 群作用の 2 公理 1.4.1 を満たす：
  (a) $\pi(e)(x) = \mathrm{id}_X(x) = x$.
  (b) 合成の定義より $\pi(g)(\pi(h)(x)) = (\pi(g) \circ \pi(h))(x)$．$\pi$ が群準同型だから，$(\pi(g) \circ \pi(h))(x) = \pi(gh)(x)$.
(3) (1),(2) で定めた対応は互いに逆写像である．

[†18] 明らかに束を意識した名前である．

■

要諦 1.4.7. テンソルっぽくもあり，基底や自由関手っぽくもある．$G \to S_n$ を作るには，$G \times [n] \to [n]$ を作れば良いのだから．これが Cayley 表現であるか．

命題 1.4.8 (Cayley's theorem). 任意の群 G に対して，埋め込み $G \hookrightarrow \mathrm{Aut}(G)$ が存在する．

[証明]. 任意の群 G の左からの乗法による自身への作用は正則であり、したがって忠実でもある：$G \to \mathrm{Aut}(G)$ が単射である。従って、任意の群 G はそれ自身の元上の対称群 $\mathrm{Aut}(G)$ に埋め込める． ■

1.4.4　作用の例

例 1.4.9 (作用を作用に移す反変関手：正則表現)**.** 集合 X への右作用 $X \times G \to X$ は，X 上の関数の空間上に左作用を定める．

$$\begin{array}{ccc} G \times \mathrm{Map}(X, \mathbb{C}) & \longrightarrow & \mathrm{Map}(X, \mathbb{C}) \\ \cup & & \cup \\ (g, f) & \longmapsto & g * f = f \circ g^* \end{array}$$

これは，一番対称的な形だと $af(x) = f(xa)$ というように，関数空間への（スカラーの）作用の持ち上げの一般論である．補題 1.4.2(2) と併せて $af(x) = f(xa) = f(a^{-1}x)$ と考えると，これは共役の例でもあるのか． □

例 1.4.10 (引数の置換)**.** 環 A 上の多項式環 $A[x_1, \cdots, x_n]$ に対して，作用

$$\begin{array}{ccc} S_n \times A[x_1, \cdots, x_n] & \longrightarrow & A[x_1, \cdots, x_n] \\ \cup & & \cup \\ (\sigma, f) & \longmapsto & (\sigma * f)(x_1, \cdots, x_n) = f(x_{\sigma(1)}, \cdots, x_{\sigma(n)}) \end{array}$$

□

例 1.4.11 (群の自身への作用（正則表現）)**.** 群の自身への作用 $\rho : G \times G \to G$ は，$\rho : G \to \mathrm{Aut}(G)$ と見れば，G の上または下に立つ射で，圏 Set の Hom 集合の間に引き起こすもの，と見ることができる，これが currying である．射の合成と見ると，左移動は加速 $\leftarrow$，右移動は衝突 $\rightarrow$，共役は $\uparrow\uparrow$

(1) 群 G の自身への作用

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ \cup & & \cup \\ (g, h) & \longmapsto & g * h := gh \end{array}$$

を**左移動**と呼ぶ．

(2) 右作用 $h \star g = hg$ に対応する左作用は $g * h = hg^{-1}$ で，これを**右移動**という．[†19]

(3) 2 つを組み合わせたもの $(g, h) \mapsto ghg^{-1}$ を**共役作用**という．これは内部自己同型 $\mathrm{Ad} : G \hookrightarrow \mathrm{Aut}(G)$ の定める群作用でもある．群の元が可換とは左移動と右移動が同じ結果を生むことであるから，右移動の左作用化と左移動の合成たる共役作用の言葉で特徴付けられるはずである．

(4) 共役作用の右作用版は，よく冪記法 $x^g = g^{-1}xg$ と表される．[†20]

(5) 左移動と右移動（＝正則表現）は，置換表現として，軌道がただ一つで安定化群が自明である置換表現として特徴付けられる．

□

例 1.4.12 (Klein の四元群)**.** 巡回群でない 4 元群が存在し，この 2 つで位数 4 の群は尽きる．巡回群ではない最も小さい群である．

$$f_1 := x_1x_4 + x_2x_3, \qquad f_2 := x_2x_4 + x_1x_3, \qquad f_3 := x_3x_4 + x_1x_2, \in \mathbb{Z}[x_1, x_2, x_3, x_4]$$

[†19] -1 は，左作用性の公理を満たすために必要．さもなくば，反変性 $\rho(gh) = \rho(h) \circ \rho(g)$ を帯びてしまう．

[†20] exponential object と currying はすごく近い．

と定めて，この対称群の引数の置換による作用のこの三元集合への制限 $S_4 \curvearrowright \{f_1, f_2, f_3\}$ を考えると，$\forall_{\sigma\in S_4}\ \forall_{i\in[3]}\ \sigma(f_i) \in \{f_1, f_2, f_3\}$ が成り立つから well-defined．したがって，群準同型 $\phi : S_4 \to S_3$ が定まるが，これは全射となり，f_1, f_2, f_3 を不変に保つ置換の仕方は全部で $V := \mathrm{Ker}\ \phi = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ である．これを Klein の四元群という．

命題 1.4.13 (Klein の四元群).

(1) V は準同型 $\phi : S_4 \to S_3$ の核なので正規である．
(2) V は Abel 群である．
(3) $\forall_{\sigma\in V}\ \sigma^2 = e$.
(4)

$$\begin{array}{ccc} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \longrightarrow & V \\ \cup & & \cup \\ (\bar{0}, \bar{0}) & \longmapsto & e \\ (\bar{1}, \bar{0}) & \longmapsto & (1\,2)(3\,4) \\ (\bar{0}, \bar{1}) & \longmapsto & (1\,3)(2\,4) \\ (\bar{1}, \bar{1}) & \longmapsto & (1\,4)(2\,3) \end{array}$$

は可逆である．

□

1.4.5　安定化群と軌道と軌道分解

群作用 $G \times X \to X$ が定まっていると，標準的な分解が存在する．flow などの概念の萌芽で，演算を加法として線型空間を考えると「軌道」という感覚がわかりやすい．各剰余類は $a + N$ と表せる．

定義 1.4.14 (stabilizer group / isotopy group, orbit through a point). $G \times X \to X$ を左作用とし，これが定める群準同型を $\rho : G \to \mathrm{Aut}(X)$ をとる．

(1) x を動かさない X 自己同型を定める群 G の元の集まり $\mathrm{Stab}_G(x) := \{g \in G \mid gx = x\}$ は G-部分群であるが，一般に正規ではない．[†21] これを G-**安定化群**と呼ぶ．
(2) x が G の元が定める自己同型で動く範囲 $Gx := \{gx \mid g \in G\} = \mathrm{Im}\ (\mathrm{ev}_x \circ \rho)$ を x を通る G-軌道という．[†22]
(3) $G\backslash X := \{Gx \mid x \in X\}$ を X の G による商と呼ぶ．右作用の場合は X/G で表す．

補題 1.4.15 .

(1) $x, x' \in X$ について，次の 3 条件は同値である．
  (a) $x' \in Gx$.
  (b) $Gx \cap Gx' \neq \emptyset$.
  (c) $Gx = Gx'$.
(2) 上の関係を $x \sim_G x'$ で表すと，これは同値関係であり，これについての x の同値類は Gx に等しい．

[証明].

(1) (a)⇒(b)

$$\begin{aligned} (a)\ x' \in Gx &\Leftrightarrow \exists_{g\in G}\ x' = gx \\ &\Leftrightarrow \exists_{g\in G}\ g^{-1}x' = x \Leftrightarrow x \in Gx' \end{aligned}$$

と $x' \in Gx'$ より，$\{x'\} \subset Gx \cap Gx' \neq \emptyset$.

[†21] G_x という記法も用いられるが軌道と紛らわしい．この軌道の本質は，不動点の全体を X^G と表すならば（群コホモロジー），余不変式の空間は X_G となるべき（群ホモロジー），というものである．これは X が G-加群である場合などを考えている．
[†22] $G \xrightarrow{\rho} \mathrm{Aut}(X) \xrightarrow{\mathrm{ev}_x} X$

(b)⇒(c)　$x'' \in Gx \cap Gx'$ のとき，$\exists_{g,g' \in G}\ gx = x'' = g'x'$.

$$\begin{aligned} y \in Gx &\Leftrightarrow \exists_{h \in G}\ y = hx \\ &\Leftrightarrow \exists_{h \in G}\ y = hg^{-1}g'x' \\ &\Leftrightarrow y \in Gx' \end{aligned}$$

(c)⇒(a)　$Gx = Gx'$ ならば特に $Gx \supset Gx' \ni x'$ より．

(2) (a)⇒(b) の証明で対称性は示した，(c) より推移的である．

■

要諦 1.4.16. 左移動の定める同値関係が $xG = yG \Leftrightarrow xy^{-1} \in G$

定理 1.4.17 (軌道分解). 左作用 $G \times X \to X$ に対して，軌道分解 $X = \coprod_{Gx \in G\backslash X} G_x$ が存在する．

[証明]. 補題 1.4.15(2) による類別から従う． ■

1.4.6　軌道分解の例

例 1.4.18.

(1) $O_2(\mathbb{R}) \curvearrowright \mathbb{R}^2$ の軌道分解は $\mathbb{R}^2 = \coprod_{r \geqslant 0} \{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 = r^2\}$.

(2) $\mathrm{GL}_2(\mathbb{R}) \curvearrowright \mathbb{R}^2$ の軌道分解は $\mathbb{R}^2 = \{(0,0)\} \coprod (\mathbb{R}^2 \backslash \{(0,0)\})$ である．

(3) 作用

$$\begin{array}{ccc} (\mathrm{GL}_m(\mathbb{C}) \times \mathrm{GL}_n(\mathbb{C})) \times M_{mn}(\mathbb{C}) & \longrightarrow & M_{mn}(\mathbb{C}) \\ \cup & & \cup \\ (g,h,X) & \longmapsto & gXh^{-1} \end{array}$$

の軌道は $M_{mn}(\mathbb{C}) = \coprod_{0 \leqslant r \leqslant \min(m,n)} \{X \in M_{mn}(\mathbb{C}) \mid \mathrm{rank}\, X = r\}$．この商集合の完全代表系は，階数標準形である．

□

1.5　群への作用の研究：内算法特論

半直積同様，自己言及させた時が一番深い

部分群 H について潰す $H\backslash G$ は，H が一点となって抽象化される．では他の点はどうなるかというと，軌道という概念が登場する．これを一度調べて，新たな集合 $H\backslash G$ が群になる条件を捉える．群では指数という特徴量が定まるのは，その射の可逆性＝方程式の解の一意性による．

1.5.1　剰余類分解：内算法による軌道分解

内算法による軌道分解

部分群 H に対して，軌道 $\{Hg\}_{g\in G}$ として右剰余類を得る．これは同値関係 $a\sim b :\Leftrightarrow ab^{-1}\in H$ としても定義でき（補題 1.4.15），$|H|$ 個の軌道に分解され，これを $G\backslash H$ で表す．一般の圏では coequalizer である．

$$H\times G \overset{\mathrm{pr}_2}{\underset{\cdot}{\rightrightarrows}} G$$

同様に左剰余類も equalizer として考えられるが，これは左作用と右作用の間の双対性として理解できる．双対性があるならば，これを綜合する双写像があるはずであり，これを共役作用と呼ぶ．そして左右の差を議論する大事な言葉となるはずで，正規性の特徴付けになって然るべきである．

定義 1.5.1 (right coset, left coset). G を群，$H\subset G$ をその部分群とする．

(1) G の G への左移動による作用（群乗法）を H に制限したもの $H\times G\to G$ の軌道分解を $H\backslash G$ と表し，この元を G **の** H **による右剰余類**という．
(2) これは，同値関係 $a\sim b :\Leftrightarrow ab^{-1}\in H$ による類別 $H\backslash G$ である．補題 1.4.15 より，$Ha=Hb\Leftrightarrow a\in Hb\Leftrightarrow ab^{-1}\in H$.[†23]

命題 1.5.2 (左右双対性).

$$G/H\simeq_{\mathrm{Set}} H\backslash G.$$

[証明]. 群準同型を

$$\begin{array}{ccc} \varphi : H\backslash G & \longrightarrow & G/H \\ \cup & & \cup \\ Hg & \longmapsto & g^{-1}H \end{array} \qquad \begin{array}{ccc} \psi : G/H & \longrightarrow & H\backslash G \\ \cup & & \cup \\ gH & \longmapsto & Hg^{-1} \end{array}$$

と定めると，これは互いに逆写像であるから，あとはこれらの写像が well-defined であること，すなわち $\forall_{g,g'\in G}\ Hg=Hg'\Rightarrow g^{-1}H=g'^{-1}H$ を示せば良い．これは補題 1.4.15 から従う．$Hg=Hg'\Leftrightarrow g'\in Hg\Leftrightarrow \exists_{h\in H}\ g'=hg$ と仮定すると，$g'^{-1}=g^{-1}h^{-1}\in g^{-1}H\Leftrightarrow g'^{-1}H=g^{-1}H$ が従う． ■

定義 1.5.3 (index).

(1) $|H\backslash G|<\infty\Leftrightarrow |G/H|<\infty$ のとき，部分群 H は指数有限であるという．
(2) 部分群 H が指数有限であるとき，$|H\backslash G|=:(G:H)\in\mathbb{N}$ と書き，G の H に於ける**指数**という．

定理 1.5.4 (剰余類分解). G を群，H をその部分群とする．

(1) $G=\coprod_{Hg\in H\backslash G} Hg$ である．
(2) $G=\coprod_{gH\in H/G} gH$ である．

[証明]. 軌道分解 1.4.17 の特別な場合である． ■

1.5.2　有限群の部分群の研究

定理 1.5.5 (部分群の位数：Lagrange's theorem). H を G の部分群とする．$\dfrac{|G|}{|H|}=|G/H|=|H\backslash G|$.

[証明].

(1) 群準同型

$$\begin{array}{ccc} \varphi_g : H & \longrightarrow & Hg \\ \cup & & \cup \\ h & \longmapsto & hg \end{array}$$

は逆写像 $\varphi_{g^{-1}}:Hg\to H$ を持つから，特に $|H|=|Hg|$ である．

[†23] 右側の元につく $^{-1}$ が，右に残った剰余の痕である．

(2) 右剰余類分解 1.5.4$G = \coprod_{Hg \in H\backslash G} Hg$ より，$|G| = |H\backslash G||H|$.

(3) $|H| > 0$ より，$\dfrac{|G|}{|H|} = |H\backslash G|$.

■

系 1.5.6. G を有限群とする．任意の元 $g \in G$ は位数有限であり，その位数は $|G|$ の約数である．

[証明].

(1) $\langle g \rangle \subset G$ と補題 1.3.10 より，g は位数有限である．
(2) Lagrange の定理 1.5.5 より，$|G| = |\langle g \rangle||G/\langle g \rangle|$ だから．

■

系 1.5.7. 有限群 G の位数 p が素数ならば，G は巡回群であり，特に Abel 群である．

[証明]. 位数 p が素数だから，$g \in G\backslash\{e\}$ を満たす元 g が取れる．これについて $\langle g \rangle = G$ を示す．（すると，補題 1.3.9 より Abel 群である．）$\langle g \rangle \subsetneq G$ と仮定して矛盾を示す．Lagrange の定理 1.5.5 より，$|G| = |\langle g \rangle||G/\langle g \rangle|$ だが，$|G|$ が素数で $|\langle g \rangle| < |G|$ より，$|\langle g \rangle| = 1$ が必要だが，これは $\{e, g\} \subset \langle g \rangle$ に矛盾. ■

系 1.5.8 (Fermat's minor theorem). p を素数とする．$x \not\equiv 0 \mod p \Rightarrow x^{p-1} \equiv 1 \mod p$.

[証明]. 乗法群 $(\mathbb{Z}/p\mathbb{Z})^\times$ は位数 $p-1$ の巡回群であるため.[†24] ■

1.5.3　軌道と安定化群：作用の像と核の関係

作用に対する準同型定理

x の軌道 Gx は，x の安定化群による剰余類 $G/\mathrm{Stab}_G(x)$ と同型である．なぜだ．おそらく作用 $\rho : G \to \mathrm{Aut}(G)$ についての準同型定理の先にある消息である．ある意味で局所と大域のフラクタル構造がある気がする．少なくとも，像である軌道よりも，核である安定化群の方が，内部化されていて記述しやすい．特に $gx = g'x \Leftrightarrow g\mathrm{Stab}_G(x) = g'\mathrm{Stab}_G(x)$.

命題 1.5.9 (orbit stabilizer theorem). $G \times X \to X$ を群作用とする．

(1) 写像

$$\begin{array}{ccc} \varphi : G/\mathrm{Stab}_G(x) & \xrightarrow{\sim} & Gx \\ \cup & & \cup \\ g\mathrm{Stab}_G(x) & \longmapsto & gx \end{array}$$

は可逆である．
(2) 特に G が有限群のとき，$|Gx| = \dfrac{|G|}{|\mathrm{Stab}_G(x)|}$.[†25]

[証明].

well-definedness　写像として定まっていること：$g\mathrm{Stab}_G(x) = g'\mathrm{Stab}_G(x) \Rightarrow gx = g'x$ を示す．前件の下では $g' \in g\mathrm{Stab}_G(x)$ すなわち $\exists_{h \in \mathrm{Stab}_G(x)}\ g' = gh$ であるが（補題 1.4.15），$gh^{-1} = g'$ より，$gh^{-1}x = gx = g'x$.

全射性　$g\mathrm{Stab}_G(x) \in \varphi^{-1}(gx)$ である．

単射性　$gx = g'x$ とする．$g'h \in g'\mathrm{Stab}_G(x)$ について $(g'h)x = g'x = gx$ より $g'h \in g\mathrm{Stab}_G(x)$ であり，逆も言えるから，$g\mathrm{Stab}_G(x) = g'\mathrm{Stab}_G(x)$.

(2) は，Lagrange の定理 1.5.5 より，$\dfrac{|G|}{|\mathrm{Stab}_G(x)|} = |G/\mathrm{Stab}_G(x)| = |Gx|$. ■

要諦 1.5.10. 結局，$gx = g'x \Leftrightarrow g\mathrm{Stab}_G(x) = g'\mathrm{Stab}_G(x)$ となるのが肝であった.

[†24] a 倍写像は単射であるため.
[†25] 像より核の方が扱いやすいという基本的な非対称性がある.

1.5.4　共役作用と類等式

共役作用の定める軌道分解を共役類分解といい，推移的作用が定める集合の同型を類等式という

左移動と右移動とを 1 つの写像の中に組み合わせて同型としたものが共役作用である．中心とは，内部自己同型で動かない元がなす「核」である（実際 $Z(G) = \mathrm{Ker}\,\mathrm{Ad} : G \hookrightarrow \mathrm{Aut}_{\mathrm{Grp}}(G)$）．したがって中心は正規である．したがって，アーベル群では内部自己同型の群は自明である．
集合 X に群 G が推移的に作用しているとき，その x に関する G-軌道からの全射 $Gx \twoheadrightarrow X$ について，関係 $G/\mathrm{Stab}_G(x) \simeq_{\mathrm{Set}} X$ が成り立つ．推移的作用 $\rho : G \times X \to X$ で $\rho(-, x) : G \twoheadrightarrow X$ と固定したとき，左剰余類 $g\mathrm{Stab}_G(x) \subset G$ は x を押し並べて $\rho(g)(x)$ に写すためである．すると，この関係を用いて，軌道分解の完全代表系を見つければ X の濃度の G の位数による表現が求まる．特に X も群である場合が重要であるから，特に共役類分解について類等式が立てられる．

[†26]

定義 1.5.11 (conjugation action). $\mathrm{Ad} : G \to \mathrm{Aut}_{\mathrm{Grp}}(G); g \mapsto \mathrm{Ad}(g) : h \mapsto ghg^{-1}$ を共役作用という．

注 1.5.12 (adjoint action, similarity transformation).

(1) 随伴作用とは，Lie 群など，別の圏から $\mathrm{Aut}_{\mathrm{Grp}}(G)$ へと表現という形で共役によって作用することをいうようであり，そのとき $h \mapsto g^{-1}hg$ と書くことも多いのはなぜだろか．
(2) また，相似変換 (similarity transformation) は $B \mapsto S^{-1}AS$ をいう．この共役類分解は，線型写像と考えられる．すなわち，相似変換は基底変換を通じて，相互に同じ線型写像を表現していると捉えられる．これが自己同型であるから，たくさんの線型写像の圏論的性質を保つ．

定義 1.5.13 (centralizer, conjugacy class). 共役作用 $\mathrm{Ad} : G \hookrightarrow \mathrm{Aut}_{\mathrm{Grp}}(G)$ について．

(1) 共役作用の安定化群 $Z_G(g) := \mathrm{Stab}_G(g) = \{h \in G \mid hgh^{-1} = g\}$ を特に**中心化群**という．
(2) g の Ad 軌道 $Gg = \{hgh^{-1} \mid h \in G\}$ を共役類といい，その元は g と共役であるという．[†27]

例 1.5.14 (共役類は可換でない要素を括り出す位相である).

(1) $e \in G$ の共役類は $\{e\}$ である．Ad によって他に写りようがないからである．
(2) Abel 群では，任意の共役類は一元集合である．「共役類で割ると Abel 群を得る」は間違っていない．

□

命題 1.5.15 (class equation). $\{g_1, \cdots, g_n\}$ を群 G の共役類の完全代表系とする．

$$|G| = \sum_{i=1}^{n} \frac{|G|}{|Z_G(g_i)|}.$$

[証明].

(1) 軌道分解 1.4.17 より，$G = \coprod_{i=1}^{m} \{hg_ih^{-1} \mid h \in G\}$ である．
(2) 軌道-安定化群の関係 1.5.9 より，$\dfrac{|G|}{\mathrm{Stab}_G(x)} = \dfrac{|G|}{Z_G(x)} |\{hg_ih \mid h \in G\}| = |Gx|$.

■

要諦 1.5.16. 共役類分割には，特に安定化群による見方をして（軌道と安定化群の関係 1.5.9），特別な名前が，方程式の方についている．これは整数の構造に仮託するためだろうか．これは元の位数によって（それよりは粗いが）分類していると見れるのでは

[†26] 双対性があるならば，これを綜合する双写像があるはずであり，これを共役作用と呼ぶ．これは随伴と呼ぶべき，自然に定まる射である．するとこれは他の作用同様，自然な軌道分解を G の上に定めているはずである．そして左右の差を議論する大事な言葉となるはずで，正規性の特徴付けになって然るべきである．こうして中心という概念が出てくる．中心の各元は単独で共役類をなす．非可換群において，その共役類の構造を研究するのが基本的な手法となる．例えば p 群と呼ばれる非可換群の中心は一発でわかる．Sylow の定理もその延長線上である．

[†27] conjugate subgroup という考え方があって，共役類分割が結構粗いものになる．なぜなら，$H_1 \sim H_2 \Leftrightarrow H_2 = \mathrm{Ad}(g)(H_1)$ による同値類である．

ないのか？

補題 1.5.17 (共役の代数的本質). h を g と共役な元とする．g と h の位数は等しい．

[証明]. $k \in G$ が存在して $h = kgk^{-1}$ の関係にあるとき，任意の自然数 $n \in \mathbb{N}$ について，$h^n = e$ と $g^n = e$ は同値である．$h^n = (kgk^{-1})^n = kg^nk^{-1}$ または $g^n = (k^{-1}hk)^n = k^{-1}h^nk$ より，$g^n = e \Rightarrow h^n = e$ で，$h^n = e \Rightarrow g^n = e$ である． ■

例 1.5.18 (S_3 の類等式)**.** $\sigma, \tau \in S_3$ について．

(1) σ の中心化群について，巡回群は可換なので $\langle\sigma\rangle = \{e, \sigma, \sigma^2\} \subset Z_{S_3}(\sigma)$ であるが，$\tau\sigma \neq \sigma\tau$ より $\tau \notin Z_{S_3}(\sigma)$ だから，$Z_{S_3}(\sigma) = \{e, \sigma, \sigma^2\}$ であることは確かめられる．が，共役類は全通り計算するしかない．しかし関係 $\dfrac{|S_3|}{|Z_{S_3}(\sigma)|} = 2$ より，σ の共役類の大きさは 2 で，**元の位数は σ と等しく 3 であるから**，$\{\sigma, \sigma^2\}$ とわかる．
(2) 続いて，同様にして $Z_{S_3}(\tau) = \langle\tau\rangle = \{e, \tau\}$ より，共役類の大きさは 3 で，$\{\tau, \sigma\tau, \sigma^2\tau\}$.

この場合も，共役類をそのまま探すのではなくて，命題 1.5.9 によって，安定化群として探す方が得策である． □

共役な元の位数が等しいとは，共役類は巡回群にはなり得ないということか？

1.5.5　中心と正規部分群

共役自己同型の核 $Z(G) := \mathrm{Ker}\ \mathrm{Ad} : G \to \mathrm{Aut}_{\mathrm{Grp}}(G)$ を中心とする．すると，動かされる側として見ても任意の元の定める共役移動について不変というわけだから，中心の元は単独で共役類をなす．中心が全体に等しい場合 $Z(G) = G$ をアーベル群という．また $\mathrm{Ad} : G \to \mathrm{Aut}_{\mathrm{Grp}}(G)$ についての準同型定理より，これによる商群は，内部自己同型群の間に同型を定める：$G/\mathrm{Ker}\ \mathrm{Ad} \simeq \mathrm{Im}\ \mathrm{Ad} \quad \Leftrightarrow \quad G/Z(G) \simeq \mathrm{InAut}(G)$.

定義 1.5.19 (characteristic group, center / zentrum).

(1) 正規部分群とは，全ての内部自己同型の下で不変な部分群をいう：$\forall_{g\in G}\ Ad(g)(N) = N$.
(2) 特性部分群とは，全ての自己同型の下で不変な部分群をいう．交換子部分群や中心がその例である．

$Z(G) := \cap_{g\in G} Z_G(g) = \mathrm{Ker}\ \mathrm{Ad}$ を中心という．定義から，常に正規な部分群となり，特性的である．

補題 1.5.20 . $G/Z(G)$ は内部自己同型群と同型である．

例 1.5.21 (中心)**.**

(1) $Z(\mathrm{GL}_n(\mathbb{C})) = \mathbb{C}I_n$．線型空間 V 上の射影一般線形群とは，$\mathrm{PSL}(V) = \mathrm{GL}(V)/Z(V)$ である．特に $\mathrm{PGL}_2(\mathbb{C}) \simeq \mathrm{Aut}(\hat{\mathbb{C}})$.
(2) $Z(D_n) = \begin{cases} \{e\}, & n \text{ が奇数のとき}, \\ \{e, \sigma^{n/2}\}, & n \text{ が偶数のとき}. \end{cases}$
(3) $Z(S_n) = \{e\}$ $(n \geqslant 3)$ である．S_2 は Abel 群なので，$Z(S_2) = S_2$.

□

命題 1.5.22 (p-群の中心は非自明である). G を有限な p 群，すなわち，位数が p の冪であるような有限群とする．G が自明でないならば，G の中心 $Z(G)$ も自明でない．

[証明]. 類別の完全代表系 (g_i) による類等式 $|G| = \sum_{i=1}^{m} \dfrac{|G|}{|Z_G(g_i)|}$ を考える．一般の状況下で，$g_i \in Z(G) \Leftrightarrow Z_G(g_i) = G \Leftrightarrow \dfrac{|G|}{|Z_G(g_i)|} = 1$ であるから，$g_i \notin Z(G) \Leftrightarrow \dfrac{|G|}{|Z_G(g_i)|} \neq 1$．$G$ が p 群のとき，中心に入らない元 $g_i \in G\backslash Z(G)$ について，$\dfrac{|G|}{|Z_G(g_i)|} = mp\ \exists_{m\geqslant 1}$ である．すなわち，類等式は $|G| = |Z(G)| + pn\ \exists_{n\geqslant 1}$ の形であるから，$|Z(G)|$ も p の倍数であり，特に 1 でない． ■

1.6　正規部分群と剰余群：左右のズレの検出

群構造が商集合上に持ち上がる時：共役類の概念と部分群の概念を合流させる

部分群からなる内部構造が退化している群を単純群という．正規部分群とは内部自己同型 $\mathrm{Ad}(n,-)$ が不変に保つ軸のようなものである．
これは左右の剰余類が一致するための必要十分条件であるので，これについて軌道分解をすると良い．ある部分集合 $A \subset G$ が，部分群 $H \subset G$ の右剰余類でありかつ左剰余類であるとは，$\forall_{a\in A} A = Ha = aH$．よって，部分群 H が $\forall_{a\in G} Ha = aH$ を初めから満たしていたら，右剰余類と左剰余類は一致する．これは $a^{-1}Ha = H$ に同値．実は $a^{-1}Ha \subset H$ に同値．
実は，左右の剰余類が一致するのはこの場合に限る．なぜならば，正規部分群 N の任意の右剰余類は Na と表せるが，$Na = aN$ であるからである．
任意の剰余類 Na, Nb について，$(Na)(Nb) = NNab = Nab$ より，新たな剰余類を得る．こうして，群構造は商集合 $G/\sim$ 上に持ち上がる．

1.6.1　正規性

正規性とは何か

部分群の正規性は圏論的概念なのだろうか．つまり，全ての正規部分群は何かの全射の核になる，など．さもなくば，像関手に対して保たれるなどの関手的な性質を持つはずがない．
どうやら congruence relation と関連がある．[α] "The coequalizer of a congruence is called a quotient object."

[α] https://ncatlab.org/nlab/show/normal+subgroup

定義 1.6.1 (normal subgroup, simple group). G を群，$N \subset G$ を部分群とする．

(1) 部分群 N が $\forall_{g\in G}\, gNg^{-1} \subset N$ を満たすとき，[†28] N は**正規**または**不変**であるという．[†29]
(2) G が $G, \{e\}$ 以外に正規な部分群を持たないとき，G を**単純**であるという．

補題 1.6.2 (正規性のイメージ). $N \lhd G$ とする．このとき，N は G の共役類のいくつかの合併として表せる．

要諦 1.6.3. 部分群 N が共役類に分割できることを正規という． この共役類分割が G/N であるはず．ここの関係が難しい．Abel 群はいわば共役類に関する離散位相で，任意の部分集合は共役類の合併だから，Abel 群の任意の部分群は正規である．Abel 化 1.12.10 とは，交換子部分群という特殊な正規部分群について割ることで，離散位相を作る行為である．ここに位相的な，集合代数的構造がある．

注 1.6.4 (characteristic group)**.** 全ての内部自己同型 $\varphi \in \mathrm{in}\,(G)$ に対して不変 $\varphi(N) = N$ な部分群が正規部分群である．より一般に，全ての自己同型 $\varphi \in \mathrm{Aut}(G)$ に対して不変な部分群を**特性部分群**と呼ぶ．交換子部分群と群の中心は特性部分群である．

命題 1.6.5 (核は正規). 準同型 $f : G \to G'$ について，$\mathrm{Ker}\, f \subset G$ は正規部分群である．

[証明]. 任意の $g \in G, h \in \mathrm{Ker}\, f$ に対して $f(ghg^{-1}) = f(g)ef(g)^{-1} = e$ だから，$G\mathrm{Ker}\, fG^{-1} \subset \mathrm{Ker}\, f$ である． ■

要諦 1.6.6. よって $A_n \subset S_n$ は指数 2 の正規部分群である．

命題 1.6.7 (像は正規性を保つ：正規性は圏論的に特徴付けられる消息である). $H \lhd G$ のとき，任意の全射 $f : G \to G'$ について，$f(H) \lhd G'$．（一般の準同型 f について，$f(H) \lhd \mathrm{Im}\, f$ と言ってもいい）．

[証明]. 任意に $g \in G'$ をとる．$gHg^{-1} \subset H$ より，$f(gHg^{-1}) = f(g)f(H)f(g)^{-1} \subset f(H)$．$f(g) \in G'$ が G' 全体を走るとき，

[†28] $gH = Hg \Leftrightarrow gHg^{-1} = H \Leftrightarrow gHg^{-1} \subset H$ に注意．条件 $\forall_{g\in G}\, gHg^{-1} \subset H$ 単独でも，g^{-1} も G 上を走るから（$^{-1} : G \to G$ が可逆），$H \subset gHg^{-1}$ が復元できる．
[†29] すなわち，$N \subset \mathrm{Ad}(-)(N)$ を満たす安定部分空間である．

$f(H)$ も正規である.[†30]　■

1.6.2　剰余群とその普遍性

正規部分群は右剰余類と左剰余類が一致するから，G/N 上に演算が well-defined に定まる．こうして出来た商群は普遍性を満たし，部分群については商位相と同様の性質を満たす．正規部分群は，共役類から見たら，まさに開集合である．**より高級な代数系では，剰余を取る際にこのような議論の必要がないところが興味深い**.

定理 1.6.8 (quotient group). $H \lhd G$ を正規部分群とする.

(1)
$$\begin{array}{ccc} G/H \times G/H & \longrightarrow & G/H \\ \cup & & \cup \\ (gH, g'H) & \longmapsto & (gg')H \end{array}$$
は群の演算を定め，G/H はこの演算について群をなす.

(2)
$$\begin{array}{ccc} \pi : G & \longrightarrow & G/H \\ \cup & & \cup \\ g & \longmapsto & gH \end{array}$$
は群の全射準同型であり，$\operatorname{Ker}\pi = H$ である.

[証明].

(1) well-definedness　$g_1H = h_1H, g_2H = h_2H \Rightarrow g_1g_2H = h_1h_2H$ を示す．仮定の $g_1H \subset h_1H, g_2H \subset h_2H$ 部より $\exists_{h,h'}\ g_1h = h_1, g_2h'h_2$ であるから，$h_1h_2 = g_1hg_2h' = g_1g_2\underbrace{(g_2^{-1}hg_2)}_{\in H}h'$ より，$h_1h_2H \subset g_1g_2H$ である．仮定の残りの仮定の $g_1H \supset h_1H, g_2H \supset h_2H$ 部から，逆も言える.

群の公理　H が単位元，$g^{-1}H$ の逆元が gH である．結合律も満たす.

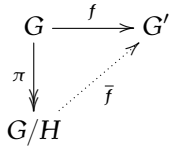
(2) functority　$\pi(g_1g_2) = g_1g_2H = (g_1H)\cdot(g_2H) = \pi(g_1)\pi(g_2)$.

kernel　補題 1.4.15 より，$g \in \operatorname{Ker}\pi \Leftrightarrow gH = H \Leftrightarrow g \in H$ より.

全射性　$\forall_{g\in G}\ g \in \pi^{-1}(gH)$.

■

命題 1.6.9 (universality). $H \lhd G$ を正規部分群とし，群準同型 $f : G \to G'$ は $H \subset \operatorname{Ker} f$ を満たすとする．このとき，次の図式を可換にする準同型 $\overline{f} : G/H \to G'$ がただ一つ存在する：



すなわち，$\operatorname{Hom}_{\mathrm{Grp}}(G/H, G') \simeq \{f \in \operatorname{Hom}_{\mathrm{Grp}}(G, G') \mid H \subset \operatorname{Ker} f\}$.

[証明].
$$\begin{array}{ccc} \overline{f} : G/H & \longrightarrow & G' \\ \cup & & \cup \\ xH & \longmapsto & f(x) \end{array}$$
と定めると，

[†30] $\forall_{g\in H}\ g^{-1}f(N)g \subset f(N)$ を示せば良い．任意に $h \in f(N)$ をとる．f は全射だから，$g' \in G, h' \in N$ が存在して，$f(g') = g, f(h') = h$ を満たす．$f(g'^{-1}h'g') = f(g')^{-1}f(h')f(g') = g^{-1}hg \in f(N)$ である.

well-definedness　$xH = x'H \Rightarrow \exists_{h\in H}\ x = x'h \Rightarrow f(x'h) = f(x')f(h) = f(x') = f(x)$ であり，
functority　$\overline{f}(xHyH) = \overline{f}(xyH) = f(xy) = f(x)f(y) = \overline{f}(xH)\overline{f}(yH)$ より，群準同型であり，
適格性　$f = \overline{f} \circ \pi$ を満たす：$f(x) = \overline{f}(\pi(x)) = \overline{f}(xH) = x$.
一意性　また，$f = \overline{f} \circ \pi = g \circ \pi$ とすると，π の全射性から $g = \overline{f}$ が従う．

■

系 1.6.10 (巡回群からの射). 任意の $n \in \mathbb{N}$ について，$\mathrm{Hom}_{\mathrm{Grp}}(\mathbb{Z}/n\mathbb{Z}, G) \simeq \{g \in G \mid g^n = e\}$.

[証明]. 命題 1.3.17 より，群準同型

$$\begin{array}{ccc} U(G) & \xrightarrow{\varphi} & \mathrm{Hom}_{\mathrm{Grp}}(\mathbb{Z}, G) \\ \cup & & \cup \\ g & \longmapsto & f_g : n \mapsto g^n \end{array}$$

は可逆なのであった．剰余群の普遍性 1.6.9 より，

$$\mathrm{Hom}_{\mathrm{Grp}}(\mathbb{Z}/n\mathbb{Z}, G) \simeq \{g \in \mathrm{Hom}_{\mathrm{Grp}}(\mathbb{Z}, G) \mid g(n\mathbb{N}) = \{e\}\}$$

である．すなわち，$\{g \in G \mid g^n e\}$ とも全単射がある．[†31]

■

1.6.3　正規部分群の対応

命題 1.6.11 (正規部分群の対応). $N \lhd G$ を正規部分群とする．

(1) 包含関係を保つ全単射が存在する：$\{H \in P(G) \mid N \hookrightarrow H \hookrightarrow G\} \simeq_{\mathrm{pos}} \{H \in P(G/N) \mid H \hookrightarrow G/N\}$. [†32]
(2) 特に，この同型によって，G の正規部分群で N を含むものと，G/N の正規部分群が対応する．すなわち，π^*, π_* は部分群の正規性を保つ．[†33]

[証明].

$$\begin{array}{ccc} H & \overset{i}{\hookrightarrow} & G \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ H/N & \overset{i}{\dashrightarrow} & G/N \end{array}$$

(1) 商写像 π の定める 2 つの Hom 集合間の写像 $\mathrm{Hom}_{\mathrm{Grp}}(H, G) \to \mathrm{Hom}_{\mathrm{Grp}}(H/N, G/N), \mathrm{Hom}_{\mathrm{Grp}}(H/N, G/N) \to \mathrm{Hom}_{\mathrm{Grp}}(H, G)$ が引き起こす写像（像写像と逆像写像）

$$\begin{array}{ccc} \pi_* : \{H \in P(G) \mid N \subset H \text{ は } G \text{ の部分群 }\} & \longrightarrow & \{H \in P(G/N) \mid H \text{ は } G/N \text{ の部分群 }\} \\ \cup & & \cup \\ H & \longmapsto & \pi(H) = H/N \end{array}$$

$$\begin{array}{ccc} \pi^* : \{H \in P(G/N) \mid H \text{ は } G/N \text{ の部分群 }\} & \longrightarrow & \{H \in P(G) \mid N \subset H \text{ は } G \text{ の部分群 }\} \\ \cup & & \cup \\ H & \longmapsto & \pi^{-1}(H) \supset \pi^{-1}(e) = N \end{array}$$

が互いに逆写像であることを示す．π が全射であることより，$\pi(\pi^{-1}(H)) = H$．$g \in \pi^{-1}(\pi(H)) \Leftrightarrow gH \in \pi(H) \Leftrightarrow g \in H$ より，$\pi^{-1}(\pi(H)) = H$．π^*, π_* はいずれも像写像・逆像写像なので，順序もたもつ．
(2) $N \subset H \lhd G \Rightarrow \pi(H) \lhd G/N$ については，$\forall_{gN\in G/N}\ gN\pi(H)(gN)^{-1} = \pi(g)\pi(H)\pi(g^{-1}) = \pi(gHg^{-1}) = \pi(H)$ より．$H' \rhd G/N \Rightarrow \pi^{-1}(H') \lhd G$ は $\forall_{g\in G} g\pi^{-1}(H')g^{-1} = \pi^{-1}(gNH'g^{-1}N) = \pi^{-1}(H)$ より．[†34]

■

[†31] $n = 0$ の時もこの議論は成り立っている．
[†32] subgroup lattice の射があるともいう．
[†33] 像も逆像も基本は正規性を保つ．
[†34] もう一つ全称量化子 $\forall_{h\in H}$ が一番外側にあるが，記法 gHg^{-1} を用いて簡略化してしまった．

1.7　準同型定理

(1) 第一同型定理は「群の圏が正規エピ–モノ分解可能、すなわち正規エピ射のクラスとモノ射のクラスはこの圏の標準分解系 (factorization system) をなす」という圏論的事実に基づく。[a]第一同型定理は，短完全列 $0 \hookrightarrow \mathrm{Ker}\, f \hookrightarrow G \twoheadrightarrow G/\mathrm{Ker}\ \twoheadrightarrow 0$ の存在を主張しているとも捉えられる．

(2) 第二同型定理は，部分群束の，結びと N の関係は，交わりと H の関係に等しいことを主張している．

(3) 第三同型定理は 9 項補題によってアーベル圏やより一般の対象の間の写像に一般化される。それはときどき略式的に "freshman theorem" と呼ばれる、なぜならば "freshman でさえわかるからだ：N たちをキャンセルアウトするだけでよい！" まるで約分である $\dfrac{G}{H} \simeq \dfrac{G/N}{H/N}$．環に対する定理のステートメントも同様であり、正規部分群の概念がイデアルの概念に取って代わる。

第二，第三同型定理に共通することは，可逆射の基点は必ず正規部分群になることである．正規部分群を中心に回転する．normal とは，完全列の normal な射が刺さっているということが大事なんだろうと思う．こう見ると割ることの本質は比を取ることなんだろうなと思う．「どういう拡大か」．Galois の esprit が普遍している．

[a] 射が normal とは，正規部分群のように，他の対象の Ker を表していると考えられる射のことをいう．

1.7.1　準同型定理

定理 1.7.1 . 準同型写像 $f : G \to G'$ は，標準的な同型 $\overline{f}$ を引き起こす：

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle i} \\ G/\mathrm{Ker}\, f & \xrightarrow{\overline{f}} & \mathrm{Im}\, f \end{array}$$

[証明].

構成　核の定義より $f(\mathrm{Ker}\, f) = \{e'\}$ であるから，剰余群の普遍性 1.6.9 より，次を可換にする準同型 $\overline{f} : G/\mathrm{Ker}\, f \to G'$ がただ一つ存在する．

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ {\scriptstyle\pi}\downarrow & \nearrow{\scriptstyle \overline{f}} & \\ G/\mathrm{Ker}\, f & & \end{array}$$

成功　$\overline{f}$ は単射である．実際, 任意に取った $g\mathrm{Ker}\, f \in \mathrm{Ker}\, \overline{f}$ に対して, $\overline{f}(g\mathrm{Ker}\, f) = e'$ を満たすということは $\overline{f}(\pi(g)) = f(g) = e'$ すなわち $g \in \mathrm{Ker}\, f$ ということだから，$g\mathrm{Ker}\, f = \mathrm{Ker}\, f$ が従う．つまり，$\mathrm{Ker}\, \overline{f} = \{\mathrm{Ker}\, f\}$ であることがわかる．よって，$\overline{f} : G/Ker \to f(G')$ は全単射であるから，命題 1.1.7 より，$\overline{f}$ は同型である．

■

例 1.7.2 (circle group).

(1)

$$\begin{array}{ccc} \mathrm{GL}_n(A) & \xrightarrow{\det} & A^\times \\ {\scriptstyle\pi}\downarrow & \nearrow{\scriptstyle \overline{\det}} & \\ \mathrm{GL}_n(A)/\mathrm{SL}_n(A) & & \end{array}$$

(2) $SO_2(\mathbb{R})$ は $\theta \in [0, 2\pi)$ 回転に限る．

$$\begin{array}{ccc} \mathbb{R} & \xrightarrow{R(2\pi\theta)} & \mathrm{GL}_2(\mathbb{R}) \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle i} \\ \mathbb{R}/\mathbb{Z} & \dashrightarrow & SO_2(\mathbb{R}) \end{array}$$

加えてユニタリ群 $U(1)$ にも同型．短完全列 $0 \to \mathbb{Z} \to \mathbb{R} \to \mathbb{T} \to 0$ がある．円群 $\mathbb{T}$ へのアーベル群からの射 $A \to \mathbb{T}$ を（乗法的）指標という．そして，$\mathrm{Aut}(U(1)) \simeq \mathbb{Z}_2$ というのは複素共役に関係があるだろう．

(3) $n \geqslant 2$ のとき，

$$\begin{array}{ccc} S_n & \xrightarrow{\mathrm{sgn}} & \{\pm 1\} \\ {\scriptstyle\pi}\downarrow & \nearrow & \\ S_n/A_n & & \end{array}$$

□

系 1.7.3 (第二同型定理). $H \subset G$ を部分群，$N \lhd G$ を正規部分群とする．このとき，

(1) HN は部分群であり，
(2) $H \cap N \lhd H$ であり，
(3) 次の同型が定まる：

$$\begin{array}{ccc} H & \xhookrightarrow{i} & HN \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ H/(H\cap N) & \dashrightarrow & HN/N \end{array}$$

[証明].

HN は部分群　任意に $n_1h_1, n_2h_2 \in NH$ を取ると，$n_1^{-1}h_1^{-1}n_2h_2 = n_1^{-1}\underbrace{h_1^{-1}n_2h_1}_{\in N}h_1^{-1}h_2 \in NH$ より，部分群の特徴付け 1.3.4 から．

$H \cap N \lhd H$　$\forall_{g\in G}\ gN = Ng$ ならば，$\forall_{h\in H}\ h(H\cap N) = (H\cap N)h$ である．

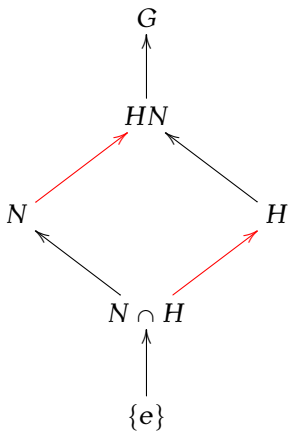
準同型定理

$$\begin{array}{ccccc} f : N & \xhookrightarrow{} & HN & \twoheadrightarrow & HN/N \\ \cup & & \cup & & \cup \\ h & \longmapsto & hN & \longmapsto & h \end{array}$$

は全射である．また，$\mathrm{Ker}\, f = H \cap N$ である．よって，これについて，準同型定理 1.7.1 より．

■

要諦 1.7.4. これは，次のような包含写像のなす部分群の束について，２つの赤い射は同じ「成長度」であることをいう．N, H の間に包含写像はあってもなくても成り立つ．NH は結びで，$N \cap H$ は交わりである．



系 1.7.5 (第三同型定理). $N \lhd G, H \lhd G$ を $N \subset H$ を満たす 2 つの正規部分群とする．このとき，$H/N \lhd G/N$ であり，

$$\begin{array}{ccc} G & \twoheadrightarrow & G/N \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ G/H & \dashrightarrow & (G/N)(H/N) \end{array}$$

[証明].

(1) $N \subset H$ より，全射 $\pi : G \twoheadrightarrow G/N$ の像が $\pi(H) = H/N$ である．全射の正規性保存命題 1.6.7 より，H/N は正規．
(2) $\operatorname{Ker} f = \pi^{-1}(H/N) = H$ より，準同型定理 1.7.1 より，$G/H \xrightarrow{\sim} (G/N)/(H/N)$ が存在する．

$$\begin{array}{ccc} G & \twoheadrightarrow & G/N \\ {\scriptstyle\pi}\downarrow & \overset{f}{\searrow} & \downarrow{\scriptstyle\pi} \\ G/H & \dashrightarrow & (G/N)(H/N) \end{array}$$

■

要諦 1.7.6. 正規部分群周りの群構造は，それぞれをより小さい正規部分群 N で割ってみても保たれる．

1.7.2　巡回群の分類

定理 1.7.7 . G を巡回群とする．

(1) G が有限ならば，$n := |G| \in \mathbb{N}$ について，$G \simeq \mathbb{Z}/n\mathbb{Z}$ である．
(2) G が無限ならば，$G \simeq \mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$.

[証明].

(1) 生成元を $G = \langle g \rangle$ とする．対応する $\mathbb{Z}$-値点 $f : \mathbb{Z} \to G$（命題 1.3.17）について，$\operatorname{Im} f = \langle g \rangle = G$．部分群 $\operatorname{Ker} \subset \mathbb{Z}$ について命題 1.3.16 より，$\exists_{n' \in \mathbb{Z}}\ \operatorname{Ker} f = n'\mathbb{Z}$．準同型定理より，$\mathbb{Z}/n'\mathbb{Z} \xrightarrow{\sim} G$.
(2) G が有限のとき，$|G| = n = n' = |\mathbb{Z}/n'\mathbb{Z}|$ をえる．G が無限群のとき，$\mathbb{Z}/n'\mathbb{Z}$ も無限群であるから，$n' = 0$ がわかる．

■

1.8　群の表示

generators and relations

一般の群を，自由群の商として捉える試みである．商写像ばかりだ．商写像による理論である．代数の極みのように，形式性が増す．数を代するという営みだと考えれば，本質的には基礎論的になるのも然りである．

例 1.8.1 (S_3 の表示)**.** 生成元 $X = \{x, y\}$ と関係式 $R = \{[xxx], [yy], [xyxy]\}$ は群 S_3 の表示を与える．

[証明].

(1) 自由群の普遍性より，$\overline{f} : F_x \twoheadrightarrow S_3$ が定まる．全射性は，$S_3 = \langle \operatorname{Im} f \rangle = \langle \sigma, \tau \rangle$ からわかる．
(2) R の構成は $R = \operatorname{Ker} \overline{f}$ を表しているが，これを構造的帰納法的に追うよりも，次のように議論することもできる．$\overline{f}([xxx]) = \sigma^3 = e, ß\overline{f}([yy]) = \tau^2 = e, \overline{f}([xyxy]) = \sigma\tau\sigma\tau = e$ より，$R \operatorname{Ker} \overline{f}$ であり，$\operatorname{Ker} \overline{f}$ は正規であるから，$\langle R \rangle_{\mathrm{nor}} \subset \operatorname{Ker} \overline{f}$．こうして全射準同型 $\widetilde{f} : F_X/\langle R \rangle_{\mathrm{nor}} \twoheadrightarrow S_3$ がただ一つ存在する．
(3) $F_X/\langle R \rangle_{\mathrm{nor}}$ の元としては，$\sigma := \pi([x]), \tau := \pi([y])$ とすると，$\tau^a\sigma^b$ $(a = 0, 1, 2, b = 0, 1)$ と言う 6 元しか存在しないから，全射 $\widetilde{f} : F_X/\langle R \rangle_{\mathrm{nor}} \twoheadrightarrow S_3$ は単射であることが必要．すなわち，$S_3 \simeq F_X/\langle R \rangle_{\mathrm{nor}}$.

■

□

例 1.8.2 (D_n の表示)**.** 二面体群 D_n について，生成元 $X = \{\sigma, \tau\}$ と関係式 $R = \{[\sigma^n], [\tau^2], [\sigma\tau\sigma\tau^{-1}]\}$ は群 D_n の表示を与える．つまり，写像

$$\begin{array}{ccc} \varphi : F_X & \longrightarrow & D_n \\ \cup & & \cup \\ \sigma & \longmapsto & \sigma \\ \tau & \longmapsto & \tau \end{array}$$

は全射で，$\mathrm{Ker}\,\varphi = \langle \sigma^n, \tau^2, \tau\sigma\tau^{-1}\sigma \rangle_{\mathrm{nor}}$ であるから，準同型定理より $F_X/\langle R \rangle_{\mathrm{nor}} \simeq D_n$. □

1.8.1　自由群

定義 1.8.3 (word).　(1) $X^{-1} := \{x^{-1} \mid x \in X\}$ に対して，$X \cup X^{-1}$ の有限列を語という．

(2) $* : W \times W \hookrightarrow W$ を結合という．

(3) 縮約 $W \hookrightarrow W$ を，語 $(a_i) \in W$ について $a_{i+1} = a_i^{-1}$ が成り立っていたとき，この 2 文字を取り除く操作として定める．これ以上縮約できない語を縮約的という．

(4) 同値関係 $W \sim W'$ を，次を満たす縮約列 $(W_i)_{i \in n}$ が存在することと定める：$W_0 = W, W_n = W', \forall_{i \in n}\ W_{i+1}$ は W_i の縮約であるか，W_i は W_{i+1} の縮約である．

(5) この同値関係についての同値類を $[W]$ と書き，$^{>\omega}(X \cup X^{-1})$ の商集合を F_X と書く．

(6) 標準単射 $\iota_X : X \to F_X$ が定まる．

補題 1.8.4 (free group). $(F_X, *, ^{-1})$ は群をなす．

[証明].

well-definedness　$W_1 \sim W_1', W_2 \sim W_2'$ とする．同じような縮約を課せば良いから，$W_1 * W_2 \sim W_1' \sim W_2'$ である．

結合律　文字の結合は結合的である．

単位元　[] は結合について中立的である．

逆元　$W = a_1 \cdots a_n$ のとき，$[a_n^{-1} \cdots a_1^{-1}]$ は逆元である．

■

補題 1.8.5 . F_X は $\mathrm{Im}\,\iota$ で生成される．

[証明]. $F_X \subset \langle \iota_X(X) \rangle$ を示せば良い．これは F_X の作り方についての構造的帰納法から従う． ■

1.8.2　自由群の普遍性

自由群から群への写像を構成するには，n 元の行き先を定めることに同値．線型空間とは，体上に自由生成された加群である．
すごく基礎論的だし，lambda 計算っぽい．

命題 1.8.6 (universality of free group). 群 G への写像 $f : X \to G$ に対して，次を Set 上可換にする群準同型 $\bar{f} : F_X \to G$ がただ一つ存在する：

$$\begin{array}{ccc} X & \xrightarrow{f} & G \\ {\scriptstyle \iota_X}\downarrow & \nearrow_{U(\bar{f})} & \\ U(F_X) & & \end{array}$$

[証明]. F_X の作り方についての構造的帰納法から従う．

(1) $f : X \to G$ は $f : X \cup X^{-1} \to G$ に延長する．

(2) $\tilde{f} : {}^{>\omega}(X \cup X^{-1}) \to G$ に延長する．

(3) 一意性：

■

系 1.8.7. $\mathbb{Z} \sim F_1$.

要諦 1.8.8. 普遍性のみから，数学的対象の同型類が指定できる．このようにして，代数は定義に戻らないことが大事になる．これが表現可能関手の一般理論につながる．

命題 1.8.9 (生成の特徴付け). $X \subset G$ を部分集合とする．包含写像 $i : X \hookrightarrow G$ が定める準同型 $\bar{i} : F_X \hookrightarrow G$ の像は，X が生成する部分群 $\langle X \rangle$ である．特に X が生成系であることは，$\bar{i} : F_X \twoheadrightarrow G$ が全射であることに同値.

[証明].

$\operatorname{Im} \bar{i} \supset \langle X \rangle$　$\bar{i}$ は i の延長だから，$\operatorname{Im} \bar{i}(X) \supset i(X) = X$ より，$\operatorname{Im} \bar{i} \supset \langle X \rangle$.
$\operatorname{Im} \bar{i} \subset \langle X \rangle$　$\operatorname{Im} \bar{i}$ の元は $i(X)$ の元の結合または逆のみからなるから，$\operatorname{Im} \bar{i} \subset \langle X \rangle$ でもある．

■

要諦 1.8.10. この最小性，閉性が，自由群構成の妙である．

命題 1.8.11 (自由群の完全代表系).

(1) W を語，W', W'' を縮約的な語とする．$W \sim W' \wedge W \sim W''$ ならば，$W' = W''$ である．
(2) $W \sim W'$ とする．このとき，$W \sim W'', W' \sim W''$ を満たす語 W'' が存在する．[†35]
(3) W, W' を相異なる縮約的な語とする．このとき，W, W' は同値でない．

1.8.3　生成系と関係式による表示

> X が全ての可能な計算列を与え，R が計算規則を縮約に仮託した形で与える．

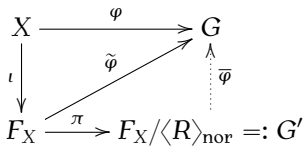
定義 1.8.12 (generators and relations). $R \subset F_X$ を部分集合とする．F_X の正規部分群であって，R を含む最小のものを $\langle R \rangle_{\mathrm{nor}}$ と表す．これによる剰余群 $F_X/\langle R \rangle_{\mathrm{nor}}$ を，**生成系 X と関係式 R によって定まる群**と呼ぶ.

命題 1.8.13 (representation). G を群とする.

(1) 集合 X とその部分集合 $R \subset F_X$ であって，$G \simeq F_X/\langle R \rangle_{\mathrm{nor}}$ を満たすものが存在する.
(2) G が有限群のとき，X, R は有限にとれる.

[証明]. $X := \{x_g \mid g \in G\}, R = \{[x_g x_h x_{gh}^{-1}] \mid g, h \in G\}$ とすると，集合の同型 $\varphi : X \xrightarrow{\sim} G$ が存在する．$G' := F_X/\langle R \rangle_{\mathrm{nor}}$ とし，$[x_g] \in F_X$ の $\pi : F_X \to F_X/\langle R \rangle_{\mathrm{nor}}$ による像を $y_g := \pi([x_g])$ と表すこととする．補題 1.8.5 より，$F_X = \langle \iota_X(X) \rangle$ だから，$S := \pi(\iota_X(X)) = \{y_g \mid g \in G\}$ とすると，$G' = \pi(F_X) = \pi(\langle \iota(X) \rangle) = \langle S \rangle$ を満たす．最後の等号は群準同型 $\pi : F_X \twoheadrightarrow F_X/\langle R \rangle_{\mathrm{nor}}$ の関手性.

(1) $G' = S$ である．$G' \subset \langle S \rangle$ が構成よりわかる．[†36]
(2) $G \simeq G'$ である.



まず自由群の普遍性 1.8.6 より，群準同型 $\tilde{\varphi} : F_X \twoheadrightarrow G$ が存在し，これは φ が同型であることより全射である．構成より $R \subset \operatorname{Ker} \tilde{\varphi}$ を満たすから，剰余群の普遍性 1.6.9 より，群準同型 $\bar{\varphi} : G' \to G$ が定まる．いま，定め方より $\bar{\varphi}$ は全単射で

[†35] 結びみたいなものである.
[†36] 命題 1.8.9 のような妙義.

ある．実際，任意の $g \in G$ に対して，$\overline{\varphi}(y_g) = \varphi([x_g]) = g$ より全射．$[y_g] \in \mathrm{Ker}\ \overline{\varphi}$ ならば，$e = \overline{\varphi}([y_g]) = g$ より，$y_g = y_e = e \in G'$ より，$\mathrm{Ker}\ \overline{\varphi} = \{e\}$ より単射．

(3) 上記の構成は，$|G| < \infty$ のとき，X, R は有限である．

■

1.9　Abel 群論

Abel 群と Abelian category

任意の Abel 群は $\mathbb{Z}$ 上の加群をみなすことができ ($\mathbb{Z}\mathrm{Mod} \simeq \mathrm{Ab}$)，2 つの「捩れ」の定義が一致する．Abel 群を扱う上でのエッセンス（アーベル圏に昇華される）の全てが詰まった定理．だが，単因子論の知識があるとそちらにもすぐに帰着するらしい．

(1) 有限アーベル群は e を中心に有限位数の元が回転している，よってこれをいくつかの周回道に分解できるというのがアーベル群の構造定理である（結果分解の仕方によって，位数に依存してアーベル群の数を数えられる）．
(2) Abel 群を射影子を用いて分解する：$e \circ e = e \Rightarrow \mathrm{Im}\,(e) \oplus \mathrm{Ker}\,(e)$．特に，$i : N \hookrightarrow M$ は N が正規である時は分解は $M \simeq N \times M/N$ と表せ，Abel 群の分解はこの場合に当たる．
(3) まず p-群への分解が解る，これは一般固有空間分解に当たる．元の位数 n から素因数 $p|n$ を乱択していくと，$n = p^m n'$ を用いて世界を最大周期 p^m の軌道とそれ以外に分ける射影子が取れる．
(4) 最終的に p-群の形を決定するには，射影子を構成するのに入射加群の技術が要るのみである．p-群の任意の元は正規部分群を生成するが，$i : \langle x_0 \rangle \hookrightarrow M$ はいつでも同型 $\langle x_0 \rangle \xrightarrow{\sim} \mathbb{Z}/p^m\mathbb{Z}$ とその延長の対応を用いて引き戻せる．

定理 1.9.1 (fundamental theorem of finitely generated abelian groups). 任意の有限生成アーベル群 A は，巡回群 $\mathbb{Z}/p^k\mathbb{Z}$ $(p \in \mathcal{P}, k \in \mathbb{N})$ とその極限としての $\mathbb{Z}$ との直積に同型である：

$$A \simeq \mathbb{Z}^n \oplus \bigoplus_i \mathbb{Z}/p_i^{k_i}\mathbb{Z}$$

1.9.1　射影子による p 群への分解

idempotent morphism による分解

アーベル群は部分群について，その内部と，それ自信を抽象化した外部とで完全に分離でき，群の間の言葉で言えば直積になる．それを検出するのが射影子であり，包含写像の引き戻しとして探せる．なぜならば，$r : A \to B, s : B \to A$ であって，$r \circ s = \mathrm{id}_B, s \circ r = e$ を満たすとき (この条件をみたす e を split idempotent といい，(r, s) を retract という)，$e \circ e = (s \circ r) \circ (s \circ r) = s \circ r = e$ が成り立つから，splitness の検出に帰着する．射影子は圏論の技法で，$e \cdot e = e$ という square to itself を満たすならば，射が「落とす情報」と「落とさない情報」により，$\mathrm{Im}\, e \oplus \mathrm{Ker}\, e$ に分解する（様な圏が重要になる）．[a] 即ち，なにかしらの直和対象からの射影 p に対して，包含射が続く様なもの $i \circ p$ が射影子の特徴づけである．この理論には莫大な応用があると思ったら，圏論的な視点だけでなく，射影は解析学全体（函数解析学，数値解析）に通底するトピックだと気づいた．

[a] Accordingly, one is interested in those categories for which every idempotent is split. These are called idempotent complete categories or Cauchy complete categories.https://ncatlab.org/nlab/show/idempotent

補題 1.9.2 (アーベル群の分解（射影子のアーベル群に対する場合の特徴付け）). M をアーベル群，$N \subset M$ を部分群とする．$i : N \hookrightarrow M$ を包含写像とする．i の引き戻し r が存在するならば，すなわち，$f|_N = \mathrm{id}_N$ を満たす群準同型 $f : M \to N$ が存在するならば，$M \simeq N \times M/N$ である．

[証明]. $\phi := (f, \pi) : M \to N \times M/N$ とすると，これが可逆であることを示せば良い．

単射性　任意の $m \in M$ について，

$$\begin{aligned}\phi(m) = 0 &\Leftrightarrow f(m) = 0 \wedge \pi(m) = 0\\ &\Leftrightarrow (m = 0 \vee m \in M\backslash N) \wedge (m \in N)\\ &\Leftrightarrow m = 0.\end{aligned}$$

全射性　任意の $(n, x) \in N \times M/N$ について，$\pi : M \twoheadrightarrow M/N$ は全射だから，$m \in \pi^{-1}(x)$ が取れる．これについて，$\phi(m) = (f(m), x)$ であるが，もし $f(m) \notin N$ ならば，$m' := m - f(m) + n$ とすると，$f(m) \in N$ なので，$\pi(m') = \pi(m) - \pi(f(m)) + n = m - 0 + 0$ であり，かつ，$f(m') = f(m) - f(f(m)) + f(n) = f(m) - f(m) + n = n$ より，$m' \in \phi^{-1}(n, x)$.

■

要諦 1.9.3 (射影子の一般化)**.** この f とは何か？確かに $f \circ f = f$ を満たすな！吸収律とは，「情報をある自然な方法に従って裁断し，それ以外には変化を加えない」写像を特定するのに用いられる代数法則である．$M = M_1 \times M_2, N = M_1 \times \{0\}$ とすると，$M = M_1 \times M_2 \simeq N \times M/N$ であり，$i : N \hookrightarrow M$ には切断 $f : M \to N$ が存在して $f|_N = \mathrm{id}_N$ である．これを，群が直積に分解できる場合の特徴付けとして用いている．

余核とはどう違うのか．半直積との双対性は何か．

要諦 1.9.4 (直観)**.** $f : M \to N$ で $f|_N = \mathrm{id}_N$ を満たすものは，M/N の部分の扱いに困る．全てを e に対応させることはできない．実際，ある $m \in M\backslash N$ について $f(m) = e$ だとすると，勝手に取った $n \in N$ について，$nm \notin N$ であるが，$f(nm) = f(n)f(m) = n$ が必要．つまり，M の N についてのそれぞれの剰余類を，N に重ねる必要がある．

補題 1.9.5 (p-群への分解)． M を Abel 群とする．次の 2 条件を満たす有限 Abel 群 $M_1, \cdots, M_r$ と素数 $p_1, \cdots, p_r$ と整数 $m_1, \cdots, m_r \geqslant 0$ が存在する：

(1) $\forall_{1 \leqslant i \leqslant r}\ \forall_{x \in M_i}\ p_i^{m_i} x = 0$.
(2) $M \simeq M_1 \times \cdots \times M_r$.

[証明]．

方針　$n := |M|$ についての帰納法で示す．$n = 1$ の時は $r = 1$ とすれば $M = M_1 = 1$ で，$p_1 = 2, m_1 = 0$ などとすれば良い．そこで，$n > 1$ の場合を考える．

p-群の抽出　$x_0 \in M\backslash\{0\}$ が取れる．この位数 $n_0 > 1$ を割り切る素数 p が取れる．これらに対して $x_0 := \dfrac{n_0}{p} x_0$ と定め直すことにより，元 $x \in M\backslash\{0\}$ を位数 p の元だと考えて良い．

すると，Lagrange の定理 1.5.6 より $p|n$ であるから，整数 $m \geqslant 1$ と p と互いに素な整数 $n' \geqslant 1$ とが存在して $n = n'p^m$ を満たす．$N := \{x \in M \mid p^m x = 0\}$ と置くと，これは M の部分群となる．

分解　ここで，$\exists_{a,b \in \mathbb{Z}}\ n'a + p^m b = 1$ 即ち $n' = \dfrac{1 - p^m b}{a}$ であるから，これを用いて準同型を

$$\begin{array}{ccc} f : M & \longrightarrow & M \\ \cup & & \cup \\ x & \longmapsto & n'ax \end{array}$$

と定める．これは，

(1)　$p^m(n'ax) = p^m(1 - p^m b)x = 0 - 0 = 0$ より $\mathrm{Im}\, f \subset N$ で，
(2)　$x \in N$ に対して，$f(x) = n'ax = (1 - p^m b)x = x - 0 = x$ を満たす

から，補題より，分解 $M \simeq N \times M/N$ を引き起こす．

いま，少なくとも $x_0 (\neq 0) \in N$ より $\{0\} \subsetneq N$ であるから，$|N/M| < n$．帰納法の仮定から，分解は続く．

■

要諦 1.9.6. n の因数分解をしている．$|M| > 1$ を満たす Abel 群 M について，位数 p の元 x を選べる．これについて，周期が p の冪である元を集めてくると，これに対する射影子が見つかるので，分解することがわかる．この算譜は最後まで繰り返せる．

1.9.2　入射的対象による p 群の分解

補題 1.9.7 (p-群の分解). M を有限アーベル群とし，N をその部分群とする．

(1) 任意の準同型 $f : N \to \mathbb{Q}/\mathbb{Z}$ は，包含写像 $i : N \hookrightarrow M$ についての延長 $\overline{f} : M \to \mathbb{Q}/\mathbb{Z}$ が存在する：

$$\begin{array}{ccc} N & \xrightarrow{f} & \mathbb{Q}/\mathbb{Z} \\ \downarrow & \nearrow_{\overline{f}} & \\ M & & \end{array}$$

(2) 特に，p を素数，$m \geqslant 0$ を整数とし，$\forall_{x \in M}\ p^m x = 0$ とする（群 M は p-群）．このとき，任意の準同型 $f : N \to \mathbb{Z}/p^m\mathbb{Z}$ に対して，準同型 $\overline{f} : M \to \mathbb{Z}/p^m\mathbb{Z}$ であって，$\overline{f}|_N = f$ を満たすものが存在する．

[証明].

(1)⇒(2)　同型（p-進小数表示）[†37]

$$\begin{array}{ccc} \mathbb{Z}/p^m\mathbb{Z} & \xrightarrow{\sim} & p^{-m}\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z} \\ \cup & & \cup \\ n + p^m\mathbb{Z} & \longmapsto & p^{-m}n + \mathbb{Z} \end{array}$$

が存在するから，準同型 $f : N \to p^{-m}\mathbb{Z}/\mathbb{Z}$ について示せば良い．射 $N \xrightarrow{f} p^{-m}\mathbb{Z}/\mathbb{Z} \hookrightarrow \mathbb{Q}/\mathbb{Z}$ に (1) を用いることにより，延長 $\overline{f} : M \to \mathbb{Q}/\mathbb{Z}$ を得る．

$$\begin{array}{ccccc} N & \xrightarrow{f} & p^{-m}\mathbb{Z}/\mathbb{Z} & \xhookrightarrow{i} & \mathbb{Q}/\mathbb{Z} \\ {\scriptstyle i}\downarrow & \nearrow_{\overline{f}} & & & \\ M & & & & \end{array}$$

ここで，任意の $x \in M$ について，$p^m\overline{f}(x) = \overline{f}(p^m x) = \overline{f}(0) = 0$ より，$x \in p^{-m}\mathbb{Z}/\mathbb{Z} = \{y \in \mathbb{Q}/\mathbb{Z} \mid p^m y = 0\}$. [†38] よって，$\operatorname{Im}\overline{f} \subset p^{-m}\mathbb{Z}/\mathbb{Z}$ だから，$\overline{f}|_N = f$ を満たす準同型 $\overline{f} : M \to p^{-m}\mathbb{Z}/\mathbb{Z}$ が定まった．

(1) **Step1：$M = \mathbb{Z}$ のとき**　部分群は $\exists_{n \in \mathbb{N}}\ N = n\mathbb{Z}$ と表せる（命題 1.3.16）．$n = 0$ の時は，$\overline{f} = 0$ とすれば良い．$n > 0$ の時は，$f(n) = r + \mathbb{Z}$ となる $r \in \mathbb{Q}$ を用いて，$\overline{f}(m) = \dfrac{rm}{n} + \mathbb{Z}$ と定めれば良い. [†39]

$$\begin{array}{ccc} n\mathbb{Z} & \xrightarrow{f} & \mathbb{Q}/\mathbb{Z} \\ {\scriptstyle i}\downarrow & \nearrow_{\overline{f}} & \\ \mathbb{Z} & & \end{array}$$

Step2：M が巡回群のとき　生成元を $M =: \langle x \rangle$ とおくと，全射準同型

$$\begin{array}{ccc} \phi : \mathbb{Z} & \longrightarrow & M \\ \cup & & \cup \\ n & \longmapsto & nx \end{array}$$

が定まる．

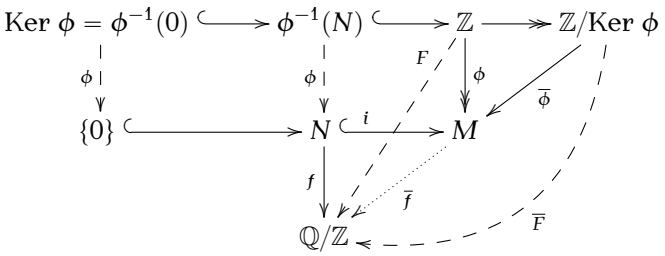
(1)　f を $\mathbb{Z}$ の部分群 $\phi^{-1}(N)$ から伸ばした射 $f \circ \phi|_{\phi^{-1}(N)} : \phi^{-1}(N) \twoheadrightarrow^{\phi} N \xrightarrow{f} \mathbb{Q}/\mathbb{Z}$ について，上述の議論より，延長

[†37] $\mathbb{Z}/p^m\mathbb{Z}$ とは，位数 p^m の巡回群であるが，これを p^m を分母にもつ真分数からなる群と考えても同一視できる，という話である．確かに，周期 p^m の群は分母 p^m の分数の世界で考えるのも直感的.

[†38] つまり，$p^{-m}\mathbb{Z}/\mathbb{Z} = \{y \in \mathbb{Q} \mid p^m y \in \mathbb{Z}\}$

[†39] f が $[n]$ を $\mathbb{Q}/Z$ のどこに写すかわからないが，これを基準として目盛りを細分すれば，$\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$ を 1 つ得る．射 $n\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$ はまさに，$[0,1]$ の繰り返しとしての数直線に附ける目盛りである．

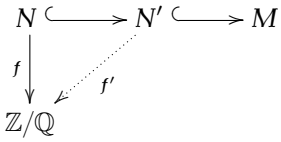
$F:\mathbb{Z}\to\mathbb{Q}/\mathbb{Z}$ で $F|_{\phi^{-1}(N)}=f\circ\phi$ を満たすものが存在する．



(2)　この F について，$F|_{\operatorname{Ker}\phi}=(f\circ\phi)|_{\operatorname{Ker}\phi}=0$ であるから，$\operatorname{Ker}\phi\subset\operatorname{Ker}F$ で，剰余群の普遍性 1.6.9 より，$\overline{F}:\mathbb{Z}/\operatorname{Ker}\phi\to\mathbb{Q}/\mathbb{Z}$ が定まる．

(3)　これに，準同型定理 1.7.1 による同型 $\overline{\phi}:\mathbb{Z}/\operatorname{Ker}\phi\xrightarrow{\sim}M$ の逆を合成して $\overline{f}:=\overline{F}\circ\overline{\phi}^{-1}:M\to\mathbb{Q}/\mathbb{Z}$ とすると，これは図式を可換にするから，条件 $\overline{f}|_N=f$ を満たす．

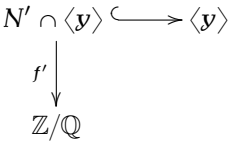
Step3：M **が一般の群のとき**　次の図式を可換にする群と準同型の組 (N',f') の全体を S とする．



$\{|N'|\in\mathbb{N}\mid(N',f')\in S\}\subset[|M|]$ は有界な集合だから，その最大値をとる N' を定めると，これが M であることを背理法で示す．

(1)　$y\in M\backslash N$ が取れるとすると，$N'+\langle y\rangle$ は N' よりも真に大きい M の部分群であるのに，$f'':N'+\langle y\rangle\to\mathbb{Q}/\mathbb{Z}$ が存在して，$(f'',N'+\langle y\rangle)\in S$ であることを示す．

(2)　まず，f' の制限 $f'|_{N'\cap\langle y\rangle}:N'\cap\langle y\rangle\to\mathbb{Z}/\mathbb{Q}$ は，上述の議論により巡回群 $\langle y\rangle$ 上に延長する：$\exists f''_y:\langle y\rangle\to\mathbb{Z}/\mathbb{Q}$ s.t. $f''_y|_{N'\cap\langle y\rangle}=f'$．



(3)　これを用いて，$f'':=f'+f''_y$ と定めると，これは well-defined な群準同型で，$f''|_N=f'|_N=f$ を満たすから，$f''\in S$ である．実際，$x+ny=x'+n'y\ \Leftrightarrow\ x-x'=y(n'-n)\in N\cap\langle y\rangle$ を満たすとき，右辺は $N\cap\langle y\rangle$ の元であるから，

$$f''(-ny+n'y)=-f''_y(ny)+f''_y(n'y)=f(x)-f(x')$$

即ち，$f(x)+f''_y(ny)=f(x')+f''_y(n'y)$ が従う．

■

要諦 1.9.8 (アーベル圏の様子とアーベル群の巡回群構造についての構造的帰納法)**.**

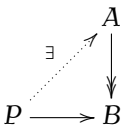
(1) アーベル群 A が $\mathbb{Z}$-加群として入射的であるための必要十分条件は，可除であることである：$\forall_{n\in\mathbb{N}}\ nG=G$（「$n$ 回足す」という G の移動が n に依らず全射）．今回の (1) の証明では，$\mathbb{Q}/\mathbb{Z}$ のこの性質しか使っておらず，任意の入射的加群に議論を一般化できる．そこで，$\mathbb{Q},\mathbb{R}$ は入射的．入射加群の任意の群による商は入射的である．$\mathbb{Q}/\mathbb{Z},\mathbb{R}/\mathbb{Z}\simeq\mathbb{T}$ も入射的．$\mathbb{Z}$ は入射的でないし，$\mathbb{Z}/n\mathbb{Z}$ も入射的ではない．

(2) $\mathbb{Z}$ についての理論が大きな後ろ支えになって，巡回群の理論を支える構図が Step2.

(3) Step3 に至っては**巡回群への分解についての構造的帰納法**である．構造的帰納法の本質を「延ばせるだけ延ばした時に，全体まで至らないと矛盾」という部分のみを抽出している．なるほど，有限アーベル群についての，緻密な論理の糸を Ab の精神に従って構築した算譜であるな．美しすぎる．

注 1.9.9. Zorn の補題を用いると，Step3 の議論を，任意のアーベル群 M とその部分群 N について拡張できる．

定義 1.9.10 (projective object). 対象 $P \in C$ が射影的であるとは，$P \to B$ が任意の epi $A \twoheadrightarrow B$ について分解する (left lifting property) ことをいう：



これは，共変 Hom 関手 $\mathrm{Hom}(P, -)$ が epi を保つことに同値.

注 1.9.11. Set で全ての対象が射影的であることは，選択公理に同値．ほとんどの具体圏の自由対象は射影的である．この双対概念である入射的対象は，延長に関係がある.

命題 1.9.12 (入射的対象の特徴付け). 次の 4 条件は同値である.

(1) アーベル群 A は可除である.
(2) A は圏 Ab の入射的対象である.
(3) Hom 関手 $\mathrm{Hom}_{\mathrm{Ab}}(-, A) : \mathrm{Ab}^{\mathrm{op}} \to \mathrm{Ab}$ は完全である.
(4) 任意の単射 $N \hookrightarrow M$ に対して，$\mathrm{Hom}(M, Q) \twoheadrightarrow \mathrm{Hom}(N, Q)$ は全射.

入射的対象は俺の霊性

Set では f_* は全射を全射に写し，f^* は全射を単射に写す．この時の表現対象がそれぞれ，射影的対象と入射的対象となる.

1.9.3　有限アーベル群の構造定理の証明

structure theorem of finite abelian group

Kronecker (1870) の定理．群の位数を因数分解した後に，各素因数の冪にどう分解するかの自由度が残る．もし $x = p_1^{m_1} \cdots p_r^{m_r}$ に対して $\mathbb{Z}/p_1^{m_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_r^{m_r}\mathbb{Z}$ と分解された場合，これは巡回群となる．$\mathbb{Z}/12\mathbb{Z} \simeq \mathbb{Z}/4 \oplus \mathbb{Z}/3$ など．$\mathbb{Z}/p_i\mathbb{Z} \oplus \mathbb{Z}/p_i^{m_i-1}$ と分解するとまた別のアーベル群をうみ，この方法で位数 x のアーベル群の個数を数え上げることができる.
あるいは見方を変えて，完全には分解し尽くさないことにすると，a_1 を G の冪数 (元の位数の最小公倍数) として，$a_{i+1} | a_i$ を満たす列 $(a_1, \cdots, a_r)$ は順序も含めて一意に定まり，各位数の巡回群への分解 $G \simeq \mathbb{Z}/a_1\mathbb{Z} \oplus \cdots \mathbb{Z}/a_n\mathbb{Z}$ が定まる．この数列 G を普遍系といい，各 a_i を単因子 (invariant factor) といい，単因子の理論の一部とみれる.

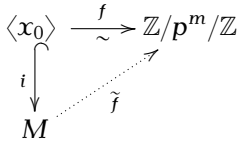
定理 1.9.13 (fundamental theorem of finite abelian groups). 有限アーベル群 M に対して，整数 $r \geqslant 0$，素数 $p_1, \cdots, p_r$，整数 $m_1, \cdots, m_r \geqslant 1$ が存在して，

$$M \simeq \mathbb{Z}/p_1^{m_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{m_r}\mathbb{Z}$$

を満たす．また，列 $\{(p_i, k_i)\}_i$ は並べ替えを除いて一意に定まる.

[証明].

存在証明　p-群への分解補題 1.9.5 より，あとは，任意の p 群 $M : \forall_{x \in M}\ p^m x = 0$ について，$\exists_{r \geqslant 0}\ \exists_{m_1, \cdots, m_r \geqslant 1}\ M \simeq \mathbb{Z}/p^{m_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{m_r}\mathbb{Z}$ を示せば良い．これを M の位数についての帰納法によって証明する．$|M| = 1$ のとき，$r = 0$ とすれば，0 項直積は自明群とする．$|M| > 1$ とすると，このとき $m \geqslant 1$ である．m を条件 $\forall_{x \in M}\ p^m x = 0$ を満たすもののうち最小のものとすると，$\exists_{x_0 \in M}\ p^{m-1} x_0 \neq 0$．つまり，位数 p^m の元 $x_0 \in M$ が存在する．よって，生成元を対応させることで同型 $f : \langle x_0 \rangle \xrightarrow{\sim} \mathbb{Z}/p^m\mathbb{Z}$ を得る．これに対して Abel 群の包含 $\langle x_0 \rangle \subset M$ に沿った準同型の延長補題 1.9.7 より，準同型 $\tilde{f} : M \to \mathbb{Z}/p^m\mathbb{Z}$ を得る：



これを用いて $\varphi := f^{-1} \circ \tilde{f}$ と定めると，これは i の引き戻しで，$\varphi|_{\langle x_0 \rangle} = \mathrm{id}_{\langle x_0 \rangle}$ を満たすから，射影子による分解補題 1.9.2 より，$M \simeq \langle x_0 \rangle \times M/\langle x_0 \rangle \simeq \mathbb{Z}/p^m\mathbb{Z} \times M/\langle x_0 \rangle$ を得る．$|M/\langle x_0 \rangle| = p^{n-m} < p^m$ より，帰納法は続く．

一意性証明　$M \simeq \otimes_{i\in[r]} \mathbb{Z}/p_i^{m_i}\mathbb{Z}$ と仮定する．このとき，パラメータの空間 $\mathcal{P} \times \mathbb{N}$ 上の列 $\{(p_i, m_i)\}_{i\in[r]}$ の中で，任意にとった (p, m) に対して，$(p_i, m_i) = (p, m)$ を満たす添字 i の数が（M, p, k の関数として）定まっていることを示せば良い．

まず，任意の (p, m) について，p^k を周期にもつ元の数は，各因子 $\mathbb{Z}/p_i^{m_i}\mathbb{Z}$ について，

$$\left|\left\{x \in \mathbb{Z}/p_i^{m_i}\mathbb{Z} \mid p^k x = 0\right\}\right| = \begin{cases} p^{\min\{k,m_i\}}, & p_i = p, \\ 1, & p_i \neq p \end{cases}$$

であるから，M 内では

$$\left|\left\{x \in M \mid p^k x = 0\right\}\right| = \prod_{p_i=p} p^{\min\{k,m_i\}}$$

よって，

$$\log_p \left|\left\{x \in M \mid p^k x = 0\right\}\right| = \sum_{p_i=p} \min\{k, m_i\}$$

これに対して，

$$\begin{aligned} \sum_{p_i=p} \min\{k, m_i\} - \sum_{p_i=p} \min\{k-1, m_i\} &= \sum_{p_i=p} (\min\{k, m_i\} - \min\{k-1, m_i\}) \\ &= \sum_{p_i=p, m_i \leqslant k-1} (\min\{k, m_i\} - \min\{k-1, m_i\}) + \sum_{p_i=p, m_i \geqslant k} (\min\{k, m_i\} - \min\{k-1, m \\ &= 0 + \sum_{p_i=p, m_i \geqslant k} 1 = |\{i \in [r] \mid p_i = p, m_i \geqslant k\}| \end{aligned}$$

が成り立つから，最右辺も M, k, p の関数．よって，$|\{i \in [r] \mid p_i = p, m_i = k\}|$ も M, p, k の min を用いた関数．

■

要諦 1.9.14.

(1) 存在証明は，任意の p-群 M に対して，射影子を構成する算譜を与えている．
(2) 一意性証明は，組 (p_i, m_i) を定める個数関数 $\mathcal{P} \times \mathbb{N} \to \mathbb{N}$ を構成している．

例 1.9.15 (elementary abelian group とは有限体上の有限次元線型空間のこと)**.** 任意の非自明な元の位数が p であるような有限群を**基本アーベル群**という．有限アーベル群の構造定理より，このような有限群は $\exists_{n\in\mathbb{N}} (\mathbb{Z}/p\mathbb{Z})^n$ と表せる．これは，n 次元 $\mathbb{F}_p$-線型空間の構造を持つ：$(\mathbb{Z}/p\mathbb{Z})^n \simeq \mathbb{F}_p^n$，とも表現できる．このような群は $n \geqslant 2$ のとき巡回群ではない 1.9.18.

一番簡単な基本アーベル群は Klein の四元群 $(\mathbb{Z}/2\mathbb{Z})^2$ である．□

例 1.9.16 (Klein の四元群の一般化)**.** 任意の素数 p について，位数 p^2 のアーベル群とは，同型を除いて次の 2 種類しかない：$(\mathbb{Z}/p\mathbb{Z}) \oplus (\mathbb{Z}/p\mathbb{Z})$ または $(\mathbb{Z}/p^2\mathbb{Z})$.　□

例 1.9.17 (一意性証明の算譜抽出)**.** 乗法群 $(\mathbb{Z}/16\mathbb{Z})^\times$ は，$\overline{n} \in \mathbb{Z}/16\mathbb{Z}$ が可逆であることが奇数であることに同値になるから，$|(\mathbb{Z}/16\mathbb{Z})^\times| = 8$ が解る．

(1) $\left\{x \in (\mathbb{Z}/16\mathbb{Z})^\times \mid x = \overline{1}\right\} = \{\overline{1}\}$ なので $\log_2|\{x \in (\mathbb{Z}/16\mathbb{Z})^\times \mid x = \overline{1}\}| = 0$.
(2) $\left\{x \in (\mathbb{Z}/16\mathbb{Z})^\times \mid x^2 = \overline{1}\right\} = \{\overline{1}, \overline{7}, \overline{9}, \overline{15}\}$ なので $\log_2|\{x \in (\mathbb{Z}/16\mathbb{Z})^\times \mid x^2 = \overline{1}\}| = 2$.
(3) $\left\{x \in (\mathbb{Z}/16\mathbb{Z})^\times \mid x^4 = \overline{1}\right\} = (\mathbb{Z}/16\mathbb{Z})^\times$ なので $\log_2|\{x \in (\mathbb{Z}/16\mathbb{Z})^\times \mid x^4 = \overline{1}\}| = 3$.

よって，

$$|\{i \mid m_i \geqslant 1\}| = 2 - 0 = 2, \qquad |\{i \mid m_i \geqslant 2\}| = 3 - 2 = 1,$$

であるから，$r = 2$ で，$(m_1, m_2) = (1, 2), (2, 1)$ しかありえない．よって，$(\mathbb{Z}/16\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$．2-torsion と 4-torsion である．□

1.9.4　巡回群の構造定理

相異なる素数 p について，相異なる基本アーベル p 群に分解できること（すなわち，$p_1^{m_1},\cdots,p_n^{m_n}$ が互いに素であること）が，巡回群の特徴付けとなる．

定理 1.9.18 (fundamental theorem of cyclic groups). 有限アーベル群 $M \simeq \mathbb{Z}/p_1^{m_1}\mathbb{Z}\times\cdots\times\mathbb{Z}/p_r^{m_r}\mathbb{Z}$ について，次の 3 条件は同値．

(1) M は巡回群である．
(2) 任意の素数 p について，$|\{x\in M \mid px=0\}| \leqslant p$.[†40]
(3) $p_1,\cdots,p_r$ は相異なる．[†41]

巡回群 $\mathbb{Z}/m\mathbb{Z}$ では p_i は互いに異なり，k_i は m の素因数分解の p_i の冪である．

[証明].

(1)⇒(2)　M を巡回群とすると，位数は $p_1^{m_1}\cdots p_r^{m_r}$ より，$M\simeq\mathbb{Z}/p_1^{m_1}\cdots p_r^{m_r}\mathbb{Z}$ だから，

$$|\{x\in M \mid px=0\}| = \begin{cases} p, & p\in\{p_1,\cdots,p_r\},\\ 1, & \text{otherwise.}\end{cases}$$

(2)⇒(3)　(2) の条件は，$\{p_i\}_{i\in[r]}$ の中に p が含まれるとしてもたかだか 1 つだということに同値であるから．もし，$(p,m_1),(p,m_2)\in((p_i,m_i))_{i\in[r]}$ として $m_1\neq m_2$ とすると，$|\{x\in M \mid px=0\}|\geqslant p^2$ がしたがってしまう．
もっと直接導けば，$|\{x\in M \mid px=0\}|$ は各 $\mathbb{Z}/p_i^{m_i}\mathbb{Z}$ の中の位数 p の巡回部分群の元の数を数えて積を取ることに同値だから，

$$|\{x\in M \mid px=0\}| = \prod_{p_i=p} p = p^{|\{i|p_i=p\}} \leqslant p$$

は，各 p に対して対応する (p_i,m_i) はただ一つ，すなわち各 $p_1,\cdots,p_r$ は異なることをいっている．

(3)⇒(1)　商写像の積 $\pi:\mathbb{Z}\twoheadrightarrow\mathbb{Z}/p_1^{m_1}\mathbb{Z}\times\cdots\times\mathbb{Z}/p_r^{m_r}\mathbb{Z}$ について，$\operatorname{Ker}\pi=\cap_{i=1}^r p^{m_i}p_i\mathbb{Z}$ となるが，各 p_i は互いに素だから，これは $p_1^{m_1}\cdots p_r^{m_r}\mathbb{Z}$ に一致．よって，これについての商写像 $\overline{\pi}:\mathbb{Z}/p_1^{m_1}\cdots p_r^{m_r}\mathbb{Z}\xrightarrow{\sim}\mathbb{Z}/p_1^{m_1}\mathbb{Z}\times\cdots\times\mathbb{Z}/p_r^{m_r}\mathbb{Z}$ は単射であり，また全射性も保たれる．

■

要諦 1.9.19. 直感的には，$p_1^{m_1}$ と $p_2^{m_2}$ が互いに素だと，$(1,1)$ から始めると全ての元を踏むのでこれによって生成される．一方，互いに素でない $(p_1\neq p_2)$ と，$(1,1)$ から始めても全ての元を踏まないし，他の方法も失敗する．これを組み合わせ論的に証明するよりかは，(2) を中間に挟んで証明する．

例 1.9.20. 有限アーベル群の構造定理を，素因数分解のように使って，有限アーベル群の分類ができることがある．

(1) 任意の相異なる素数 $p_1\neq p_2$ について，位数 p_1p_2 のアーベル群は巡回群ただ一つである：$\mathbb{Z}/p_1p_2\mathbb{Z}\simeq\mathbb{Z}/p_1\mathbb{Z}\times\mathbb{Z}/p_2\mathbb{Z}$．任意の位数 p_1p_2 のアーベル群は，必ずこのように分解できてしまうため．
(2) 例 1.9.16 と併せると，位数 $p_1^2p_2$ のアーベル群は同型を除いて 2 つある．例えば，$(\mathbb{Z}/12\mathbb{Z})\simeq(\mathbb{Z}/4\mathbb{Z})\oplus(\mathbb{Z}/3\mathbb{Z})$ または，$(\mathbb{Z}/2\mathbb{Z})^2\oplus(\mathbb{Z}/3\mathbb{Z})$.

□

[†40] $m=0$ の時は個数は 0．$m=1$ の時は p 個ある．他のスロットルは別の素数 q についての q 群なので，位数 p の元は生まれようがない．$m\geqslant 2$ のときも同様．真に驚くべき非本質的な結果は，これが巡回群を特徴づけるということである．
[†41] したがって，通常冪数＝元の位数の最小公倍数は群の位数より小さくなるが，冪数と群の位数が一致するとき，有限アーベル群は巡回群となる．

1.10　半直積

群の可換性を射で緩める：群の標準的な拡大法

群の群への作用（群同型表現）の言葉を使った構成法の言葉で，群の直積を一般化する．第一引数（左の元）について ρ で twist することを許し，これが退化した状態を直積とするいかにも圏論的一般化である．これは，$G \hookrightarrow^{i} G \rtimes H \twoheadrightarrow^{\mathrm{pr}_2} H$ という体 H の拡大の標準的な例であり，G という正規部分群を中心とした中心拡大となる．[a] G の上に回転する H を積み上げた群を構成する強力な方法である．

実は，単完全列 $K \hookrightarrow G \twoheadrightarrow H$[b] が分裂する（＝切断 $s : H \hookrightarrow G$ が存在して H 上で id_H となる）ことと，この群の拡大が半直積 $\exists_{\rho \in \mathrm{Hom}(H, \mathrm{Aut}(K))}\ G = K \rtimes_{\rho} H$ で表されることは同値であり，したがって分裂拡大の分類は半直積の分類，したがって群同型表現 $\rho : H \to \mathrm{Aut}_{\mathrm{Grp}}(K)$ の問題に帰着する．そしてこの必ず存在する切断が chain rule という関手性を満たし，微分となる．[c]

群の拡大が自明ならば直積，分裂するならば半直積で表せるのだが，どちらでもない場合がある．すなわち，$N, G/N$ を知っているが，G を $N \rtimes G/N$ で表せない場合がある．逆は常に成り立つ．

[a] 群の拡大の同型類は $\mathrm{Ext}(K, H)$ と書かれ，群構造が入る．また，$K \hookrightarrow K \times H \twoheadrightarrow H$ と同型な拡大は自明な拡大と呼ばれる．
[b] 単完全列は，G で完全であるだけでなく，$0 \hookrightarrow K \hookrightarrow G$，$G \twoheadrightarrow H \twoheadrightarrow 0$ についても完全である必要がある．これはそれぞれ単射，全射の定義とできる（特徴付け）．
[c] ρ でねじってるものが何に当たるんだ？接続？捩率？

1.10.1　定義と例

定義 1.10.1 (semidirect product).

(1) 群同型による（左）作用＝群同型表現 $\phi : H \to \mathrm{Aut}_{\mathrm{Grp}}(G)$ を一つ定める．この値を $\phi(h) =: \phi_h : G \xrightarrow{\sim} G$ と表すこととする．このとき，直積集合上の次の構造は群となる．

$$\begin{array}{ccc} (G \times H) \times (G \times H) & \longrightarrow & G \times H \\ \cup & & \cup \\ ((g,h),(g',h')) & \longmapsto & (g\phi_h(g'), hh') \end{array}$$

(2) ϕ が id_G への定値写像 $\phi : H \to 1 \to \mathrm{Aut}_{\mathrm{Grp}}(G)$ である場合が，直積である．

(3) 射影 $\mathrm{pr}_2 : H \times G \to G$ の切断 $s : G \to H \times G$ は，$d(hg) = d(h) \cdot \phi_h(dg)$ を満たすため，微分（接写像）d とみなせる．[†42]

(4) 自然な単射 $G \hookrightarrow G \rtimes H, H \hookrightarrow G \rtimes H$ により G, H を部分群とみなすと，$G := \mathrm{Ker}\ (\mathrm{pr}_2)$ であるから，$G \lhd G \rtimes H$ である．

要諦 1.10.2 (射によって可換性条件を緩める)**.** これは可換性の拡張になっている．

$$(e,h) \cdot (g,e) = (e\phi_h(g), he) = (\phi_h(g), e) \cdot (e,h)$$

という計算が成り立つから，これを象徴的に書くと $hg = \phi_h(g)h$ となる．このように緩められた可換性は至る所でみられる，二面体群でも $\tau\sigma = \sigma^{n-1}\tau$ という交換法則がある．あるいは Hermite 内積も Hermite 共役による作用についての半直積と捉えられる．(3) の通り，Chain Rule もその一種と考えられる．

注 1.10.3 (群であることの確認)**.**

結合法則

$$\begin{aligned} \big((g,h)(g',h')\big)(g'',h'') &= (g \cdot \phi_h(g') \cdot \phi_{hh'}(g''), hh'h'') \\ (g,h)\big((g',h')(g'',h'')\big) &= (g\phi_h(g'\phi_{h'}(g'')), hh'h'') \end{aligned}$$

より，ϕ が群準同型であること：$\phi_{hh'}(g'') = \phi_h(\phi_{h'}(g''))$ から従う．

[†42] $\phi_h(g')$ を ${}^h g'$ ともかく．

逆元　「ねじれた交換則」より，$(gh)^{-1} = h^{-1}g^{-1} = \phi_{h^{-1}}(g^{-1})h^{-1}$ と予測できるから，$(g,h)^{-1} = (\phi_{h^{-1}}(g^{-1}), h^{-1})$ とすれば良い．実際，

$$(g,h)(\phi_{h^{-1}}(g^{-1}), h^{-1}) = (g\phi_h(\phi_{h^{-1}}(g^{-1})), hh^{-1})$$
$$(\phi_{h^{-1}}(g^{-1}), h^{-1})(g,h) = (\phi_{h^{-1}}(g^{-1})\phi_{h^{-1}}(g), h^{-1}h).$$

例 1.10.4 (affine 変換群の構成は半直積で定義できる)**.**

(1) $\mathrm{Aff}(\mathbb{R}^n)$ の積は $(A_1, b_1)\cdot(A_2, b_2) = (A_1A_2, A_1b_2 + b_1)$ というもので，$\mathbb{R}^n \rtimes \mathrm{GL}_n(\mathbb{R})$ の構造になっている．
(2) 二面体群は $D_{2n} = C_n \rtimes C_2$ である．
(3) 可逆な上三角行列の集合 B は，対角成分が全て 1 の行列がなす部分集合 U と対角行列 T を用いて $B = U \rtimes T$ と表せる．

□

1.10.2　群の拡大との関係

定義 1.10.5 (group extension).

(1) 完全列 $A \hookrightarrow \widehat{G} \twoheadrightarrow G$ について，$\widehat{G}$ を，A による G **の拡大**という．[†43]
(2) 単射 $A \hookrightarrow \widehat{G}$ が $\widehat{G}$ の中心について分解する場合，これを**中心拡大**という．すなわち，$A \subset Z(\widehat{G})$ のときである．[†44]
(3) 全射 $\widehat{G} \twoheadrightarrow G$ が切断を持つとき，これを**分裂拡大** (split extension) という．[†45]このとき $\widehat{G}$ は，ある準同型 $\rho : G \to \mathrm{Aut}_{\mathrm{Grp}}(A)$ について，半直積 $A \rtimes_\rho G$ である．

注 1.10.6 (拡大とはファイバーである)**.** 圏論的には，拡大は，底空間について，ファイバーによって為される．On the other hand, our terminology conflicts with the usual meaning of “extension” in algebra. For example, in Galois theory if k is a field, then an extension of k contains k as a subfield.[†46]

例 1.10.7.

(1) 実は $\mathrm{Aut}_{\mathrm{Grp}}(U(1)) = \mathbb{Z}/2\mathbb{Z}$ である．これは体 $\mathbb{R}$ の拡大とパラレルな状況ではないか？そこで，$\rho : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(U(1))$ とすると，$U(1) \hookrightarrow U(1) \rtimes_{\rho_{\mathrm{Aut}}} \mathbb{Z}_2 \to \mathbb{Z}_2$．なにこれ．1 次元の ± 1 の拡大は回転？ $U(1)$ を拡大して直交変換をえたのだろうか．[†47]
(2) 単完全列 $1 \to A_n \to S_n \to C_2 \to 1$ は分裂するから，$S_n \simeq A_n \rtimes C_2$ であり，かつ $n \geqslant 5$ の時は A_n 以外の真の正規部分群を持たない．

□

1.10.3　直積への分解

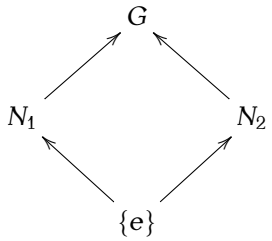
Abel 群の射影子による分解 1.9.2 では，非可換な元を考えなかったから半直積もない．補題 1.10.13 で，$\phi = 1$ と取れる場合の特徴付けを与えているとも読める．

定理 1.10.8 . G の正規部分群 N_1, N_2 について，

(1) 次の 2 条件は同値．
  (a) $N_1N_2 = G$ かつ $N_1 \cap N_2 = \{e\}$.
  (b) N_1 の元と N_2 の元は可換：$\forall_{x_1\in N_1, x_2\in N_2}\ x_1x_2 = x_2x_1$ かつ $\forall_{g\in G}\ \exists!_{x_1\in N_1, x_2\in N_2}\ x = x_1x_2$.
(2) (1) の同値な条件が満たされるとき，$G \simeq N_1 \times N_2$

[†43] G の e の周りに潰れていたと考えられる A を挿入する動き．
[†44] G の e の周りに潰れていたと考えられる A を挿入すると，これが新たに中心を作ること．
[†45] 群の拡大の中で「最も単純なもの」と捉えられる．
[†46] https://ncatlab.org/nlab/show/group+extension
[†47] https://ncatlab.org/nlab/show/semidirect+product+group

要諦 1.10.9. すなわち，結びと交わりを次のようにもつ N_1, N_2 を見つければ良い．

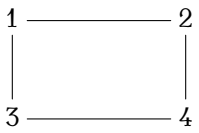


これはすごく線型空間の直積っぽい．

例 1.10.10. Klein の 4 群 $V = \{(1), (13)(24), (12)(34), (14)(23)\}$ は，対辺の垂直二等分線に関する対象変換について

$$N_1 := \{(1), (13)(24)\} \quad N_2 := \{(1), (12)(34)\}$$

とすれば，中心を中心とした 180 度回転は折り返し 2 回で作れるから，$V \simeq N_1 \times N_2$ となる．



□

1.10.4　半直積への分解

積と商の双対性が露わになっているのは偶然か？

終域について，商で表す方法が準同型定理で与えられるならば，作用の言葉で，定義域については半直積で表す方法がある．$N \lhd G$ で $H \simeq G/N$ となる H が見つかるとき，もし epimorphism $\pi : N \twoheadrightarrow G$ が split ならば，$G \simeq N \rtimes H$ である．おそらく Set とは違って，Grp では全ての epi が split なわけではない．このとき暗躍するのが切断と共役変換である．複雑怪奇．

射影子のアーベル群の場合についての特徴付け 1.9.2 では，包含 $N \hookrightarrow M$ に引き戻しが存在すれば，$\operatorname{Cod} i = M \simeq N \times M/N = \operatorname{Im} i \times \operatorname{Ker} i$ というものであった．今回は，射影 $\pi : G \twoheadrightarrow H$ に切断が存在すれば，$\operatorname{Dom} \pi = G =\simeq N \rtimes H = \operatorname{Ker} \pi \rtimes \operatorname{Im} \pi$ という条件である．

定理 1.10.11 . $H, N \leqslant G$ について，ある準同型 $\rho : H \to \operatorname{Aut}(N)$ が存在し，同型 $N \rtimes_\rho H \xrightarrow{\sim} G$ であって，H, N への制限が包含写像になるものが存在するための必要十分条件は，次の 3 条件である：

(1) $G = HN$.
(2) $N \cap H = \{e\}$.
(3) $N \lhd G$.

またこのとき，ρ は H による共役作用の N への制限となる．[†48]

要諦 1.10.12. (1),(2) は，商写像の制限 $\pi : H \to G/N$ が同型であるための必要十分条件である．だから特に，$G = N \rtimes N \Rightarrow G/N \simeq H$．また (1),(2) によって，$S_4 \simeq V \rtimes S_3$ も確認できる．

補題 1.10.13 (半直積への分解). $\pi : G \twoheadrightarrow H$ を全射準同型とし，その核を $N := \operatorname{Ker} \pi$ とする．（すなわち，$H \simeq G/N$）．このとき，切断 $s : H \to G$ が存在するならば，作用を $\phi := \operatorname{Ad} \circ s : H \hookrightarrow G \to \operatorname{Aut}_{\mathrm{Grp}}(N)$ とおくことで，これについての半直積 $N \rtimes_\phi H$ を考えると，$G \simeq N \rtimes_\phi H$ と表せる．

要諦 1.10.14. 切断 s を合成した共役変換 ϕ により，$N \rtimes_\phi H$ の交換規則は $hn = s(h)ns(h)^{-1}h$ の通り．

[†48] https://geolog.mydns.jp/www.geocities.jp/aoirei2002/math/papers/groupdif.pdf

アーベル群の射影子による分解 1.9.2 では，$i : N \hookrightarrow G$ に対して，この引き戻し $r : G \twoheadrightarrow N$ が群準同型ならば，$G = N \times G/N$ と表せる．splitness が，G/N が群であるか（N が正規かどうか），そして群であるなら N と $G \simeq N \times G/N$ を満たすような関係で作用し合うかの判定に対応している．逆に $\pi : G \twoheadrightarrow G/N$ 主体で考えて，切断 $s : G/N \hookrightarrow G$ が群準同型であるならば，

[証明].

$$\begin{array}{ccc} f : N \rtimes H & \longrightarrow & G \\ \cup & & \cup \\ (n,h) & \longmapsto & n \cdot s(h) \end{array}$$

と定めると，これが同型になる．

関手性

$$\begin{aligned} f((n,h),(n',h')) &= f((n\phi_h(n'),hh')) \\ &= n \cdot s(h)n's(h)^{-1} \cdot s(hh') = ns(h)n's(h') \\ &= f((n,h))f((n',h')) \end{aligned}$$

単射性　$(n,h) \in \operatorname{Ker} f \Leftrightarrow ns(h) = e$ とする．両辺の π による像を取ると，$\pi(n)\pi(s(h)) = e \cdot h = e$ より，$h = e$．したがって $n = e$ も従う．

全射性　$g \in G$ を任意に取る．s で作ったのが f であるから，π を使って戻すことを考える．$h := \pi(g), n := g \cdot s(h)^{-1} \in G$ と置くと，$\pi(n) = \pi(gs(h)^{-1}) = \pi(g)h^{-1} = \pi(g)\pi^{-1}(g) = e$ より $n \in N$．これについて，$(n,h) \in f^{-1}(g)$.

■

要諦 1.10.15. 基本的に全知全能の構成による証明が与えられたが，何が読み取れるのか判らない．

例 1.10.16 (上三角行列の空間).

$$G := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{GL}_n(\mathbb{C}) \;\middle|\; ad \neq 0, a, b, d \in \mathbb{C} \right\}$$

とすると，$G \simeq \mathbb{C} \rtimes_\phi (\mathbb{C}^\times \times \mathbb{C}^\times)$．つまり，右上成分の一次元線型空間 $\mathbb{C}$ を中心として，2 つの成分は $\mathbb{C}^\times \times \mathbb{C}^\times$ を作って回転している．この結果は一般の次元に一般化できる．

(1) 全射準同型を

$$\begin{array}{ccc} \pi : G & \longrightarrow & \mathbb{C}^\times \times \mathbb{C}^\times \\ \cup & & \cup \\ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} & \longmapsto & (a,d) \end{array}$$

とすると，$\operatorname{Ker} \pi = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \;\middle|\; b \in \mathbb{C} \right\} \simeq \mathbb{C}$ である．ただし，$\mathbb{C}$ は加法群とみた．

(2)

$$\begin{array}{ccc} s : \mathbb{C}^\times \times \mathbb{C}^\times & \longrightarrow & G \\ \cup & & \cup \\ (a,d) & \longmapsto & \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \end{array}$$

と定めると，確かに $\pi \circ s = \mathrm{id}_{\mathbb{C}^\times \times \mathbb{C}^\times}$.

(3) 準同型 $\phi = \mathrm{Ad} \circ s$ は，

$$s(a,d) \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} s(a,d)^{-1} = \begin{pmatrix} 1 & \frac{ab}{d} \\ 0 & 1 \end{pmatrix}$$

より，

$$\begin{array}{ccc} \phi : \mathbb{C}^\times \times \mathbb{C}^\times & \longrightarrow & \mathrm{Aut}_{\mathrm{Grp}}(\mathbb{C}) \\ \cup & & \cup \\ (a,d) & \longmapsto & \mathrm{Ad}_s : b \mapsto \frac{a}{d} b \end{array}$$

で与えられ，$G \simeq \mathbb{C} \rtimes_\phi (\mathbb{C}^\times \times \mathbb{C}^\times)$ と表示できる．

□

1.10.5　輪積

定義 1.10.17 (wreath product). 半直積のうち，2 つの置換群 $H \leqslant \mathrm{Sym}(n), G \leqslant \mathrm{Sym}(m)$ について，G が成分の置換によって H^m に作用して得るもの $H^m \rtimes G =: H \wr G$ を**輪積**という．

定理 1.10.18 (普遍埋め込み定理). 群 G が A の H による拡大ならば、輪積 $A \wr H$ の部分群で G に同型なものが存在する．

1.11　組成列と Jordan Hölder の定理

有限アーベル群の分類で群の標準的な構造分解が見えてきた．さらに半直積の言葉を手に入れたことによって，S_3 は正規部分群 $\langle\sigma\rangle = A_3 \simeq \mathbb{Z}/3\mathbb{Z}$ とその周りの $\langle\tau\rangle = S_3/A_3 \simeq \mathbb{Z}/2\mathbb{Z}$ とを，ねじれ $\varphi(\tau)(\sigma) = \sigma^{-2}$ を介して「積み重ねた」ものだと考えられる．そして $S_3 \simeq \mathbb{Z}/3 \rtimes_\varphi \mathbb{Z}/2$ とは，σ, τ の指数法則のみを追っている行為に当たる．すると $\mathbb{Z}$ は無限巡回群だというのがすっとわかる，終わりのない指数をもつ．また，半直積は 2 つの群 G, H から，G を正規部分群に指定し，その上に H の構造を持たせて「積み上げる」群のための構成法で，準同型 $\varphi : H \to \mathrm{Aut}_{\mathrm{Set}}(G)$ の数だけある．
正規部分群 $H \lhd G$ が存在したとき，単完全列 $0 \hookrightarrow H \hookrightarrow G \twoheadrightarrow G/H \twoheadrightarrow 0$ が存在する．これは標準分解の理論の一般化である．これに沿って組成列が分解することを用いて，任意の群に対して組成列の長さが一定であることが帰納法により証明できる．

1.11.1　単純群

群自体が一つの共役類（軌道）からなる群

A_4 の特異性は何だろうか．また，補題中で，S_n は共役によって A_n に作用することを考えるが，$n \neq 6$ の場合に限り $\mathrm{Aut}(A_n) \simeq S_n$ が成り立つ．

定義 1.11.1 (simple group).

(1) 自明でない正規部分群を持たない非自明な群を**単純群**という．
(2) 一般に，零対象 0 をもつ圏 C において，商対象を $0, X$ の 2 つしか持たない対象 $X \in C$ を**単純対象**という．[†49]
(3) 単純対象の直和は，semisimple object という．

例 1.11.2 (単純なアーベル群の特徴付け)**.** アーベル群 G が，単純であることと $\exists_{p \in \mathcal{P}}\ G \simeq \mathbb{Z}/p\mathbb{Z}$ であることは同値である．ただし，too simple to be simple に注意．

[証明].

⇐　部分群が $H \lhd G$ であることは，Lagrange の定理 1.5.5 より $|H| \mid |G|$ なので，$|H| = 1, p$ に同値．よって，G は単純．

⇒　$x \in G \backslash \{e\}$ とすると，部分群 $\langle x\rangle \subset G$ は正規であるから（アーベル群の任意の部分群は正規），$\langle x\rangle = G$ が従う．よって，G は巡回群だから，同型 $\exists_{n \in \mathbb{N}}\ G \simeq \mathbb{Z}/n\mathbb{Z}$ が存在する．$n = 0$ ならば $\mathbb{Z}/2\mathbb{Z}$ を部分群にもち，矛盾．$n = 1$ ならば自明群となり矛盾．$n \geqslant 2$ となり合成数であった場合は，$2 \leqslant m < n$ が $m \mid n$ とすると，$m\mathbb{Z}/n\mathbb{Z}$ を部分群にもち，矛盾．[†50]

■

□

命題 1.11.3 (方程式の可解性の消息). $n \geqslant 5$ に対して，交代群 A_n は単純である．

[†49] 「割れない」.「内部構造がない」をこれで測る．C が Abel 圏の時は，商対象には言及せず，部分対象 (subobject) で (1) のように定義できる．The zero object itself is not simple, as it has only one quotient object. It is too simple to be simple.
[†50] 有限アーベル群の構造定理には，この主張を引き出す力はない．

[証明]. 保留.

(1)

■

補題 1.11.4 (交代群の観察：位数 3 の巡回置換). $n \geqslant 3$ とする.

(1) 交代群 A_n は位数 3 の巡回置換全体の集合 $\{(m_1\ m_2\ m_3) \mid m_1, m_2, m_3$は相異なる $\}$ で生成される.
(2) 位数 3 の巡回置換は，A_n において $(1\,2\,3), (1\,3\,2)$ のいずれかと共役である.
(3) H を A_n の正規部分群とする．H が位数 3 の巡回置換を少なくとも一つ含むならば，$H = A_n$ である.

[証明].

(1) 任意に 2 つの互換 $(a\ b), (c\ d)$ $(a \neq b, c \neq d)$ を取る．この積は

$$(a\ b)(c\ d) = \begin{cases} (a\ d\ c)(a\ b\ c), & \{a,b\} \cap \{c,d\} = \varnothing, \\ (x\ z\ y), & \{a,b\} \cap \{c,d\} = \{x\}, \{a,b\} = \{x,y\}, \{c,d\} = \{x,z\}, \\ \mathrm{id}_{A_n}, & \{a,b\} = \{c,d\}. \end{cases}$$

となり，位数 3 の巡回置換の積で表せる．よって，偶数個の互換の積で表せる置換全体の集合 A_n は，位数 3 の巡回置換で表せる.

(2) 任意に $(m_1\ m_2\ m_3) \in A_n$ を取る．置換 $\sigma \in S_n$ を $\sigma(m_i) = i$ $(i = 1,2,3)$ と定めると，$\sigma(m_1\ m_2\ m_3)\sigma^{-1} = (1\,2\,3)$ となる．$\sigma \in A_n$ のとき, $(m_1\ m_2\ m_3) \in A_n$ は $(1\,2\,3)$ に共役．$\sigma \notin A_n$ のとき, $\sigma' := (2\,3)\sigma \in A_n$ であり, $\sigma'(m_1\ m_2\ m_3)\sigma'^{-1} = (2\,3)(1\,2\,3)(2\,3)^{-1} = (1\,3\,2)$ である.

(3) 正規部分群 H が位数 3 の巡回置換を含むならば，正規部分群とは任意の内部自己同型に対して不変であるから，$(1\ 2\ 3), (1\ 3\ 2)$ のいずれかを含む．$(1\ 2\ 3)^2 = (1\ 3\ 2), (1\ 3\ 2)^2 = (1\ 2\ 3)$ であるから，H は結局いずれも含む．すると (2) より，H は全ての位数 3 の巡回置換を含む．よって (1) より，$H = A_n$.

■

要諦 1.11.5. (1) は $A_n \subset \langle \{(m_1\ m_2\ m_3) \mid m_1, m_2, m_3$は相異なる $\} \rangle$ しか確認していなくないか？これはすごい描像だ．A_n $(n \geqslant 3)$ の正規部分群は位数 3 の巡回置換を 1 つでも含めば，共役類構造により，全体に伝播する.

1.11.2　組成列とその完全系列に沿った結合・分解

円錐のだるま落としの構造を暴き出す，群論王道の構造定理．あるいは filtration と呼んでも良い．その際の一歩一歩が，「飛びすぎていない」「何かを見落としていない」ことのチェックのために，「商群が単純である」という条件を用いる．これを組成列と名付けると，この長さは不変量となる！
組成列は，その定義からして，だるま落としの構造 $G \simeq H \rtimes G/H$ が存在した場合，この 2 つの組成列の結合となる．逆に，G の組成列がある場合，$i : H \hookrightarrow G$ と $\pi : G \twoheadrightarrow G/H$ の組成列は，標準射 i, π が引き起こす部分群対応 i^*, π_* により構成できる.

定義 1.11.6 (subnormal series, composition series). G を群とする．その部分群の列 $G =: G_0 \supset G_1 \supset \cdots \supset G_n = \{e\}$ を考える.

(1) 任意の $0 \leqslant i \leqslant n-1$ について，G_{i+1} が G_i の正規部分群である時，この列を**正規鎖**という．n を正規鎖の長さという.
(2) 正規鎖が任意の $0 \leqslant i \leqslant n-1$ について，G_i/G_{i+1} が単純群である時，この列を**組成列**という．各 G_i/G_{i+1} を組成因子という.

注 1.11.7.

(1) Galois 拡大の Galois 拡大は Galois 拡大とは限らないように，関係 $H \lhd G$ は推移的ではない.
(2) 組成列は真の減少列であることは，自明群は単純ではないことに含意されている.

定義 1.11.8 (length).

(1) Abel 圏 C において，対象 $X \in C$ の長さとは，
(2) Abel 圏が $C = \mathrm{Vect}$ であった場合，対象 $V \in \mathrm{Vect}$ の長さとは次元をさす. [†51]

例 1.11.9.

(1) $S_3 \supset A_3 \supset \{e\}$ は S_3．組成因子は $\{\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}\}$ なので単純である．
(2) $n \geqslant 5$ のとき A_n は単純であるから，$S_n \supset A_n \supset \{e\}$ は S_n の組成列であり，長さは 2．例 1.10.7 も参照.
(3) $\mathbb{Z}$ は組成列を持たない．仮に $\mathbb{Z} = G_0 \supset \cdots \supset G_n = 0$ を組成列とすると，特に最後の部分に注目すれば，$G_{n-1} = 0$ ならば $G_{n-1}/G_n = 0$ は単純ではなく，$G_{n-1} \neq 0$ すなわち $\exists_{k \in \mathbb{N}}\ G_{n-1} \simeq k\mathbb{Z}$ ならばやはり $G_{n-1}/G_n \simeq k\mathbb{Z}$ が単純であることに矛盾．有限なアーベル群で単純なのは $\mathbb{Z}/p\mathbb{Z}$ のみである 1.11.2.

□

補題 1.11.10 (組成列の結合). 商 $\pi : G \to G/H$ を考える．

$$H = H_0 \supset \cdots \supset H_n = \{e\}, \qquad G/H = Q_0 \supset \cdots \supset Q_m = \{e\}$$

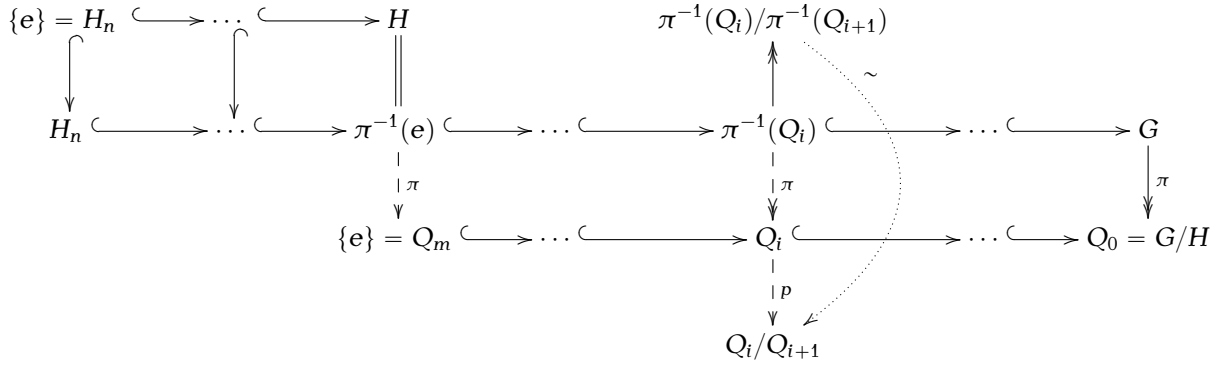
とすると，

$$G = \pi^{-1}(Q_0) \supset \cdots \supset \pi^{-1}(Q_m) = H = H_0 \supset \cdots \supset H_n = \{e\}$$

は G の組成列である．さらに，$\pi^{-1}(Q_i)/\pi^{-1}(Q_{i+1}) \simeq Q_i/Q_{i+1}$.

[証明]. 上記の組成列について，$\pi^{-1}(Q_i)/\pi^{-1}(Q_{i+1}) \simeq Q_i/Q_{i+1}$ を示せば，組成列であることが従う．任意の $i \in m$ について，全射の合成 $\pi^{-1}(Q_i) \twoheadrightarrow^{\pi} Q_i \twoheadrightarrow Q_i/Q_{i+1}$ は全射であり，その核は $\pi^{-1}(Q_{i+1})$ であり，これは $\pi^{-1}(Q_i)$ の正規部分群と分かる．準同型定理より，$\pi^{-1}(Q_i)/\pi^{-1}(Q_{i+1}) \simeq Q_i/Q_{i+1}$ が従う．右辺が単純であるから左辺も単純. ■

要諦 1.11.11 (i で組成列を押し上げ，π が組成列を引き戻す)**.** 組成列を結合できるという圏論的現象を描写している．次の包含写像の列で，２段目の階差列（？）と３段目の階差列は同型対応があるから，３段目を２段目に π を用いて落として，１段目を２段目に押し上げれば，G の組成列を得る．



補題 1.11.12 (有限群の分類への希望). 有限群 G は組成列を持つ

[証明]. G の位数についての帰納法で示す．$|G| = 1$ のとき，$G_0 = G = \{e\}$ は組成列で，長さは 0 である．$|G| > 1$ とする．単純群ならば，$G \supset \{e\}$ は長さ 2 の組成列である．単純群でないならば，真の正規部分群 $H \lhd G$ が存在するので，これについて帰納法の仮定より，$G/H, H$ は組成列を持つ．これを補題の方法によって結合すれば良い. ■

補題 1.11.13 (組成列の分解（双対命題）). $H \lhd G$，$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\}$ を組成列とする．

(1) $J := \{i \in n \mid H \cap G_i \supsetneq H \cap G_{i+1}\}$ とおき，$J \cup \{n\} =: \{j_0 < j_1 < \cdots < j_r\}$ と元を表すと，

$$H = H \cap G_{j_0} \supset H \cap G_{j_1} \supset \cdots \supset H \cap G_{j_r} = \{e\}$$

は H の組成列である．さらに，任意の $i \in r$ について，$(H \cap G_{j_i})/(H \cap G_{j_{i+1}}) \simeq G_{j_i}/G_{j_i+1}$.

[†51] Vect とは simple object は（同型を除いて）一次元空間 k のみで，何度 0 を排出することができるかの階数が次元に当たる．群論的な「積み上げ」構造とは違う構造をしているな.

(2) $K := \{i \in n \mid \pi(G_i) \supsetneq \pi(G_{i+1})\}$ とおき,[†52] $K \cup \{n\} =: \{k_0 < \cdots < k_s\}$ とおくと,

$$G/H = \pi(G_{k_0}) \supset \pi(G_{k_1}) \supset \cdots \supset \pi(G_{k_s}) = \{e\}$$

は G/H の組成列である．さらに，任意の $i \in s$ について，$\pi(G_{k_i})/\pi(G_{k_{i+1}}) \simeq G_{k_i}/G_{k_i+1}$.

(3) J, K は無縁で，$J \sqcup K = n$ が成り立つ．したがって (1),(2) より，置換 $\sigma : n \to J \sqcup K$ が存在して，

[証明].

(1) $j = j_i \in J$ を任意にとって，$(H \cap G_{j_i})/(H \cap G_{j_{i+1}}) \simeq G_{j_i}/G_{j_{i+1}}$ を先に示す．まずすぐにわかることとしては，$H \cap G_j \xrightarrow{i} G_j \xrightarrow{\pi} G_j/G_{j+1}$ は準同型であり（全射とは限らないことに注意），その核は $H \cap G_{j+1}$ であるから，剰余群の普遍性より，単射 $H \cap G_j/H \cap G_{j+1} \hookrightarrow G_j/G_{j+1}$ が引き起こされる．これが全射でもあることを示せば良いのだが，これを G_j/G_{j+1} の単純性から示す．まず，この単射の定義域と像を同一視すると，$(H \cap G_j)/(H \cap G_{j+1}) \lhd G_j/G_{j+1}$ とみなせる．$H \cap G_j \lhd G$ の全射 $\pi : G_j \twoheadrightarrow G_j/G_{j+1}$ の像だからである．すると，$(H \cap G_j)/(H \cap G_{j+1})$ は自明であるか G_j/G_{j+1} であるかのいずれかであるが，前者は J の定め方に反する．J の定め方から，$H \cap G_{j_i+1} = H \cap G_{j_i+2} = \cdots = H \cap G_{j_{i+1}}$.
よって，$(H \cap G_j)/(H \cap G_{j+1})$ も単純であるから，正規鎖 $H = H \cap G_{j_0} \supset H \cap G_{j_1} \supset \cdots \supset H \cap G_{j_r} = \{e\}$ は H の組成列.[†53]

(2)

$$\begin{array}{ccccccc}
G_{k_{i+1}} & \hookrightarrow \cdots \hookrightarrow & G_{k_i+1} & \hookrightarrow & G_{k_i} & \hookrightarrow \cdots \hookrightarrow & G \\
\downarrow & & & & \downarrow \pi & & \downarrow \pi \\
\pi(G_{k_{i+1}}) & & \hookrightarrow & & \pi(G_i) & \hookrightarrow \cdots \hookrightarrow & G/H \\
 & & & & \downarrow p_i & & \\
 & & & & \pi(G_{k_i})/\pi(G_{k_{i+1}}) & &
\end{array}$$

射 $G_{k_i} \to \pi(G_{k_i})/\pi(G_{k_i+1})$ ($\pi(G_{k_{i+1}}) = \cdots = \pi(G_{k_i+1})$ なのでどっちをとってもいい．便宜上，上の図には乗っていない方を取った[†54]) の核は，$\pi^{-1}(\pi(G_{k_i+1})) = G_{k_i} \cap G_{k_i+1}H = G_{k_i+1}(H \cap G_{k_i})$[†55] (補題 1.3.14)．これは H によって定まらないが，いずれにしろ全射 $\tilde{\pi} : G_{k_i}/G_{k_i+1} \twoheadrightarrow \pi(G_{k_i})/\pi(G_{k_i+1})$ は定まる．ここで，始域は単純だから，$\operatorname{Ker}\tilde{\pi} = \{e\}$ が必要．でないと，$\pi(G_{k_i})/\pi(G_{k_i+1}) \neq \{e\}$ という K の元としての条件と $\tilde{\pi}$ の全射性に矛盾する．よって，$G_{k_i}/G_{k_i+1} \simeq \pi(G_{k_i})/\pi(G_{k_i+1})$.
添字 j が $k_i + 1$ から k_{i+1} までのときは群 $\pi(G_j)$ は全て同一だから，$G_{k_i}/G_{k_i+1} \simeq \pi(G_{k_i})/\pi(G_{k_{i+1}})$ も従う．
これより，列 $(\pi(G_{k_j}))_{j=0,\cdots,s}$ は正規鎖であるだけでなく各 step が単純なので，組成列である．

(3) $i \in K \iff j \notin J$ を示せば良い．$i \in K$ とした時，まず現状の確認をする．(2) の冒頭の，議論が特殊化する前までの議論と同様，射 $G_i \xrightarrow{\pi} \pi(G_i) \xrightarrow{p_i} \pi(G_i)/\pi(G_{i+1})$ の核は，$G_i \cap \pi^{-1}(\pi(G_{i+1})) = G_i \cap G_{i+1}H = G_{i+1}(H \cap G_i)$ である．実際，$g \in G_{+1}, h \in H$ かつ $gh \in G_i$ という条件は，$g \in G_{i+1} \Rightarrow g \in G_i$ に注目すれば，$g \in G_{i+1}, g \in H$ かつ $h \in G_i$ としても同値．よって，準同型定理 1.7.1 より，$G_i/G_{i+1}(H \cap G_i) \simeq \pi(G_i)/\pi(G_{i+1})$ である．ここまで一般論.
特に，K の元としての条件と併せると，

$$\begin{aligned}
i \in K \iff \pi(G_i) \supsetneq \pi(G_{i+1})G_{i+1}(H \cap G_i) \subsetneq G_i \\
\iff G_{i+1}(H \cap G_i)/G_{i+1} \subsetneq G_i/G_{i+1}
\end{aligned}$$

まできた．最後の同値変形は，部分群の対応 1.6.11 より，π_* は部分群の包含関係を保つため．また $G_{i+1}(H \cap G_i)/G_{i+1}$ は正規部分群 $G_{i+1}(H \cap G_i) \lhd G_i$ の標準全射による像だから 1.6.7，正規である．よって，G_i/G_{i+1} の単純性より，$G_{i+1}(H \cap G_i)/G_{i+1} = \{e\}$．これは $G_{i+1}(H \cap G_i) = G_{i+1}$，$H \cap G_i \subset G_{i+1}$，$H \cap G_i \subset H \cap G_{i+1}$，$H \cap G_i = H \cap G_{i+1}$ ($G_{i+1} \subset G_i$ より) と引き出せるから，$i \notin J$ と同値であることがわかった.

■

要諦 1.11.14. $H \cap G_i \xrightarrow{i} G_j \xrightarrow{p_i} G_j/G_{j+1}$ の核は簡単であるが，射 $G_i \xrightarrow{\pi} \pi(G_i) \xrightarrow{p_i} \pi(G_i)/\pi(G_{i+1})$ の核は簡単ではないという

[†52] 番号が小さくなると部分群は大きくなるが，真に大きくなるときの行き先を i と附番していく．
[†53] 組成列とは，部分群からなる正規鎖で，各 step が単純であるもの.
[†54] すると添字 $i+1$ は登場しないから，$k_i = k$ として議論を進めたのが先生の講義ノート.
[†55] 初めは $\pi^{-1}(\pi(G_{k_i+1})) = G_{k_i+1} \cup H$ と書いていた

mono-epi 非対称性がある．一般に上の可換図式の状況で，$G_i/G_{i+1}(H\cap G_i)\simeq \pi(G_i)/\pi(G_{i+1})$ である．ここから，(2),(3) は各論に走る．

(1) は i について引き戻す i^*，(2) は π について押し出す π_* が定めていることに注意．

1.11.3　Jordan-Hölder の定理

More generally a form of the theorem holds in any homological category.

任意の群の組成列は，長さが等しく，置換の別を除いて一意である．こうして得た安定的概念を組成因子という．こうして Abel 群には長さ（「次元」）が定まる．一般の Abel 圏における組成列の概念を Jordan-Hölder sequence という．

定理 1.11.15 (Jordan-Hölder). 群 G の任意の 2 つの組成列

$$G=G_0\supset G_1\supset\cdots\supset G_n=\{e\},\qquad G=G'_0\supset G'_1\supset\cdots\supset G'_m=\{e\},$$

について，$m=n$ であり，かつ，$(G_i/G_{i+1})_{i\in n}$ と $(G'_i/G_{i+1})_{i\in m}$ は並べ替えと同型（置換の合成の分を除いて同型）である．多重集合 $\{G_i/G_{i+1}\}_{i\in n}$ を G の**組成因子**と呼ぶ．

[証明]. G の組成列の長さの最小値 $l(G)\in\mathbb{N}$ についての帰納法で示す．

(1) $l(G)=0$ のとき，組成列は $G=\{e\}$ の一通りだから条件を満たす．$l(G)=1$ のとき G は単純群であるから，任意に組成列 $(G'_i)_{i=0,\cdots,m}$ を取ると，まず $G'_1\rhd G'_0$ より，$G'_1=\{e\}$．もし $G'_1=G'_0$ ならば $G'_0/G'_1=\{e\}$ が単純であることに矛盾．よって，$m=1$ であり，$G'_0/G'_1\simeq G_0/G_1=G$.

(2) $l(G)=:n>1$ とする．組成列 $(G'_i)_{i=0,\cdots,m}$ を別の組成列とする．単完全列を $G_1\hookrightarrow^{i}G\twoheadrightarrow^{\pi}G/G_1$ として，これについて

$$J:=\{i\in m\mid H\cap G'_i\supsetneq H\cap G'_{i+1}\},\qquad K:=\{i\in m\mid \pi(G'_i)\supsetneq\pi(G'_{i+1})\},$$

とし，$J\cup\{m\}=:\{j_0<\cdots<j_r\}, K\cup\{m\}=:\{k_0<\cdots<k_s\}$ とする．完全系列に沿った組成列の分解補題 1.11.13 より，$(G'_{j_i}\cap G_1)_{i=0,\cdots,r}$ は G_1 の組成列となり，$(\pi(G_{k_i}))_{i=0,\cdots,s}$ は G/G_1 の組成列となる．ここで，G_1 の組成列としてはすでに G_0 の部分列 $(G_i)_{i=1,\cdots,n}$ があるから，長さは $n-1$ より $r=n-2$ で，ある置換 $\sigma:\{1,\cdots,n\}\xrightarrow{\sim}\{0,\cdots,n-1\}$ が存在して $(G_{j_i}\cap G_1)/(G'_{j_{i+1}}\cap G_1)\simeq G_{\sigma(i)}/G_{\sigma(i)+1}$．$G/G_1$ は単純だから，長さ 2 より $s=1$ で，$\pi(G_{k_0})/\pi(G_{k_1})\simeq G/G_1$．再び補題 1.11.13 より，$m=r+s=(n-2)+2=n$ で，置換 $\sigma:m\xrightarrow{\sim}n$ が存在して，各 $i\in m$ について，$G_i/G_{i+1}\simeq i^{-1}(G'_{\sigma(i)})/i^{-1}(G'_{\sigma(i)+1})$ または $G_i/G_{i+1}\simeq\pi(G'_{\sigma(i)})/\pi(G'_{\sigma(i)+1})$ となる．したがって，$G_i/G_{i+1}\simeq G'_{\sigma(i)}/G_{\sigma(i+1)}$.

■

例 1.11.16 (対称群の組成因子). 完全系列に沿った組成因子の連結補題 1.11.10 と併せると，正規部分群 $H\lhd G$ が定める完全系列 $H\hookrightarrow G\twoheadrightarrow G/H$ について，G の組成因子を，H の組成因子と G/H の組成因子の合併として得ることができる．対称群の組成因子が考えられる．

(1) S_3 は $\{e\}\xrightarrow{\mathbb{Z}/3\mathbb{Z}}A_3\xrightarrow{\mathbb{Z}/2\mathbb{Z}}(A_3\rtimes C_2\simeq)S_3$．$A_3\lhd S_3$ は $A_3=\operatorname{Ker}\operatorname{sgn}$ であるし，$\tau^2=1$ より $\tau\sigma=\sigma\tau$ と考えても良い．また A_3 は単純であることに注意．単純でないのは $V\lhd A_4$ のみ．よって，S_3 の組成因子は $\{\mathbb{Z}/2\mathbb{Z},\mathbb{Z}/3\mathbb{Z}\}$.

(2) Klein の四元群 1.4.12 の全射 $S_4\twoheadrightarrow S_3$ に注目すると，その核は $V\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ だから，S_4 の組成因子は S_3 の組成因子に 2 つの位数 2 の巡回群を加えて，$\{\mathbb{Z}/2\mathbb{Z},\mathbb{Z}/2\mathbb{Z},\mathbb{Z}/2\mathbb{Z},\mathbb{Z}/3\mathbb{Z}\}$ となる．

(3) S_n の組成因子は $n\geqslant 5$ 以降のとき，$\{e\}\lhd A_n\lhd S_n$ となるから，$\{\mathbb{Z}/2\mathbb{Z},A_n\}$ となる．

こうして見ると S_4 のみが特異的である．親族構造は正規性に関係があるのか？　□

1.12　可解群と冪零群

構造決定からは別の風景に目をやると，正則鎖に代数的な要件（可換性）を付したくなる．これはアーベル群から有限回の拡大を施して得られる群，ということになる．一方でこれに対してだるま落としを行うことで特徴づけるのが導来群＝交換子部分群である．

1.12.1　可解群

どんな群も正規部分群のだるま落としとして表示できることはみたが，その構成要素が全て Abel 群になっているようなクラスの群を考える．

定義 1.12.1 (solvable group). 群 G が任意の $i \in n$ について G_i/G_{i+1} がアーベル群となるような正規鎖 (G_i) を持つとき，**可解群**という．

補題 1.12.2 (組成因子による可解性の特徴付け). G を有限群とすると，これは組成因子を持つ．このとき，組成因子が全て Abel 群であることと，G が可解であることは同値．

[証明]. 組成因子が全て Abel 群であるとき，この組成列が存在することから G が可解群であることが従うから，可解であるときに組成因子が全て Abel 群であることを示せば良い．群 G が可解であるとは，Abel 群のみからなる正規鎖 (G_i/G_{i+1}) が存在することであった．すると G の組成因子は，任意の正規部分群 H について H/G の組成因子と H の組成因子とを合わせたものとして得られる 1.11.16 から，G/G_{i+1} の組成因子を全て再帰的に集めたものに等しい．Abel 群の組成因子は全て Abel 群である．　■

例 1.12.3.

(1) アーベル群はどんな部分群もアーベル群だから，必然的に可解である．
(2) 対称群の組成因子 1.11.16 を考えると，S_n が $n \leqslant 4$ のとき可解群であり，$n \geqslant 5$ のとき可解群ではない．
(3) これは代数方程式が根号を用いて解くことができるかを反映している．方程式を解くには群の拡大を解消していく．三次方程式は $S_3/A_3 \simeq \mathbb{Z}/2\mathbb{Z}$ で平方根をとき（二次方程式を解き），$A_3/\{e\} \simeq \mathbb{Z}/3\mathbb{Z}$ で立方根を解くこととなる．一方四次方程式は，$S_4/A_4 \simeq \mathbb{Z}/2\mathbb{Z}$ と $A_4/V \simeq \mathbb{Z}/3\mathbb{Z}$ とは三次方程式を解くことになる．$V/\{e\} \simeq \mathbb{Z}/2 \times \mathbb{Z}/2\mathbb{Z}$ で平方根を 2 回解く？

□

命題 1.12.4 (可解性の遺伝). $H < G$ とする．

(1) G が可解ならば H も可解である．また，$H \lhd G$ であるときは G/H も可解である．
(2) $H \lhd G$ で，$H, G/H$ が可解であるとする．このとき，G も可解である．

[証明].

(1) G が可解のとき，各 G_i/G_{i+1} が可換であるような正規鎖 (G_i) が存在する．
　H の可解性　$(G_i \cap H)$ は H の正規鎖であり，$(G_i \cap H)/(G_{i+1} \cap H)$ は単射準同型 $(G_i \cap H)/(G_{i+1} \cap H) \hookrightarrow G_i/G_{i+1}$ により Abel 群である．[†56]
　G/H の可解性　$\pi : G \twoheadrightarrow G/H$ を全射準同型とする．全射準同型の定める像関手は正規性を保つ 1.6.7 から，$(\pi(G_i))$ は G/H の正規鎖である．全射 $G_i/G_{i+1} \twoheadrightarrow \pi(G_i)/\pi(G_{i+1})$ より，像 $\pi(G_i)/\pi(G_{i+1})$ も Abel である．
(2) 略．

■

[†56] 以前は単射準同型があると部分群だと思ってしまうことは乱暴だと感じていたが，これで腑に落ちた．部分群という概念の根拠が mono の存在であるから，こちらの方が真の数学的概念と考えるのが良いだろう．実際，$i : H \hookrightarrow G$ が存在するとき，$\forall_{h_1,h_2 \in H}$ について，$i(h_1h_2) = i(h_1)i(h_2) = i(h_2)i(h_1) = i(h_2h_1)$ が従う．これが，Abel 群の部分群も Abel であることの証明抽出になっている．

要諦 1.12.5. (1) の含む 2 つの主張が完全なる双対命題になっている．証明も，$i : H \hookrightarrow G$ による引き戻しが定める $i_* : (H \cap G_i)/(H \cap G_{i+1}) \hookrightarrow G_i/G_{i+1}$ による Abel 性の遺伝と，$\pi : G \twoheadrightarrow G/H$ による引き戻し $\pi_* : G_i/G_{i+1} \twoheadrightarrow \pi(G_i)/\pi(G_{i+1})$ による Abel 性の遺伝とで全く双対的である．この単完全列による構造の図示は相変わらず要諦 1.11.11.

注 1.12.6 (Abel 性についての証明抽出)**.**

(1) 単射 $H \hookrightarrow G$ があるとき，G が可換ならば H も可換．実際，$i : H \hookrightarrow G$ が存在するとき，$\forall_{h_1,h_2 \in H}$ について，$i(h_1h_2) = i(h_1)i(h_2) = i(h_2)i(h_1) = i(h_2h_1)$ が従う．
(2) 全射 $G \twoheadrightarrow H$ があるとき，G が可換ならば H も可換．実際，任意の $h_1, h_2 \in H$ に対してそのファイバーの元 $g_1, g_2 \in G$ があるから，$h_1h_2 = \pi(g_1g_2) = \pi(g_2g_2) = h_2h_1$ が従う．

この 2 つはそれぞれ，引き戻しと切断を持つからであろうか．このことはどれくらい直接的な要因になっているのだろうか？

1.12.2　導来列による特徴付け：中心化群と交換子群と Abel 化

導来列が自明群で有限停止することが可解群の特徴付けになる．導来群（交換子部分群）を取ることは，群の拡大の逆である．つまり，商群 G/H を取る時の正規部分群 H が交換子部分群を含むことが，G/H が可換であることに同値．

群構造の持ち上げに続いて，可換性の持ち上げ

正規性 $\forall_{g \in G} gN = Ng$，すなわち $\{n_1g, n_2g, \cdots, n_rg\} = \{gn_1, gn_2, \cdots, gn_r\}$ よりも強い条件を考える．これが中心である．明らかに中心 $Z(G)$ の部分群は全て正規である．

定義 1.12.7 (commutater, derived / commutator subgroup). G を群，$H_1, H_2 \subset G$ を部分群とする．

(1) 積 $[a,b] = aba^{-1}b^{-1}$ を元 a, b の**交換子**という．これが単位元に等しければ，a, b は可換になる．
(2) $[H_1, H_2] := \{[h_1, h_2] \in H_1H_2 \mid h_1 \in H_1, h_2 \in H_2\}$ で生成される部分群 $[G, G]$ は正規になる．これを**導来群**または**交換子群**と呼ぶ．

注 1.12.8 (perfect group)**.**

(1) Abel 群は，$[G, G] = \{e\}$ を満たす群として特徴付けられる．
(2) $[G, G] = G$ を満たす群を**完全群**という．すなわち，$G^{\mathrm{Ab}} = \{e\}$ となる．有限群の導来列は必ず完全群で停止し，これが自明かどうかが可解かどうかの特徴づけとなる．$\{e\}$ は完全で，次に小さいものは A_5 が完全群である．

例 1.12.9 (交換子部分群の例)**.**

(1) $[\mathrm{GL}_n(K), \mathrm{GL}_n(K)] = \mathrm{SL}_n(K)$.
(2) $[S_n, S_n] = A_n$．全ての交換子は偶置換になるから $[S_n, S_n] \subset A_n$．$S_n/A_n \simeq C_2$ は可換だから，$A_n \subset [S_n, S_n]$.
(3) $[A_4, A_4] = V$．Klein の四元群．実は，$[V, V] = \{e\}$．よって A_4, S_4 は可解．
(4) $[A_n, A_n] = A_n$ $(n \geqslant 5)$（$n \geqslant 5$ のとき可解でない．実は A_5 が位数最小の非可解群である）．任意の長さ 3 の巡回置換 (ijk) は，$n \geqslant 5$ のとき，$m, l \in [n] \backslash \{i, j, k\}$ を用いて $[(ijm), (ikl)]$ と表せるため，$A_n \subset D(A_n)$.
(5) 四元数群について，$[Q_8, Q_8] = \{\pm 1\}$.

□

補題 1.12.10 (商群がアーベル群になる条件). G を群とする．

(1) G の導来群 $[G, G]$ は正規部分群である．
(2) $G^{\mathrm{Ab}} := G/[G, G]$ は Abel 群である．これを群 G の**アーベル化**という．

[証明].

(1) $S := \{[g_1, g_2] \in G \mid g_1, g_2 \in G\}$ とおくと，$[G, G] = \langle S \rangle$.

$hSh^{-1} \subset S$　任意の $g_1, g_2, h \in S$ について，

$$\begin{aligned} h[g_1, g_2]h^{-1} &= hg_1g_2g_1^{-1}g_2^{-1}h^{-1} \\ &= (hg_1h^{-1})(hg_2h^{-1})(hg_1h^{-1})^{-1}(hg_2h^{-1})^{-1} = [hg_1h^{-1}, hg_2h^{-1}] \in S. \end{aligned}$$

$h\langle S\rangle h^{-1} \subset \langle S\rangle$　いま，$hSh^{-1} \subset S \quad \Leftrightarrow \quad S \subset h^{-1}Sh \subset h^{-1}\langle S\rangle h$ より，$\langle S\rangle = [G,G] \subset h^{-1}\langle S\rangle h$．すなわち，$h[G,G]h^{-1} \subset [G,G]$.

(2) 任意の $g, h \in G$ について，$(gh)[G,G] = (hg)[G,G]$ を示せば良い．実際，$gh = [g,h](hg)$ より，$gh \in (gh)[G,G]$ と $gh \in [G,G](gh) = (hg)[G,G]$ とは同値．

■

要諦 1.12.11. ここからの重要な証明抽出は $xy = xyx^{-1}y^{-1}yx = [x,y]yx$ という関係である．可解性の特徴付け 1.12.14 の (2) で用いる．

注 1.12.12 (交換子とは自由構成の発想である)**.** Abel 化関手 $^{\mathrm{Ab}} : \mathrm{Grp} \to \mathrm{Ab}$ は，包含関手 $U : \mathrm{Ab} \hookrightarrow \mathrm{Grp}$ の左随伴である．一方で，中心 Z はこのような関手性を持たない．これが実は自由関手であったことは，交換子の発想の形式性の高さからわかる．

定義 1.12.13 (derived sequence). 群 G に対して，その交換子部分群を取り続けて得られる部分群の列 $G =: D^0(G) \supset D^1(G) \supset \cdots \supset D^n(G) \supset \cdots$ を次のように定める：

(1) $D^0(G) := G$.
(2) $\forall_{n \geqslant 1}\ D^n(G) := [D^{n-1}(G), D^{n-1}(G)]$.

すると補題より，$(D^n(G))$ は正規鎖であり，また $D^n(G)/D^{n+1}(G)$ は Abel 群である．

命題 1.12.14 (可解群の導来列による特徴付け). 群 G について，次の 2 条件は同値．

(1) G は可解である．
(2) $\exists_{n \in \mathbb{N}}\ D^n(G) = \{e\}$.

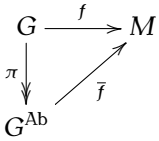
[証明].

(2)⇒(1)　$(D^n(G))$ の存在が，G が可解であるための要件を充足させる．

(1)⇒(2)　G が可解であるとき，G_i/G_{i+1} が Abel であるような正規鎖 (G_i) が存在する．このとき，$\forall_{n \in \mathbb{N}}\ D^n \subset G_n$ を示す．$n = 0$ のときは $D^0(G) = G \subset G_0$．$n > 0$ のとき，全射準同型 $\pi : G_{n-1} \twoheadrightarrow G_{n-1}/G_n$ に注目すると，G_{n-1}/G_n は Abel 群だから，$[G_{n-1}, G_{n-1}] \subset \mathrm{Ker}\ \pi = G_n$．(本質的には Abel 化の普遍性 1.12.15 による)．
よって，特に $D^n(G) \subset G_n = \{e\}$ より $D^n(G) = \{e\}$ である．

■

命題 1.12.15 (Abel 化の普遍性). 任意のアーベル群 M と準同型 $f : G \to M$ について，次の図式を可換にする準同型 $\overline{f} : G^{\mathrm{Ab}} \to M$ がただ一つ存在する：



すると，G/H が Abel 群であることと，$[G,G] \subset H \lhd G$ であることとは同値．

[証明].

(1) 任意の $g_1, g_2 \in G$ について $f(g_1g_2g_1^{-1}g_2^{-1}) = e$ より，$S \subset \mathrm{Ker}\ f$.
(2) よって，$\langle S\rangle = [G,G] \subset \mathrm{Ker}\ f$.
(3) 剰余群の普遍性 1.6.9 より．

■

要諦 1.12.16. 結局この交換子の構成が強力なのは，上の論法が成り立つからである．

定理 1.12.17 (Feit – Thompson 63). 位数が奇数な有限群は可解である．

1.12.3　冪零群

冪零群とは，（アーベル群の有限回の拡大で表される）可解群のうち，特に中心拡大を繰り返すことで得られる群である．つまり，「拡大した結果，$A \hookrightarrow \widehat{G} \twoheadrightarrow G$ で，$A \subset Z\widehat{G}$ となる」を繰り返す．

定義 1.12.18 (nilpotent group, central series). 群 G が冪零群であるとは，次を満たす正規鎖 (G_i) が存在することを言う：$\forall_{i\in\mathbb{N}}\ G_i \lhd G$，$\forall_{i\in\mathbb{N}}\ G_i/G_{i+1} \subset Z(G/G_{i+1})$．このような正規鎖を**中心列**という．

要諦 1.12.19 (同値な定義)**.** 冪零群は次の 2 条件で帰納的に定義される．

(1) 自明群 $\{e\}$ は冪零である．
(2) 冪零群 G'' に対して，完全列 $1 \to G' \to G \to G'' \to 1$ が中心拡大である（したがって特に G' は Abel 群である）とき，G も冪零である．

命題 1.12.20 (冪零性の遺伝). $H < G$ とする．

(1) G が冪零ならば H も冪零である．また，$H \lhd G$ であるときは G/H も冪零である．
(2) $H \overset{\text{subgrp}}{\subset} Z(G)$ で，G/H が冪零であるとする．このとき，G も冪零である．[†57]

命題 1.12.21 (p-群は冪零である). 任意の素数 p について，p-群は冪零である．

[証明].

(1) $|G| = 1$ のとき，自明群は冪零である．
(2) $|G| > 1$ とする．冪零性の遺伝 1.12.20 より，$G/Z(G)$ が冪零群であることを示せば良い．$|G/Z(G)|$ の位数は再び p の冪であり p-群であるから，帰納法の仮定より従う．

■

要諦 1.12.22. 冪零性の遺伝 1.12.20 より，群 G が冪零であることを示すには，$G/Z(G)$ が冪零であることを示せば良い．これは帰納法に繋がる．

例 1.12.23 (冪零群の例)**.**

(1) Abel 群は可解群であったが，冪零群でもある．というよりも，冪零群とは「ほとんど Abel 群」であるという意味で，Abel 群の一般化である．
(2) 冪零群の直積は冪零であり，逆に，有限冪零群は p-群の直積である．
(3) 任意の体 K 上の n 次単上三角行列全体のなす乗法群は，冪零度 $n-1$ の冪零群である．
(4) 最小の非 Abel な p-群である四元数群 Q_4 は，冪零度 2 の冪零群である．
(5) S_3 は可解であった 1.12.3 が，冪零ではない．実際，$C^1(S_3) = [S_3, S_3] = A_3$ である．$S_3 \simeq A_3 \rtimes C_2$ の非自明な正規部分群は A_3 のみであり，$S_3/A_3 \simeq C_2$ は Abel 群であるため．また，$C^2(S_3) = [S_3, A_3] = A_3$ である．実際，$(1\ 2) \in S_3$ は $(1\ 2\ 3) \in A_3$ と交換しない．が，A_3 は Abel 群なので．以上より，S_3 の降中心列は停止しない．

□

[†57] 冪零群とは，「拡大した結果，$A \hookrightarrow \widehat{G} \twoheadrightarrow G$ で，$A \subset Z\widehat{G}$ となる」を繰り返すので，当然である．

1.12.4　降中心列による特徴付け

可解群における導来列同様，冪零群は降中心列が有限停止することとして特徴付けられる．論法としては，標準的な中心列が，降中心列として構成できるのである．

定義 1.12.24 (lower / decending central sequence). 群 G に対して，その G との交換子部分群を取り続けることで得られる部分群の列 $(C^n(G))$ を次のように定める：

(1) $C^0(G) := G$.
(2) $C^n(G) := [G, C^{n-1}(G)]$.

補題 1.12.25. G を群とする．降中心列について，

(1) $C^n(G) \lhd G$.
(2) $C^n(G)/C^{n+1}(G) \overset{\text{subgrp}}{\subset} Z(G/C^{n+1}(G))$.

[証明].

(1) $C^0(G) = G \lhd G$ より，$n > 0$ とする．$S := \{[g_1, g_2] \in G \mid g_1 \in G, g_2 \in C^{n-1}(G)\}$ とおく．任意の $g_1 \in G, g_2 \in C^n(G), h \in G$ について，$h[g_1, g_2]h^{-1} = [hg_1h^{-1}, hg_2h^{-1}] \in S$ は，$C^{n-1}(G)$ が正規部分群であることから従う．したがって，$h\langle S\rangle h^{-1} \subset \langle S\rangle$（補題 1.12.10 の証明抽出）.
(2) 任意の $g \in G, h \in C^n(G)$ について，$gC^{n+1}(G) \cdot hC^{n+1}(G) = hC^{n+1}(G) \cdot gC^{n+1}(G)$ を示せば良い．$gh = ghg^{-1}h^{-1}hg = [g, h](hg)$ より，$gh \in (gh)C^{n+1}(G)$ と $gh = [g, h](hg) \in C^{n+1}(G)(hg)$ は同値.

■

命題 1.12.26 (冪零群の特徴付け). 群 G について，次の 2 条件は同値.

(1) G は冪零である.
(2) $\exists_{n\in\mathbb{N}}\ C^n(G) = \{e\}$.

[証明].

(2)⇒(1)　自明.
(1)⇒(2)　略.

■

定義 1.12.27 (nilpotency class). 中心列 $(C^i(G))_{i=0,\cdots,n}$ の長さ n は一意とは限らないが，その最小値を**冪零度**という．するとこれは降中心列の長さの最小値に一致する．冪零度が 0 の群は自明群ただ一つである.

1.13　Sylow の定理

Lagrange の定理 1.5.5 の逆（特定の位数の部分群は必ず存在する）が成り立つ場合がある．それは，有限群の位数が $|G| = p_1^{m_1} \cdots p_r^{m_r}$ と素因数分解できるとき，位数 $p_i^{m_i}$ の p-群が必ず存在し，その個数は $1 + r'p$ $(r' \in \mathbb{N})$ 個であり（個数は確定しない），互いに共役であることがわかる.

1.13.1　p-Sylow 部分群

ある群の部分束の中で，p-群は p-Sylow 部分群を根 (root) とした束のようになっている．p-Sylow 部分群 P はただ一つ存在するか，その周りに P による共役作用について，p の冪の位数を持った軌道で回っているかのいずれかであり，この共役作用を G にまで延長すると全ての p-Sylow 部分群は一つの軌道に入る（したがって，p-Sylow 部分群がただ一つの場合は，それが正規部分群となり，複数ある場合はどの p-Sylow 部分群も正規でないことに同値）．その結果，任意の部分群 $H < G$ を指定すれば，H を含む p-Sylow 部分群が巡回道に必ず見つかる．

定義 1.13.1 (Sylow p-subgroup). 有限群 G と素数 p について，$P \overset{\text{subgrp}}{\subset} G$ が **p-Sylow 部分群**であるとは，次の 2 条件を満たすことを言う：

(1) P は p 群である．
(2) $\dfrac{|G|}{|P|}$ が p と互いに素である．

要諦 1.13.2 (素イデアルに通じる)**.** この定義は，位数 $|G|$ の素因数分解の言葉で特定の部分群を位数によって指定しているだけであるが，これが必ず存在することが従う対象である．S の部分群束のうち，p-部分群がなす束のうち，（必然的に）極大であるものが p-Sylow 部分群である．存在様態としては素イデアルに少し似ている気がする．したがって，群 G の p-Sylow 部分群の位数は一定であるし，位数が $p_i^{m_i}$ の部分群が存在した場合，それは p-群かつ極大であるから，p-Sylow 部分群そのものである．なお，p-群の p-Sylow 部分群とは，自分自身である．

例 1.13.3 (一般線型群)**.** $G := \mathrm{GL}_n(\mathbb{F}_p)$ $(n \geqslant 1, p$: 素数 $)$ とすると，上三角行列であって対角成分が全て 1 であるようなもの全体 $U \overset{\text{subgrp}}{\subset} G$ は p-Sylow 部分群である．

(1) $|G| = (p^n - 1)(p^n - p)\cdots(p^n - p^{n-1}), |U| = p^{1+2+\cdots+(n-1)}$ より，U は p-群である．$\mathbb{F}_p^n$ の n 個の基底の行き先となる元を考えると，初めは零ベクトルを除いて $p^n - 1$ 通りある．次に最初に選んだベクトルと平行なベクトル p 個を除いて，$p^n - p$ 通りある．これを繰り返す．
(2) $\dfrac{|G|}{|U|} = (p^n - 1)(p^{n-1} - 1)\cdots(p - 1)$ である．

□

補題 1.13.4 (部分群への p-Sylow 部分群の遺伝). G を有限群とし H をその部分群とする．p を素数とし，P を G の p-Sylow 部分群とする．このとき，$g \in G$ が存在して，$H \cap gPg^{-1}$ は H の p-Sylow 部分群である．

[証明].

構成　左作用 $H \times G/P \to G/p; h * gP = (hg)P$ による軌道分解を考える．p-Sylow 部分群 P の極大性より，$|G/P| = \dfrac{|G|}{|P|}$ は p の倍数ではないので，$\forall_{gP \in G/P}\ |H| = |HgP||\mathrm{Stab}_H(gP)|$1.5.9 より，全ての軌道は p の倍数ではない．このとき，任意の元 $gP \in G/P$ について，

$$\begin{aligned}\mathrm{Stab}_H(gP) &= \{h \in H \mid hgP = gP\} \\ &= \left\{h \in H \mid g^{-1}hg \in P\right\} \\ &= \left\{h \in H \mid h \in gPg^{-1}\right\} = H \cap gPg^{-1}\end{aligned}$$

が成り立つ．

証明　(1)　$H \cap gPg^{-1}$ は p-群 $gPg^{-1} = \mathrm{Ad}(g)(P)$ の部分群であるから p-群である．

(2)　安定化群と軌道の関係より，gP の H-軌道の個数が $\dfrac{|H|}{|\mathrm{Stab}_H(gP)|} = \dfrac{|H|}{|H \cap gPg^{-1}|}$ に等しいから，特に p の倍数ではない．

■

要諦 1.13.5. これと Sylow の定理を併せると，G の p-Sylow 部分群の位数 p^a について，位数 p^b $(1 \leqslant b \leqslant a)$ の部分群は必ず存在し，入れ子式になっており，最大のものが p-Sylow 部分群である．

定理 1.13.6 (Sylow (1872)). G を有限群，p を素数とする．

(1) G の p-Sylow 部分群が存在する．
(2) P, P' を G の p-Sylow 部分群とすると，P と P' は共役である：$\exists_{g\in G}\ P' = gPg^{-1}$．特に，互いに同型である：$P \simeq_{\mathrm{Ad}(g)} P'$．
(3) G の p-Sylow 部分群の個数を $n_{G,p}$ とおくと，$n_{G,p}$ は $|G|$ を割り切り[†58]，かつ $n_{G,p} \equiv 1 \mod p$ である．

[証明].

(1) **表現の構成**　$\mathbb{F}_p$-線型形式の空間 $V := \mathrm{Map}(G, \mathbb{F}_p)$ は，G が有限であることより，有限次元な $\mathbb{F}_p$-線型空間であるが，これへの作用 $G \times V \to V; (g, f) \mapsto (g * f)(g') := f(g'g)$ と定める．

(a)　対応する表現 $\rho : G \to \mathrm{Aut}_{\mathrm{Set}}(V)$ は単射である．実際，$\delta_e(g) = \begin{cases} 1, & g = e, \\ 0, & g \neq e. \end{cases}$ という V の元に注目すると，

$$g \in \mathrm{Ker}\,\rho \Rightarrow g\delta = \delta \Rightarrow (g\delta)(e) = \delta(e) \Leftrightarrow \delta(g) = 1 \Leftrightarrow g = e$$

が従う．

(b)　$\rho(g) : V \xrightarrow{\sim} V; f \mapsto g * f$ は $\mathbb{F}_p$-線型写像であるから，$\mathrm{Im}\,\rho \subset \mathrm{GL}(V) = \mathrm{End}_{\mathbb{F}_p}(V)$ である．

以上で，単射準同型 $\rho : G \hookrightarrow \mathrm{GL}(V)$ を得る．

一般線型群の消息への帰着　有限次元線型空間 V の基底を取ることで，$n := \dim V$ について $V \simeq \mathbb{F}_p^n$ と見て，$\mathrm{GL}(V) \simeq \mathrm{GL}_n(\mathbb{F}_p)$ と同一視し，$G \hookrightarrow^{\rho} \mathrm{GL}(V) \xrightarrow{\sim} \mathrm{GL}_n(\mathbb{F}_p)$ によって G を $\mathrm{GL}_n(\mathbb{F}_p)$ の部分群と見る．すると，例 1.13.3 より，$\mathrm{GL}_n(\mathbb{F}_p)$ には p-Sylow 部分群 U が存在する．したがって，部分群への p-Sylow 部分群の遺伝補題 1.13.4 より，$g \in \mathrm{GL}_n(\mathbb{F}_p)$ が存在して，$G \cap gUg^{-1}$ が G の p-Sylow 部分群となる．

(2) p-Sylow 部分群 P' についても，補題 1.13.4 より，$g \in G$ が存在して，$P' \cap gPg^{-1}$ が P' の p-Sylow 部分群となる．しかしそもそも P' も p-群なので，$\dfrac{|P'|}{|P' \cap gPg^{-1}|} = 1$ が必要．すなわち，$P' \cap gPg^{-1} = P'$ である．これは $P' \subset gPg^{-1}$ を含意する．等号は，p-Sylow 部分群の位数が一定であることより，$|P'| = |P| = |gPg^{-1}|$ から従う．

(3) (a)　$n_{G,p}$ が $|G|$ の約数であることは，G の p-Sylow 部分群全体からなる集合 S_p への共役による作用からわかる．(2) は，この作用はただ一つの G-軌道からなることを言っている．そこで，任意の $P \in S_p$ を取り，$N_G(P) := \mathrm{Stab}_G(P) = \{g \in G \mid gPg^{-1} = P\}$ と定めると，$n_{G,p} = |S_p| = \dfrac{|G|}{|N_G(P)|}$ が成り立つ 1.5.9．よって特に，$n_{G,p}$ は $|G|$ の既約元は一次式のみという主張が代数学の基本定理なのであるな．

(b)　$n_{G,p} \equiv 1 \mod p$ であることは，この共役作用の P への制限 $P \times S_p \to S_p$ に注目する．P の P-軌道は一元集合 $\{P\}$ である．このとき，任意の他の p-Sylow 部分群 $P' \in S_p \backslash \{P\}$ に対して，正規化群 $N_P(P') = \{g \in P \mid gP'g^{-1} = P'\}$ が $N_P(P') \subsetneq P$ を満たすことを示せば，(P'の P 軌道の元の個数) $= \dfrac{|P|}{|N_P(P')|}$ が p の倍数となることから，$|S_p \backslash \{P\}|$ も p の倍数だとわかる．

$\forall_{gg' \in N_P(P')P'}\ gg'P'(gg')^{-1} = g(g'P'g'^{-1})g^{-1} = gP'g^{-1} = P'$ より，$P' \lhd N_P(P')P'$ であるから，第二同型定理 1.7.3 より，$N_P(P')P'/P' \simeq N_P(P')/(N_P(P') \cap P')$ である．[†59]

ここで，$N_P(P')$ は P の部分群より p-群．よって位数の等しい $N_P(P')P'/P$ も p-群．P' も p-群だから $N_P(P')P'$ も第二同型定理と剰余群の位数に関する Lagrange の定理 1.5.5 より $|N_P(P')P'| = \dfrac{|N_P(P')||P'|}{|N_P(P')| \cap P'}$ だから p-群であるが，これは p-Sylow 部分群 P' を含むでの，p-Sylow 群の極大性より $P' = N_P(P')P'$ が必要．すなわち，$N_P(P') \subset P'$ であるから[†60]，$N_P(P') = P$ と仮定すると $P \subset P'$ が従い，p-Sylow 群の位数の一意性から $P = P'$ が必要になってしまう．よって，$N_P(P') \subsetneq P$.

■

要諦 1.13.7. 各種作用を考えながら地に足のついた結果を統一的に引き出すのが天衣無縫の極み．この先に表現論があるのか？

(1) まさかの表現論による有限体の一般線型群 1.13.3 への帰着！代数では値域が重要で，これに F を取ると F-線型表現を得る．特に F を有限に取れるのはあまりに強力である．

[†58] 指数 $[G : P]$ を割り切ることに同値．なお，$\gcd([G : P], p) = 1$ である．
[†59] 実は第二同型定理と設定が違うが，第二同型定理のより簡単な場合となっている．
[†60] P の左移動による G への作用を考えると，P' と同じ軌道に $N_P(P')$ も入っているということなので，これは部分群の定義である．

(2) 部分群の集合に対する共役作用についての中心化群を特に**正規化群**という．p-Sylow 部分群への G の共役作用を考えると $|S_p|$ は $|G|$ の約数で，その P への制限$=P$ による剰余類を考えると $\{P\}$ と p の倍数の位数を持った軌道とに軌道分解される．というのは結局，p-Sylow 部分群が一意的でなかった場合は，P' に対する P の共役 $pP'p^{-1}$ が必ず他の p-Sylow 部分群を産んでしまい，その軌道の数は必ず p の倍数となることを言っている．

(3) (3) において，$n_{G,p}=1$ とは，p-Sylow 部分群が正規であることに同値となる．S_4 は正規部分群も p-Sylow 部分群も持つが，正規な p-Sylow 部分群は持たない．

系 1.13.8．G を有限群とし H をその部分群とする．p を素数とし，H を p-群と仮定する．このとき，H を含む G の p-Sylow 部分群が存在する．

1.13.2　Sylow 部分群による構造決定

多分，退化して降りてきた p-Sylow 部分群の理論が，Abel 群の構造定理と結びついて威力を発揮する．すなわち，p-Sylow 部分群が正規になるとき，そこへの共役作用の制限を考える．正規にならない場合は，p-Sylow 部分群全体の集合 S_p のなす構造への作用を考えると，S_n への作用が定まる．

命題 1.13.9．p,q を $p<q$ かつ $q\not\equiv 1 \mod p$ を満たす素数とする．このとき，位数 pq の群（15, 33 など）G は $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z}$ と同型な Abel 群である．

[証明]．

p-Sylow 部分群の決定　G の p-Sylow 部分群 P を一つとる．G の p-Sylow 部分群の個数 $n_{G,p}$ は $|G|=pq$ の約数であることより，$1,p,q,pq$ のいずれかであるが，$n_{G,p}\equiv 1 \mod p$ より，$n_{G,p}=1$ が必要．すると，P は G の正規で唯一の p-Sylow 部分群である．また位数が p であることよりこれは巡回群 1.5.7 で，$P\simeq\mathbb{Z}/p\mathbb{Z}$ である（巡回群の分類 1.7.7）．

well-definedness　よって，その可逆元について $\mathrm{Aut}_{\mathrm{Grp}}(P)\simeq(\mathbb{Z}/p\mathbb{Z})^\times$ が成り立つ．[†61]準同型 $\mathrm{Ad}: G\to\mathrm{Aut}_{\mathrm{Grp}}(P)$ の像の位数は，準同型定理より $|\mathrm{Im\ Ad}||\mathrm{Ker\ Ad}|=|G|=pq$ の約数で，$\mathrm{Aut}_{\mathrm{Grp}}(P)$ の部分群より $|\mathrm{Aut}_{\mathrm{Grp}}(P)|=p-1$ の約数でもある．$p<q$ より $pq,p-1$ は互いに素であるから，$\mathrm{Im\ Ad}=\{\mathrm{id}_P\}$ である．したがって，G の任意の元は P の任意の元と可換である．

同型の構成　G の q-Sylog 部分群 Q を取ると，全く同様の議論より $Q\simeq\mathbb{Z}/q\mathbb{Z}$ である．

$$\begin{array}{ccc}\varphi: P\times Q & \longrightarrow & G\\ \cup & & \cup\\ (g_1,g_2) & \longmapsto & g_1g_2\end{array}$$

は，P の任意の元と Q の任意の元は可換であるから well-defined で，群準同型である．

可逆性の証明　$|P\times Q|=pq=|G|$ より，φ が単射であることを示せば可逆であることが従う．任意の $(g_1,g_2)\in\mathrm{Ker}\,\varphi$ を取ると，$g_1g_2=e\Leftrightarrow g_1=g_2^{-1}$ より，$g_1,g_2\in P\cap Q$．しかし，Lagrange の定理 1.5.5 より $|P\cap Q|=1$ だから，$g_1=g_2=e$ が従う．

■

命題 1.13.10．p を素数とする．位数 $2p$ の群 G は次のいずれかである．

(1) 巡回群 $G\simeq\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\simeq\mathbb{Z}/2p\mathbb{Z}$.

(2) 二面体群 $G\simeq D_p$.

[証明]．$p=2$ のとき，$G=\mathbb{Z}/4\mathbb{Z},\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2Z$ は Abel 群である．$p=3$ のとき，$G=\mathbb{Z}/6\mathbb{Z}$ は Abel 群で，$S_3=D_3$ は非可換な二面体群である．以下，$p\geqslant 3$ の場合を考える．

p-Sylow 部分群　G の p-Sylow 部分群 P を取ると，その位数は p であるから，これは $P\simeq\mathbb{Z}/p\mathbb{Z}$ なる巡回群である．$n_{G,p}|2p$ かつ $n_{G,p}\equiv 1 \mod p$ より，$n_{G,p}=1$ より，P は正規部分群である．

[†61] どうやら極めて非自明.

2-Sylow **部分群**　G の 2-Sylow 部分群 Q を取るとこれは位数 2 の正規な巡回群で，その元のうち単位元でないもの τ を取ると，τ の位数は 2 だから $\tau \notin P$ となり，$G/P = \{P, \tau P\}$ と表せる（$|G/P| = 2$ より）．

鏡映の定める共役作用への注目　同型 $\mathrm{Ad}(\tau) \in \mathrm{Aut}_{\mathrm{Grp}}(P) = (\mathbb{Z}/p\mathbb{Z})^\times$ の位数は，$p-1$ の約数であるが，2 回合成すると必ず恒等写像となるので，1 か 2 である．

(1)　$\mathrm{Ad}(\tau)$ の位数が 1 であるとき，Q の任意の元は P の任意の元と可換であるから，同型 $P \times Q \xrightarrow{\sim} G; (g_1, g_2) \to g_1 g_2$ が定まる（命題 1.13.9 の証明抽出）．したがって $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ は Abel 群かつ巡回群である．

(2)　$\mathrm{Ad}(\tau)$ の位数が 2 であるとき，$(\mathbb{Z}/p\mathbb{Z})^\times$ の位数 2 の元は -1 のみであるから，$\mathrm{Ad}(\tau)(-) = -^{-1}$ である．P は位数 p の巡回群であるから，その生成元を σ と表すと，$G/P = \{P, \tau P\}$ と併せて，$G = \{e, \sigma, \cdots, \sigma^{p-1}, \tau, \tau\sigma, \cdots, \tau\sigma^{p-1}\}$.

■

注 1.13.11 (二面体群)**.** $n \geqslant 3$ について，D_n は S_n の部分群で，$n = 3$ のとき位数 $2 \cdot 3 = 3 \cdot 2 \cdot 1$ を比べれば明らかなように，両者は一致し，$n \geqslant 4$ のとき真の部分群になる．また，$\varphi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}_{\mathrm{Set}}(\mathbb{Z}/n\mathbb{Z})$ を $\varphi(0) = \mathrm{id}_{\mathbb{Z}/n\mathbb{Z}}, \varphi(1)(-) = -^{-1}$ と定めると，$D_n = \mathbb{Z}/n\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$ となる．$\mathbb{Z}/2\mathbb{Z}$ の元が鏡映変換である．また，$D_{2n} = D_n \times \mathbb{Z}/2\mathbb{Z}$.

二面体群の Sylow 部分群は，n が奇数のとき，$\langle\tau\rangle = \{\sigma^k, \sigma^k\tau\}$ $(k = 0, 1, \cdots, n-1)$ は 2-Sylow 部分群であり，全部で n 個ある．これらが回転について共役であることに注意．中心は単位元のみからなる．一方で n が偶数のとき，中心は単位元と 180 度回転からなる．

第 2 章

Ring

群の射が咲き乱れる世界！

2.1 環の定義と例

（単位的）環とは圏 Ab 内のモノイド対象である（ここでは環は unital で not-necessarily commutative とする）．non-unital である場合は半群対象である．代数（線型構造と環の構造が両立する対象）は圏 R-Mod 内のモノイド対象であるように．乗法が可換であるかと（零元を除いて）可逆であるかがそれぞれ試験紙となる．なお，単位的かどうかも試験紙となる．一般の位相空間上の関数？では落とせば良い．
また，環には演算が 2 種類あるわけだから，多項式という自由対象とそこへの evaluation の発想が肝要になる．この手法が「方程式」というものである．

定義 2.1.1 (ring). 次の 3 条件を満たすアーベル群 A を環という．

(1) $1 \in R$.
(2) 双線型写像 $\cdot : R \otimes R \to R$ が，結合性と 1 に関する単位性を満たす．

要諦 2.1.2. 演算の整合性 $r \cdot (r_1 + r_2) = r \cdot r_1 + r \cdot r_2$ とは，テンソル積の空間から出る双線型性とみなせる．

2.1.1 圏論的対象

例 2.1.3.

(1) Ring の終対象は零環 $(1, \mathrm{id}_1, \mathrm{id}_1)$ である．$1 = 0$ が成り立つことと，零環であることは同値である．
(2) Ring の始対象は整数環 $\mathbb{Z}$ である 2.3.2．群としては生成元が 2 つ ± 1 とあったため大域点としては使えるが始対象ではなかった．もう一つの演算が入ったために方向が確定した，まったく使い勝手が違う．
(3) Grp では $\mathbb{Z}$ だった，大域点として使える対象は $\mathbb{Z}[x]$ に移る 2.3.7.

□

2.1.2 数

例 2.1.4. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ は可換環である． □

例 2.1.5 (整数の剰余環)**.** 任意の整数 $n \geqslant 1$ に対し，$\mathbb{Z}$ の可換環構造が，$\mathbb{Z}/n\mathbb{Z}$ の可換環構造を引き起こす．これは $\mathbb{Z}/(n)$ と同型 **??**．n が素数 p である時は $p\mathbb{Z}$ は極大イデアルとなる 2.5.4 から $\mathbb{Z}/p\mathbb{Z}$ は体となり，$\mathcal{F}_p$ とも表す． □

2.1.3　多項式の環

2 つの演算が定まると多項式という一番形式的で一番基本的な対象が定まり，代数幾何学が始まる．実は函数芽の環は可換局所環で，極大イデアルは $f(0)=0$ を満たす関数の全体と考えられる．[a]

[a] https://ja.wikipedia.org/wiki/局所環

例 2.1.6. 一般の環 A に対し，形式的には環 $A^{\mathbb{N}}$ の部分環 $\{(a_i)\in A^{\mathbb{N}} \mid a_n=0 \text{ f.e.}\}$ として[†1]，A 係数多項式環 $A[X]$ が構成できる．これは単一生成元 X 上の自由 R-結合代数である．[†2]A が可換であることと $A[X]$ が可換であることとは同値．$k[X^1,\cdots,X^n]$ の剰余環として得られる環を体上の有限生成環と言い，特別な対象となる．実は，n 変数多項式について，$(X_1-a_1,X_2-a_2,\cdots,X_n-a_n)$ という形のイデアルは極大になり，F が代数閉体のとき，この形のものに尽きる．□

例 2.1.7. 根の数が考えられるのは整域においてである 2.4.7．整域でない環係数の多項式には，根が無限個存在し得る．□

例 2.1.8 (有理関数体)**.** 多項式も数に似ていて，構成 $\mathbb{Z}\hookrightarrow\mathbb{Q}$ を商体として定式化することにより，有理関数体を得る 2.6.19．□

例 2.1.9. 位相空間 X に対して，$C(X)=\mathrm{Hom}_{\mathrm{Top}}(X,\mathbb{R})$ は可換環となる．□

2.1.4　作用素の環

例 2.1.10. 環 A に対し，$M_n(A)$ $(n\geqslant 1)$ は行列積に関して環になる．A は可換でも $M_n(A)$ が可換でない例がある．□

例 2.1.11. $M_n(\mathbb{C})$ のイデアルは決定される 2.2.13．□

2.1.5　環の射の例

例 2.1.12 (Frobenius map)**.** k を標数 $p>0$ の体とする．$F:k\to k; x\mapsto x^p$ は体の準同型となる：$(xy)^p=x^py^p,(x+y)^p=x^p+y^p,1^p=1$．$F$ は一般に単射であり（一般に被約な環について単射となる），k が有限体のとき全射でもあるから可逆である．Frobenius 写像は，標数 p の可換環がなす圏の恒等関手の間の自然変換である．□

2.2　部分環・イデアル・剰余群

環の乗法は群から可逆性を落とした演算になる．すると，部分群の特徴付け 1.3.4 の消息を失うわけであるから，必然的に加法部分群 I であって，$II^{-1}\subset A$ を満たすような中間的な性質を持つクラスに注目することが自然になる．実際，イデアルの概念は数学を通底して重要になる．そして最初からイデアルの概念はフィルターの双対であることを感じる．
イデアルの振る舞いは群の場合と対照的で，結びは $I+B$ で表せる．交わり $I\cap J$ について，可換環で I,J が互いに素 $(I+J=A)$ ならば，$I\cap J=IJ$ という結果が中国剰余定理である．

2.2.1　部分環・中心

可換環の生成部分環は，その部分環係数の多項式へ代入して得られる元の全体に他ならない．こうして，2 つの演算が定められているとき，多項式が一番基本的で形式的な対象となる．

定義 2.2.1 (subring). $B\subset A$ が部分環であるとは，次の 3 条件が成り立つことをいう：

[†1] ただの place holder とするから，$X_iX_j=X_jX_i, aX_i=X_ia$ とする．
[†2] 自由対象を内部に持つという点で環という代数系は特徴付けられる？

(1) B は A の加法に関する部分群である.
(2) $\forall_{b_1,b_2\in B}\ b_1b_2 \in B$.
(3) $1 \in B$[†3].

例 2.2.2.

(1) $\mathbb{Z},\mathbb{Q},\mathbb{R}$ はいずれも $\mathbb{C}$ の部分環である.
(2) A は $A[X]$ の部分環である. 上述の数の関係の一般化とみれるのが肝である.
(3) $\{0\} \subset A$ は自明な部分群であるが, これは A 自身が零でない（すなわち $0=1$ でない）限り部分環ではない.
(4) $A\times\{0\} \subset A\times B$ は部分群であり, 積について閉じてもいるが, B が零でない限り, $(1,1)\notin A\times B$ であるから部分環ではない.

□

定義 2.2.3 (generated ring). $S \subset A$ を部分集合, B を部分環とする. S,B の両方を含む部分環で最小であるものが存在する. これを $B[S]$ と表す.

補題 2.2.4 (可換環の生成部分環は自由環を潰して作れる). A が可換であるとき,

$$B[a_1,\cdots,a_n] = \{f(a_1,\cdots,a_n)\in A \mid f\in B[X_1,\cdots,X_n]\}$$

と表せる.

[証明].

$\subset$　右辺は確かに, $B,S=\{a_1,\cdots,a_n\}$ を含む A の部分環である.
$\supset$　右辺の元を任意に取ると, B の元と S の元の有限積の有限和であるから, 確かに左辺にも含まれる.

■

例 2.2.5.

(1) $\mathbb{C}$ の部分環 $\mathbb{Z}$ と $\sqrt{2}\in\mathbb{C}$ を考えることより, 生成される部分環 $\mathbb{Z}[\sqrt{2}]$ を考えることができる. $\mathbb{Z}[\sqrt{2}] = \left\{a+b\sqrt{2} \mid a,b\in\mathbb{Z}\right\}$ である.
(2) $\mathbb{R}[\sqrt{-1}]=\mathbb{C}$ である.

□

補題 2.2.6 . 中心を

$$Z(A) := \{a\in A \mid \forall_{b\in A}\ ab=ba\}$$

と定めると, これは A の部分環である.

[証明]. アーベル群 $Z(A)$ は, 積について閉じており, 1 も含むため. ■

2.2.2　部分環の束

$S_1\cap S_2, S_1S_2$ も部分環になるが, この振る舞いはイデアルの振る舞いと対照的である. 簡単に言えば, 部分環は高次項も含むが, イデアルは特定の元を「基底」とみなしてその線型結合で表される元のみに注目する.

[†3] 一般に環を非単位的とし, 部分環と言ったときは単位元が違っていても良いとする定義もある.

2.2.3　イデアル

イデアル＝部分加群

正規部分群に当たる概念である．A 自身を A-加群とみなしたときの，部分 A-加群（空間）の概念に一致．生成イデアルも，部分環同様，自由生成を潰すことによって得られる．違いは，1 次の項しか用いないことである．これがある種の線型性を意味する（部分加群っぽさ）．

定義 2.2.7 ((left, right, two-sided) ideal). 部分集合 $I \subset A$ について，

(1) I が A の**左イデアル**であるとは，次の 3 条件が成り立つことをいう．
  (a) $0 \in I$.
  (b) $\forall_{x,y\in I}\ x+y \in I$.
  (c) $\forall_{a\in A}\ \forall_{x\in I}\ ax \in I$.
(2) I が A の**右イデアル**であるとは，上述の 3 条件のうち，(c) を $\forall_{a\in A}\ \forall_{x\in I}\ xa \in I$ としたものが成り立つことをいう．
(3) I が左イデアルかつ右イデアルであるとき，**両側イデアル**であるという．
(4) A が可換であるとき，3 つの概念は同値になり，まとめて**イデアル**という．

注 2.2.8 (名前の由来)**.** 名前の由来は，Kummer が Fermat 予想の研究の際に，素因数分解の一意性を成り立たせるための道具として開発した理想数の概念を Dedekind が整理して生まれた．

注 2.2.9 (加法部分群との関係)**.**

加法部分群との関係　左イデアル I は，条件 (c) について $a=-1$ とすれば $-x \in I$ だから，I は特に加法について部分群である．一般の加法部分群 $H < A$ が左イデアルでもあるための必要十分条件は，条件 (c) を確かめれば良い．

乗法中立元との関係　$I = A \iff 1 \in I$ である．条件 (c) について，$x=1$ とできてしまえるのならば，これは $\forall_{a\in A}\ a \in I$ と同値になってしまうため．

定義 2.2.10 (generated ideal).

(1) $S \subset A$ を含む最小の左・右・両側イデアルが存在する．
(2) A が可換であるとき，これらは一致し，これを (S) と表す．
(3) $(S) = I$ が成り立つとき，S を I の**生成系**であるという．
(4) 有限な生成系が存在する I を**有限生成イデアル**，単元集合を生成元にもつ I を**単項イデアル**という．

注 2.2.11. 単項イデアルが，巡回群に当たる概念である．また，最大公約数に関する記法 $(a,b)=1$ は $(a,b)=(1)$ の略記であった．では有理式の記法は？

補題 2.2.12 (生成イデアルの表示：部分加群の元の一次結合による表示). $S \subset A$ とする．

(1) S で生成される左イデアルは $\left\{ \sum_{s\in S} a_s S \;\middle|\; (a_s)_{s\in S} \in \bigoplus_{s\in S} A \right\}$.[†4]
(2) S で生成される右イデアルは $\left\{ \sum_{s\in S} S b_s \;\middle|\; (b_s)_{s\in S} \in \bigoplus_{s\in S} A \right\}$.
(3) S で生成される両側イデアルは $\bigcup_{n\in\mathbb{N}} \left\{ \sum_{i=1}^{n} a_i s_i b_i \;\middle|\; s_i \in S, a_i, b_i \in A \right\}$．ただし，$n=0$ のとき，$\sum_{i=1}^{0} a_i s_i b_i = 0$ とする．
(4) 特に A が可換であるとき，$(x_1,\cdots,x_n) = \left\{ \sum_{i=1}^{n} a_i x_i \;\middle|\; a_1,\cdots,a_n \in A \right\}$.

[証明]. ■

[†4] $\bigoplus_{s\in S} A$ は f.e. であることに注意．よって，無限和は発生しない．

例 2.2.13 (整数のイデアル)**.**

(1) $\mathbb{Z}$ のイデアルは，$\mathbb{Z}$ の部分群でもあるから，ある $n \in \mathbb{N}$ が存在して $I = n\mathbb{Z}$ と表せる 1.3.16．逆に，部分群 $n\mathbb{Z}$ はイデアルになる：$\forall_{a\in\mathbb{Z}}\ an\mathbb{Z} = n\mathbb{Z}$．よって，$n\mathbb{Z} = (n)$ とも表せる．

(2) $\mathbb{C}[X,Y]$ のイデアル (X,Y) とは，

$$\begin{aligned}(X,Y) &= \{fX + gY \in \mathbb{C}[X,Y] \mid f,g \in \mathbb{C}[X,Y]\}\\ &= \left\{f \in \mathbb{C}[X,Y] \mid f \text{ の定数項は } 0\right\}\end{aligned}$$

となる．これが単項イデアルではないことは，次のようにしてわかる．$(X,Y) = (f) \Rightarrow X, Y \in (f) \Rightarrow f \in \mathbb{C}^\times$ である．すると，$1 \in (f)$ より，$(f) = \mathbb{C}[X,Y] = (X,Y)$ が必要だが，これは矛盾．

(3) 非可換環 $M_n(\mathbb{C})$ の左イデアル，両側イデアルを調べる．

□

2.2.4　剰余環

補題 2.2.14 (quotient ring). 環 A とその両側イデアル I について，剰余群 A/I は，

$$\begin{array}{ccc} A/I \times A/I & \longrightarrow & A/I \\ \cup & & \cup \\ (a+I, b+I) & \longmapsto & ab+I \end{array}$$

を積として環となる．

[証明].

well-definedness　$a + I = a' + I, b + I = b' + I$ すなわち $\exists_{x,y\in I}\ a' = a + x, b' = b + y$ として，$ab + I = a'b' = I$ を導く．I は両側イデアルだから，

$$a'b' = (a + x)(b + y) = ab + xb + ay + xy = ab + I.$$

環の公理　乗法の結合性と単位性，分配性は A の環構造から自然に従う．

■

例 2.2.15. ?? $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \cdots, \overline{n-1}\}$ と形式的に構成した環は，剰余環 $\mathbb{Z}/(n)$ と同一視できる．□

2.3　環の射と準同型定理

2.3.1　環の射と引き起こされるイデアル対応

定義 2.3.1 . 写像 $f : A \to B$ が次の 3 条件を満たすとき，環準同型であるという．

(1) f は群準同型である．

(2) $\forall_{a,a'\in A}\ f(aa') = f(a)f(a')$.

(3) $f(1) = 1$.

例 2.3.2 (整数環は始対象である)**.** 任意の環 A について，$\varphi_A : \mathbb{Z} \to A$ が，$\varphi_A(0) = 0, \varphi_A(1) = 1$ の時点で，その他についても帰納的に定まる．実際，$f : \mathbb{Z} \to A$ も準同型とすると，$f(1) = 1 = \varphi_A(1)$ を満たすが，大域点としての $\mathrm{Hom}(\mathbb{Z}, A)$1.3.17 より，$f = \varphi_A$ が従う（乗法単位元をどこに移すかで，$\mathbb{Z}$ からの写像は一意に定まるということを言い換えただけ）．

この関係より，$\varphi_A(n)$ のことも n と表す．$\mathbb{Z}$ が可換であるため，$\mathrm{Im}\ \varphi_A \subset Z(A)$ が成り立つ．□

補題 2.3.3 (可逆性の特徴付け). 準同型 $f : A \to A'$ について，次の 2 条件は同値．

(1) f は可逆である．

(2) f は全単射である．

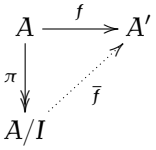
[証明]. (2)⇒(1) を示せば良い．f が全単射である時，逆写像 f^{-1} は群準同型である．これが積と単位元を保つことを示せば良い．

(1) $a', b' \in A'$ を任意にとり，対応する元を $a, b \in A$ とすると，$f(ab) = f(a)f(b) = a'b'$ より，$f^{-1}(a'b') = ab = f^{-1}(a)f^{-1}(b)$.
(2) $f(1) = 1$ より，$1 = f^{-1}(1)$.

■

命題 2.3.4 (イデアルの対応). $\pi : A \twoheadrightarrow A/I$ を自然な全射とする．このとき，A のイデアルで I を含むものと，A/I のイデアルとの間に，包含関係を保つ全単射 π^*, π_* が存在する．

命題 2.3.5 (剰余環の普遍性). I を A の両側イデアルとする．任意の環準同型 $f : A \to A'$ に対して，$f(I) = 0$ を満たすならば，次の図式を可換にする準同型 $A/I \to A'$ がただ一つ存在する：



[証明]. $f : A \to A'$ はアーベル群 A, A' の間の群準同型であり，$I \lhd A$ であるから，剰余群の普遍性 1.6.9 より，上の図式を可換にする群準同型 $\bar{f} : A/I \to A'$ がただ一つ存在する．これが積と単位元を保ち，環準同型でもあることを示せば良い．

(1)

■

2.3.2　多項式環の普遍性

$\mathbb{Z}$ は Grp では $F(1)$ と同型であるから大域点として用いることができた．Ring では始対象となった．では大域点として使えるのは何かというと，$\mathbb{Z}[X]$ である．自由対象とそこへの evaluation というのが，大域点の本質であったのかもしれない．

命題 2.3.6 (多項式環からの準同型). A, B を環とし，$n \geqslant 1$ を整数とする．

(1) $\mathrm{Hom}(A[X_1, \cdots, X_n], B) \simeq_{\mathrm{Set}} \{(\phi, b_1, \cdots, b_n) \in \mathrm{Hom}(A, B) \times B^n \mid b_i b_j = b_j b_i, \phi(a) b_i = b_i \phi(a)\}$.
(2) 特に，B が可換であるとき，$\mathrm{Hom}(A[X_1, \cdots, X_n], B) \simeq \mathrm{Hom}(A, B) \times B^n$

[証明]. 互いに逆な 2 つの写像を構成する．

$\subset$　$f \in \mathrm{Hom}(A[X_1, \cdots, X_n], B)$ に対し，$\phi := f|_A : A \to B, b_i := f(X_i)$ と定めると，$X_i X_j = X_j X_i, aX_i = X_i a$ より，$b_i b_j = b_j b_i, \phi(a) b_i = b_i \phi(a)$ が成り立つ．

$\supset$　$(\phi, b_1, \cdots, b_n)$ が定める対応

$$\sum_{(i_1, \cdots, i_n) \in \mathbb{N}^n} a_{i_1, \cdots, i_n} X_1^{i_1} \cdots X_n^{i_n} \mapsto \sum_{(i_1, \cdots, i_n) \in \mathbb{N}^n} \phi(a_{i_1, \cdots, i_n} b_1^{i_1} \cdots b_n^{i_n})$$

は環準同型になる．

■

系 2.3.7 (ある種の evaluation). 任意の環 A に対して，次の自然な同型が存在する：$\mathrm{Hom}(\mathbb{Z}[X], A) \simeq_{\mathrm{Set}} U(A)$.

[証明]. $\mathbb{Z}$ は始対象である 2.3.2 から，$\phi : \mathbb{Z} \to A$ は一意的に存在する．したがって，$f : \mathbb{Z}[X] \to A$ と $f(X)$ とが対応づけられる．■

2.3.3　像と核

命題 2.3.8 . 準同型 $f : A \to B$ について，

(1) 部分群 $\mathrm{Ker}\, f < A$ は A の両側イデアルである.
(2) 部分群 $\mathrm{Im}\, f < B$ は B の部分環である.

[証明].

(1) 任意の $a \in A, x \in \mathrm{Ker}\, f$ について, $f(ax) = f(a)f(x) = 0$ より, $ax \in \mathrm{Ker}\, f$. 逆も同様.
(2) 任意の $f(a), f(a') \in B$ について, $f(a)f(a') = f(aa') \in \mathrm{Im}\, f, 1 = f(1) \in \mathrm{Im}\, f$ より.

■

例 2.3.9 (factor theorem). $(\mathrm{id}, a) \in \mathrm{Hom}(B, A) \times A^n$ に対応する群準同型の核を, $B = A[X]$ の時について考える.

(1) 評価写像 $\phi_a : A[X] \to A; f \mapsto f(a)$ について, $\mathrm{Ker}\, \phi_a = (X - a)$ が成り立つ.
(2) $n \geqslant 2$ について, $\underline{a} := (a_1, \cdots, a_n) \in A^n$ とする. $\phi_{\underline{a}} : A[X_1, \cdots, X_n] \to A; f \mapsto f(a_1, \cdots, a_n)$ の核は, $\mathrm{Ker}\, \phi_{\underline{a}} = (X_1 - a_1, \cdots, X_n - a_n)$ である.

□

[証明].

(1) $(X - a)$ を因数に含む多項式は a で評価すると 0 になるから, $\supset$ が成り立つ. $f(X) = c_n X^n + \cdots + c_0 \in \mathrm{Ker}\, \phi_a$ を任意に取る. すると $f(a) = 0$ であるから,

$$f(X) = f(X) - f(a) = c_n(X^n - a^n) + \cdots + C_1(X - a)$$

であるが, 一般に $k \geqslant 1$ について, $X^k - a^k = (X - a)(X^{k-1} + \cdots + a^{k-1}) \in (X - a)$ より, $f(X) \in (X - a)$ が従う.
(2) $f \in \mathrm{Ker}\, \phi_{\underline{a}}$ を任意に取る. 一文字固定して, $f_n := f(X_1, \cdots, X_{n-1}, a_n) \in A[X_1, \cdots, X_n]$ と置くと, $f_n \in \mathrm{Ker}\, \phi_{(a_1, \cdots, a_{n-1})}$ より, $f_n \in (X_1 - a_1, \cdots, X_{n-1} - a_{n-1}) \subset A[X_1, \cdots, X_{n-1}]$ が帰納法の仮定より従うから, 特に, $f_n \in (X_1 - a_1, \cdots, X_{n-1} - a_{n-1}) \subset A[X_1, \cdots, X_n] = A[X_1, \cdots, X_{n-1}][X_n]$. すると, $\varphi_{a_n} : A[X_1, \cdots, X_{n-1}][X_n] \to A[X_1, \cdots, X_{n-1}]$ について, $(f - f_n)(a_n) = 0$ より, $f - f_n \in \mathrm{Ker}\, \phi_{a_n} = (X_n - a_n) \subset A[X_1, \cdots, X_n]$ が従う. よって, $f = (f - f_n) + f_n \in (X_1 - a_1, \cdots, X_n - a_n)$.

■

要諦 2.3.10. 自由生成 $A[X_1, \cdots, X_n] = (A[X_1, \cdots, X_{n-1}])[X_n]$ が成り立つことに注意.

2.3.4　準同型定理

準同型定理とは, 単完全列への分解である. これは変わらないが, 第二同型定理が「部分環とイデアル」という非対称性をあらわにしている.

定理 2.3.11 (準同型定理). 環準同型 $f : A \to A'$ に対して, 次の図式を可換にするただ一つの同型 $\overline{f} : A/\mathrm{Ker}\, f \xrightarrow{\sim} \mathrm{Im}\, f$ が存在する:

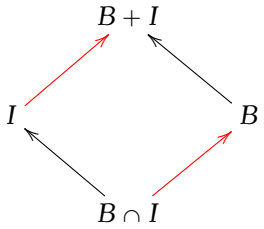
$$\begin{array}{ccc} A & \xrightarrow{f} & A' \\ \downarrow & & \uparrow \\ A/\mathrm{Ker}\, f & \xrightarrow[\overline{f}]{\sim} & \mathrm{Im}\, f \end{array}$$

[証明]. 構成は, 全射準同型 $f : A \twoheadrightarrow \mathrm{Im}\, f$ に対する剰余環の普遍性 2.3.5 による. この $\overline{f} : A/\mathrm{Ker}\, f \twoheadrightarrow \mathrm{Im}\, f$ が可逆であることを示せば良い.

これは, その一意性より, $f : A \to \mathrm{Im}\, f$ に剰余群の普遍性を適用して得られる準同型に一致し, 群の準同型定理 1.7.1 より, 可逆である. 特に, 全単射である. よって, 2.3.3 より, 環の同型でもある. ■

系 2.3.12 (第二同型定理). I を A の両側イデアル, B を A の部分環とする.

(1) $B+I$ は部分環である.
(2) $B\cap I$ は両側イデアルである.
(3) $B/(B\cap I)\xrightarrow{\sim}(B+I)/I$.[†5]

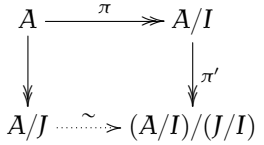


[証明].

(1) 任意の $b+x, b'+x'\in B+I$ に対して，$(b+x)(b'+x')=bb'+bx'+xb'+xx'$ は，I が両側イデアルであることより，再び $B+I$ の元．また，$1=1+0\in I+B$.
(2) 合成 $\varphi: B\hookrightarrow^{i} B+I\twoheadrightarrow (B+I)/I$ の核は，$\operatorname{Ker}\varphi=i^{-1}(I)=B\cap I$．よって，$B\cap I$ は両側イデアルである.
(3) あとは，φ が全射であることを示せば，準同型定理より，同型 $\overline{\varphi}: B/B\cap I\xrightarrow{\sim}(B+I)/I$ を得る．$(B+I)/I$ の元は，任意の $b\in B, x\in I$ について $b+x+I=b+I$ と表せるが，これは $\varphi(b)$ である.

■

系 2.3.13 (第三同型定理). I, J を A の両側イデアルで，$I\subset J$ とする．J/I は A/J の両側イデアルであり，$A/J\simeq (A/I)/(J/I)$.



[証明]. $J/I=\pi_*(J)$ より，J/I は A/I の両側イデアルである（イデアルの対応 2.3.4）.
合成 $\varphi:=\pi'\circ\pi$ は全射の合成であるから全射である．$\operatorname{Ker}\varphi=\pi^{-1}(\operatorname{Ker}\pi')=\pi^{-1}(J/I)=J$ より，準同型定理 2.3.11 から，$A/J\xrightarrow{\sim}(A/I)/(J/I)$ が引き起こされる.

■

2.3.5　射の扱い

単射は左可逆かはまだ検証していないが，単射の性質が，「部分構造」であるための性質の全てである.

命題 2.3.14 .

(1) $f: A\to B$ を準同型とする．イデアル $I\subset A$ に対して，$f(I)$ は B の部分環 $\operatorname{Im} f$ のイデアルである.
(2) 単射 $i: A\hookrightarrow B$ に対して，A が零でないとき，B が整域ならば A も整域.

[証明].

(1)　(i) $0=f(0)\in f(I)$.
　(ii) 任意の $f(x), f(y)\in f(I)$ について，$f(x)+f(y)=f(x+y)\in f(I)$.
　(iii) 任意の $f(a)\in\operatorname{Im} f, f(x)\in f(I)$ について，$f(a)f(x)=f(ax)\in f(I)$.
(2) 任意の $a, b\in A$ について，$ab=0$ とする．$i(ab)=i(a)i(b)=0$ より，B が整域であることから $i(a)=0\vee i(b)=0$ である．i は単射であるから $\operatorname{Ker} i=\{0\}$ より，$a=0\vee b=0$ が従う.

■

[†5] はみ出たイデアル I で割ると，内部で割ったのと同じ.

2.4　可換環論

可換環の重要なクラスを 2 つ定義する．

(1) 非自明な零因子を持たない可換環を整域という．
(2) 非自明な不可逆元を持たない可換環を体という．

可逆元は正則元だから，体は整域である．

記法 2.4.1. I, J を可換環 A のイデアルとすると，次のようにイデアルの構成を定める．

(1) $I+J$ は再び A のイデアルである．
(2) $IJ := (xy \in A \mid x \in I, y \in J)$．$I^k$ $(k \in \mathbb{N})$ も同様に定める．$IJ \subset I \cap J$ に注意．逆も成り立つのは I, J が互いに素のとき 2.9.4.
(3) 環準同型 $f : A \to B$ について，$f(I)$ で生成される B のイデアルを $f(I)B := (f(I))$ と定める．[†6] $f(I)$ の生成する B のイデアルの任意の元は bx $(b \in B, x \in f(I))$ と表せる（補題 2.2.12）からである．f が mono など明らかな場合は IB とも表す．

例 2.4.2 (イデアルとしての n 次以上の式)**.** 体係数多項式の環 $F[X,Y]$ のイデアル $I = (X,Y)$ について，$I^k = (X^k, X^{k-1}Y, \cdots, Y^k)$ $(k \geqslant 1)$．□

2.4.1　整域

非自明な零因子を持たない可換環

整域の概念は整数全体の成す環の一般化になっており、整除可能性を調べるのに自然な設定を与える。$A[X]$ の可逆元は $A^\times$ だけに思えるが，これは可換環 A が整域である場合にしか成り立たない（非自明な零因子がなければ良い）．

定義 2.4.3 (regular, zero divisor, integral domain). A を可換環とする．

(1) $a \in A$ が**正則元**であるとは，これが定める左移動 $\varphi_a : A \to A$ が単射であることをいう．正則でない元を**零因子**と呼ぶ．[†7]
(2) 可換環 A が**整域**であるとは，$\{a \in A \mid a \text{ は正則 }\} = A \backslash \{0\}$ が成り立つことをいう．

注 2.4.4.

(1) 可逆元＝単元は，左移動は全単射となるため，正則元である．
(2) 零因子は非可換環についても左・右・両側が考えられる．
(3) 零環は整域となるには単純すぎる．$\{a \in A \mid a \text{ は正則 }\} = A$ が成り立ってしまうため．
(4) A が整域であることの必要十分条件は，$A \neq 0$ かつ任意の零でない元が正則であること，また，$A \neq 0$ かつ $\forall_{a,b \in A}\ ab = 0 \Leftrightarrow a = 0 \vee b = 0$．すなわち，$0 \subset A$ が素イデアルになることと同値．

命題 2.4.5. A が整域ならば，$A[X]$ も整域であり[†8]，$A[X]^\times = A^\times$．

[証明].

整域である　$A \neq 0$ より，$A \subset A[X] \neq 0$ である．任意に $f, g \in A[X] \backslash \{0\}$ をとり，$fg \neq 0$ を示す．f, g の最高次項を aX^m, bX^n $(a, b \in A \backslash \{0\}, m, n \geqslant 0)$ とおくと，$ab \neq 0$ より，fg の最高次項は $abX^{m+n} \neq 0$（環 A の可換性を使った）．

乗法群　$A^\times \supset A[X]^\times$ を示せば良い．$f \in A[X]^\times$ を任意にとると，$fg = 1$ を満たす $g \in A[X]^\times$ が存在する．f, g の最高次項をそれぞれ aX^n, bX^m と置くと，$abX^{n+m} = 1$ より（環 A の可換性を使った），$ab = 1, n + m = 0$ すなわち $a \in A^\times, n = 0$

[†6] イデアルの対応により，一般に $f(I)$ は $\operatorname{Im} f$ のイデアルではあるが，B のイデアルであるとは限らない．
[†7] 左移動 $\varphi_a : A \to A$ が単射でないとは非自明な核を持つということだから，非自明な零を発生させ得る因子ということである．
[†8] $A \subset A[X]$ より，実はこれが必要十分条件である

が必要．よって，$f = a \in A^\times$．

■

注 2.4.6. A を整域でない可換環とすると，$A = \mathbb{Z}/p^2\mathbb{Z}$ が反例となる．$(\overline{p}X + \overline{1})(-\overline{p}X + \overline{1}) = -\overline{p}^2X^2 + \overline{1} = \overline{1}$ である．

命題 2.4.7 (多項式の根の数). A を整域とし，$f \in A[X]\backslash\{0\}$ とする．$n := \deg f$ とすると，

$$|\{a \in A \mid f(a) = 0\}| \leqslant n.$$

[証明]. 因数定理 2.3.9 による．

$n = 0$ のとき　$|\{a \in A \mid f(a) = 0\}| = |\varnothing| = 0 \leqslant 0.$

$n > 0$ のとき　$\{a \in A \mid f(a) = 0\} \neq \varnothing$ とすると，$f(a_1) = 0$ を満たす $a_1 \in A$ が存在する．すると，a_1 での評価写像 $\mathrm{ev}_{a_1} : A[X] \to A$ について，$\mathrm{Ker}\,\mathrm{ev}_{a_1} = (X - a_1)$ であるから，ある $g(X) \in A[X]$ が存在して，$f(X) = g(X)(X - a_1)$ と表せる．特に，$\deg g < n$．このとき，

$$\begin{aligned} f(a) = 0 &\Leftrightarrow g(a)(a - a_1) = 0 \\ &\Leftrightarrow g(a) = 0 \vee a = a_1 \qquad \because A \text{ は整域} \end{aligned}$$

より，$\{a \in A \mid f(a) = 0\} = \{a \in A \mid g(a) = 0\} \cup \{a_1\}$.

■

2.4.2　体

体とは素数である

非自明な不可逆元を持たない可換環を体という．この体にはイデアルが 2 つ（非自明なイデアルを持たない）という特徴づけがある．これは単純群同様，素数の一般化と思える．連結性も，ある種の素数性をいう．

2.4.2.1　定義と特徴付け

定義 2.4.8 (field). 可換環 A が体であるとは，$A^\times = A\backslash\{0\}$ を満たすことをいう（A を一般の環とするとき，斜体という）．

注 2.4.9 (too simple to be prime)**.**

(1) 零環は体ではない．$A^\times = \{0\} \neq A\backslash\{0\} = \varnothing$ である．
(2) 可換環 A が体であるための必要十分条件は，$A \neq 0$ かつ $A\backslash\{0\}$ の任意の元が可逆であること．

命題 2.4.10 (体の特徴付け). 可換環 A について，

(1) A は体である．
(2) A のイデアルは 2 つである．

[証明].

$\Rightarrow$　$0 \subsetneq A$ に注意．$0 \subsetneq I \subset A$ を満たすイデアル I を任意に取ると，零でない元 $x \in I\backslash\{0\}$ が取れる．これは可逆だから，$y \in A$ が存在して $xy = 1 \in I$．よって，$A = I$ が従う．

$\Leftarrow$　零環のイデアルはただ一つなので，$A \neq 0$．任意に $a \in A\backslash\{0\}$ を取ると，これが生成するイデアルは $(a) = A$ である．よって，$1 \in (a)$，すなわち，$\exists_{b \in A}\, ab = 1$.

■

系 2.4.11 (体とは素数である). 可換環 $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ は体である．

[証明]. 任意にイデアル $I \subset \mathbb{F}_p$ を取ると，これは特に部分群だから，$|I| = 1, p$ である 1.5.6. ■

2.4.2.2　体からの射は単射

命題 2.4.12 (体から出る射). F を体，A を零でない環とする．任意の環準同型 $f : F \to A$ は単射である．

[証明]. $\mathrm{Ker}\, f$ は体 F のイデアル 2.3.8 なので，$\mathrm{Ker}\, f = 0$ または F（体の特徴付け 2.4.10）．しかし，$\mathrm{Ker}\, f = F$ とすると，$1 = f(1) = 0$ が従うので，A が零環であることが必要だが，これは仮定に矛盾する． ■

2.4.2.3　体の乗法群は巡回群

体の乗法群の有限部分群は巡回群になる．これは殆ど多項式の根の数 2.4.7 より従う．

命題 2.4.13 . F を体，G を $F^\times$ の有限部分群とする．このとき，G は巡回群である．特に，有限体 F の乗法群 $F^\times$ は巡回群である（原始根の存在定理）．[†9]

[証明]. F は体であり特に可換環であるから，その乗法群の部分群 G は Abel 群である．有限 Abel 群が巡回群であるための特徴付け 1.9.18 より，任意の素数 p について $|\{x \in G \mid x^p = 1\}| \leqslant p$ であることを示せば良い．これは，体 F は特に整域であるから，多項式の根の数 2.4.7 より従う． ■

2.4.3　環の捩れと根基

群の捩れとは，$\exists_{n\in\mathbb{N}}\, g^n = e$ を満たす元を呼ぶのであった（定義 1.2.8）．環の冪零元とは，$\exists_{n\in\mathbb{N}}\, a^n = 0$ を満たす元を呼ぶ．このような元の集まりを冪零根基と呼ぶ．歴史上この概念を一般化して，「n 乗するとイデアル I に入る元全体の集まり」を根基 $\sqrt{I}$ というようになった．冪零根基は $I = 0$ の場合である．

定義 2.4.14 (radical).

(1)

定義 2.4.15 (nilpotent, nilradical, reduced).

(1) 可換環の元 $a \in A$ が**冪零**であるとは，次が成り立つことをいう：$\exists_{n\in\mathbb{N}}\, a^n = 0$.
(2) A の冪零元全体はイデアルをなし，A の**冪零根基**といい，$\sqrt{0}$ と表す．
(3) $\sqrt{0} = 0$ を満たす，冪零根基の縮退した可換環を**被約**という．[†10]

注 2.4.16 (radical). 環のイデアル $I \subset R$ について，対応する**根基**とは，新たなイデアル $\sqrt{I} := \{r \in R \mid \exists_{n\in\mathbb{N}}\, r^n \in I\}$ を指す．冪零根基とは自明なイデアル $0 \subset R$ に対応する根基である．この根基の対応が実は関手的であり（根基関手），これを研究する分野を torsion theory と呼ぶ．

[証明]. $\sqrt{0}$ がイデアルの 3 つの公理を満たすことを確認する．

(1) $0 \in \sqrt{0}$ である．
(2) 任意に $x, y \in \sqrt{0}$ を取ると，$\exists_{n,m\in\mathbb{N}}\, x^m = y^n = 0$．すると，$A$ は可換環であるから，二項展開して $(x+y)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} x^i y^{m+n-i} = 0$ より，$x + y \in \sqrt{0}$.
(3) 任意に $a \in A, x \in \sqrt{0}$ を取ると，$ax \in \sqrt{0}$.

■

例 2.4.17 (有限体の冪零根基). $\mathbb{Z}/p^m\mathbb{Z}$ $(m \geqslant 1)$ の冪零根基は $p\mathbb{Z}/p^m\mathbb{Z}$ である．よって，$\mathbb{Z}/p^m\mathbb{Z}$ が被約であることは，

[†9] ただし原始根とは，有限体 $\mathbb{F}_p$ について，$(\mathbb{F}_p)^\times$ を生成する元のことをいう．
[†10] 商環 $R/\sqrt{0}$ を簡約部分 (reduced part) と呼ぶ．

$p\mathbb{Z}/p^m\mathbb{Z} = 0$ すなわち $m = 1$ と同値．実際，

$$\begin{aligned}\overline{a} \in \sqrt{0} &\Leftrightarrow \exists_{n\in\mathbb{N}}\ p^m \mid a^n \\ &\Leftrightarrow \exists_{n\in\mathbb{N}}\ p \mid a \Leftrightarrow \overline{a} \in p\mathbb{Z}/p^m\mathbb{Z}.\end{aligned}$$

□

2.5　素イデアルと極大イデアル

素イデアルの性質は半順序を定める．束と双対なのが強調される．

2.5.1　素イデアル・極大イデアルの定義と特徴付け

整数環 $\mathbb{Z}$ の性質 $p \mid ab \Rightarrow p \mid a \vee p \mid b$ とは，イデアルの言葉では $ab \in (p) \Rightarrow a \in (p) \vee b \in (p)$ である．これが素イデアルの源霊性である．素イデアルは割ると整域になり，極大イデアルは割ると体になる（ように作った）．つまり，$\pi : A \twoheadrightarrow A/I$ が定めるイデアルの対応により，A/I の言葉で特徴付けられる．0 というイデアルは特別であり，これとどのように対応づくかによってイデアルの性質が決まる．実は素イデアルの例に極大イデアルがある．ここで極大性が現れるとは．近いのか．

定義 2.5.1 (prime, maximal). 可換環 A のイデアルについて，

(1) イデアル $\mathfrak{p}$ が**素**であるとは，次の 2 条件を満たすことをいう：
  (a) (properness) $\mathfrak{p} \neq A$.
  (b) $\forall_{a,b\in A}\ ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p} \vee b \in \mathfrak{p}$.
(2) イデアル $\mathfrak{m}$ が**極大**であるとは，次の 2 条件を満たすことをいう：
  (a) (properness) $\mathfrak{m} \neq A$.
  (b) A のイデアル I であって，$\mathfrak{m} \subsetneq I \subsetneq A$ を満たすものは存在しない．

命題 2.5.2 (素・極大の特徴付け). I を可換環 A のイデアルとする．

(1) I が素であることは，A/I が整域であることに同値．
(2) I が極大であることは，A/I が体であることに同値．

[証明]. まず，I が真のイデアルであることは，A/I が零でないことに同値．したがって，残りは整域と体の特徴付け 2.4.4,2.4.9 を確認すれば良い．

(1) I が素であるための条件 (b)$\forall_{a,b\in A}\ ab \in I \Rightarrow a \in I \vee b \in I$ は (逆は自明)，A/I が整域であるための条件 2.4.4$\forall_{a',b'\in A/I}\ a'b' = 0 \Leftrightarrow a' = 0 \vee b' = 0$ に同値．
(2) 体の特徴付け 2.4.10 より，A/I が体であることは $0 \subsetneq \bar{J} \subsetneq A/I$ を満たす A/I のイデアル $\bar{J}$ が存在しないことと同値で，これはイデアルの対応 2.3.4 より，I が極大であるための条件 (b)$I \subsetneq J \subsetneq A$ を満たす A のイデアル $J(= \pi^*(\bar{J}))$ が存在しないことに同値．

■

系 2.5.3 . 極大イデアルは素である．

[証明]. 体は整域である（可逆元は正則なので）ことと，素イデアルの特徴付け 2.5.2 より． ■

例 2.5.4 (素イデアルと極大イデアル).

(1) $\mathbb{Z}$ のイデアルは $n\mathbb{Z}$ の形をしている 2.2.13．$n\mathbb{Z}$ が素であることは，$\mathbb{Z}/n\mathbb{Z}$ が整域であることに同値だから，$n = 0$ であるか，n が素数であることに同値．$n\mathbb{Z}$ が極大であることは，n が素数であることに同値．

(2) $(X-a)$ は $F[X,Y]$ の素イデアルであるが，極大イデアルではない．実際，評価写像 $\mathrm{ev}_a : F[X,Y] \twoheadrightarrow F[Y]$ について，準同型定理より $F[X,Y]/(X-a) \simeq F[Y]$ であるが，$F[Y]$ は F が体だから整域である 2.4.5 が，体ではない．
(3) $(X-a, Y-b)$ は $F[X,Y]$ の極大イデアルになる：$\overline{\mathrm{ev}_{a,b}} : F[X,Y]/(X-a,Y-b) \xrightarrow{\sim} F$.

□

注 2.5.5 (体上有限生成環の理論)**.** 体上有限生成環とは，$k[X^1,\cdots,X^n]$ の剰余環として得られる環のことであり，代数幾何学における affine 代数多様体の理論[†11]や，Noether 環のイデアル論の雛形として重要であった．Hilbert の零点定理とは，このような体上有限生成環 A の素イデアルは，これを含む極大イデアルの共通部分として書けることを主張する．n 変数多項式について，$(X_1-a_1, X_2-a_2, \cdots, X_n-a_n)$ という形のイデアルは極大になり，F が代数閉体のとき，この形のものに尽きる．したがって，F^n の元 (affine 平面) と $F[X_1,\cdots,X_n]$ の極大イデアルとが対応する．素イデアルも考えるのは scheme 論.

2.5.2　素イデアル・極大イデアルの対応

イデアルが素であるまたは極大であるという性質は，射 $\pi : A \to A/I$ について関手的である．これは妙である．また，素イデアルの逆像は素イデアルである．

命題 2.5.6 (逆像関手は素イデアルを保つ). $f : A \to B$ を環準同型とする．B の素イデアル $\mathfrak{p}$ に対し，$f^{-1}(\mathfrak{p})$ は A の素イデアルである．

[証明]. f が定める単射 $\bar{f} : A/f^{-1}(q) \hookrightarrow B/q$ について，B/q が整域だから $A/f^{-1}(q)$ も整域となる（包含写像としての単射 2.3.14）．■

注 2.5.7. 整域の部分環は整域だが，一方で体の部分環は体とは限らない（その部分環が，全ての逆元も含んでいるとは限らない）．したがって，同様の命題は極大イデアルについては成り立たない．$f : \mathbb{Z} \hookrightarrow \mathbb{Q}$ の $f^{-1}(0) = 0$ が反例となる．

例 2.5.8 (characteristic)**.** 体の素イデアルは 0 だけだから，体 F への，ただ一つの整数環からの射 $\phi_F : \mathbb{Z} \to F$ の核 $\mathrm{Ker}\,\phi_F$ は素イデアルになる．よって，$\exists_{n\in\mathbb{N}}\ \mathrm{Ker}\,\phi_F = n\mathbb{Z}$ で，$n = 0$ または n は素数である 2.2.13．この n を体 F の**標数**という．□

命題 2.5.9 (素イデアル・極大イデアルの対応). $\pi : A \twoheadrightarrow A/I$ を標準全射とする．π^*, π_* は素イデアル，極大イデアルを保つ．すなわち，

(1) A の素イデアルであって I を含むものと，A/I の素イデアルとは包含関係も含めて一対一に対応する．
(2) A の極大イデアルであって I を含むものと，A/I の極大イデアルとは包含関係も含めて一対一に対応する．

[証明]. $I \subset J \subset A$ について，第 3 同型定理 2.3.13 より $A/J \simeq (A/I)/(J/I)$ であるから，A/J が整域・体であることと $(A/I)/(J/I)$ が整域・体であることは同値．■

2.5.3　極大イデアルの存在と局所環

イデアルは可換環の部分集合系 $P(A)$ の中で帰納的順序集合を成している．その極大イデアルが一意的＝上に完備な束を成しているとき，これを局所環という．代数幾何学的立場からは，空間内の 1 点の局所的な振る舞いを記述すると考えられる．函数芽の環は可換局所環で，極大イデアルは $f(0) = 0$ を満たす関数の全体と考えられる．[α]

[α] https://ja.wikipedia.org/wiki/局所環

命題 2.5.10 (AC). 可換環 A が零でないならば，極大イデアルは存在する．特に，素イデアルは存在する．[†12]

[†11] これは一般の代数多様体の局所理論にあたる．
[†12] 体論への帰着が使える．

[証明].

$$S := \{I \subsetneq A \mid I \text{ は } A \text{ のイデアル}\}$$

とすると，S は包含順序について帰納的である．実際，任意の全順序部分集合 $\Lambda \subset S$ を取ると，$\Lambda = \varnothing$ ならば $0 \in S$ は上界になる（A が零環でないことより）．$\Lambda \neq \varnothing$ の場合は，$I_\Lambda := \cup_{I\in\Lambda} I \in S$ が上界になることを示す．

(1) 任意の $x, y \in I_\Lambda$ を取ると，$I, I' \in \Lambda$ が存在して，$x \in I, y \in I'$．すると Λ は全順序だから $I \subset I'$ または $I' \subset I$ で，I, I' の大きい方を I'' とすると，$x, y \in I''$ が成り立つ．よって，$x + y \in I'' \subset I_\Lambda$.
(2) $\forall_{a\in A}\ \forall_{x\in I_\Lambda}\ ax \in I_\Lambda$ は $a = 0$ の場合も含めて明らかに成り立つ．
(3) $1 \notin I_\Lambda$ より，$I_\Lambda \neq A$ より，確かに $I_\Lambda \in S$.

よって，Zorn の補題から，S は極大元 $\mathfrak{m}$ を持つが，S の極大元とは，A の極大イデアルに他ならない．■

要諦 2.5.11. Zorn の補題の要件である帰納的順序集合とは，「任意の全順序部分集合は上界を持つ」であるが，これは空でないことも含意している．また，重要な証明抽出として，イデアルの任意合併はイデアルである．任意共通部分も同じだろうか？ネーター環の議論もそうであるが，環論が基礎論に近づいていくのは面白い．イデアルがここまで基本的な対象であることが不思議である．

系 2.5.12 . 任意の可換環のイデアル $I \subsetneq A$ に対して，A の極大イデアルであって I を含むものが存在する．

[証明]. 商環 A/I に関する極大イデアルの存在 2.5.10 と極大イデアルの対応 2.5.9 より．■

要諦 2.5.13. 極大イデアルは一般に複数存在し，イデアル $I \subsetneq A$ を指定するたびに，いくつかが対応する描像が浮かび上がる．例えば $\mathbb{Z}$ の構造 2.5.4.

定義 2.5.14 (local ring (38 年)). 可換環 A の極大イデアルが一意的であるとき，これを**局所環**という．

例 2.5.15.

(1) 体は一意な極大イデアル 0 を持つので，局所環である．
(2) $n \geqslant 1$ について，$\mathbb{Z}/n\mathbb{Z}$ が局所環であることと，n を割り切る素数がただ一つであることは同値．実際，$\mathbb{Z}$ の極大イデアルは素数 p を用いて $p\mathbb{Z}$ と表せるものに限られる 2.5.4 から，極大イデアルの対応 2.5.9 より．

□

命題 2.5.16 (局所環の特徴付け). 可換環 A について，次の 2 条件は同値．

(1) A は局所環である．
(2) $\mathfrak{m} := A\backslash A^\times$ は A のイデアルである．

また，この同値な条件が成り立つとき，$\mathfrak{m}$ は A のただ一つの極大イデアルとなる．

[証明].

(1)⇒(2)　A は局所環だから，極大イデアル $\mathfrak{m}_A$ が一意的に存在する．$\mathfrak{m} = \mathfrak{m}_A$ と示す．
- (1)　$\mathfrak{m}_A \subset \mathfrak{m}$ を示す．$a \in \mathfrak{m}_A$ のとき，$a \notin A^\times$ である．$a \in A^\times$ ならば，$a^{-1} \in A$ について，$a^{-1}a = 1 \in \mathfrak{m}_A$ がしたがって $\mathfrak{m}_A \neq A$ に矛盾．よって，$a \in \mathfrak{m}_A \Rightarrow a \in \mathfrak{m}$.
- (2)　$\mathfrak{m}_A \supset \mathfrak{m}$ を示す．$a \in A\backslash A^\times$ ならば，$1 \notin (a)$ より，$(a) \subsetneq A$．よって，(a) を含む極大イデアルが存在することが必要である 2.5.12 が，これが $\mathfrak{m}_A$ である必要があるから，$(a) \subset \mathfrak{m}_A \subsetneq A$．よって特に，$a \in \mathfrak{m}_A$.

(2)⇒(1)　$\mathfrak{m} := A\backslash A^\times$ が A のイデアルになるとする．$A = 0$ ならば $A\backslash A^\times = \varnothing$ はイデアルではないから，$A \neq 0$．よって，極大イデアル $\mathfrak{m}' \subsetneq A$ が存在する 2.5.10．極大イデアルについては $\mathfrak{m}' \subset A\backslash A^\times = \mathfrak{m}$ が成り立つ．しかし，$\mathfrak{m} \neq A$ で，$\mathfrak{m}'$ は極大イデアルであるから，これは $\mathfrak{m} = \mathfrak{m}'$ を意味する．よって，A の極大イデアルは一意的であるから，A は局所環である．

■

要諦 2.5.17. 一般に極大イデアルがただ一つしか存在しない場合は，その表示は $\mathfrak{m} := A\backslash A^\times$ となり，この構成がイデアルを作る場合は必ず一意的な極大イデアルとなる．また，次の 2 条件とも同値．

(1) R と異なるイデアルは $\mathfrak{m}$ に含まれる．
(2) $\mathfrak{m}$ の任意の元 x に対し，$1+x$ は単元である．

2.6　局所化と商体

環に分母を付けて元を増やし，特に単元を増やす操作を考える．$s \in S$ について，$\iota(s) = \frac{s}{1}$ となるから，これに対して $\frac{1}{s}$ という逆元が見つかる．非可逆元を積閉集合 S に入れるのが良い．環を一番大きくする構成が商体の構成であり，$\mathbb{Z} \hookrightarrow \mathbb{Q}$ にあたる．

2.6.1　局所化の定義と普遍性

局所環とは $A \backslash A^\times$ が極大イデアルを与えるような環である．環に分母を附ける操作を一般化する．素イデアルが点で，その間の準同型が関数であり，局所化は近傍を表す．局所化の普遍性は，目標の積閉集合 S を単元に埋め込むようなもののうち，最小のもの（始対象）である．

定義 2.6.1 (multiplicative subset). 可換環の部分集合 $S \subset A$ が**積閉集合**であるとは，次の 2 条件を満たすことをいう：

(1) $1 \in S$.
(2) $\forall_{s,t \in S}\ st \in S$.

例 2.6.2.

(1) A の素イデアル $\mathfrak{p}$ に対して，$A \backslash \mathfrak{p}$ は積閉集合である．実際，素イデアルの公理の同値変形となっている．
  (a) $\mathfrak{p} \neq A \iff 1 \in A \backslash \mathfrak{p}$.
  (b) $\forall_{a,b \in \mathfrak{p}}\ ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p} \vee b \in \mathfrak{p} \iff a \notin \mathfrak{p} \wedge b \notin \mathfrak{p} \Rightarrow ab \notin \mathfrak{p}$.
(2) $f \in A$ に対し，$\{f^n \in A \mid n \in \mathbb{N}\}$ は積閉集合となる．

□

定義 2.6.3 (localization). 可換環 A とその積閉集合 $S \subsetneq A$ について，

(1) 関係 $(a,s) \sim (a',s') :\Leftrightarrow \exists_{t \in S}\ t(as' - a's) = 0$ は $A \times S$ 上に同値関係を定める．[†13]
(2) 商集合を $S^{-1}A := A \times S/\sim$ と表し，その元を $\frac{a}{s} := [(a,s)]$ と表す．すると，次の演算について，$S^{-1}A$ は再び可換環となる：
$$\frac{a}{s} + \frac{a'}{s'} = \frac{as' + a's}{ss'}, \quad \frac{a}{s} \cdot \frac{a'}{s'} = \frac{aa'}{ss'}.$$
(3) A のイデアル I に対し，$S^{-1}I$ は $S^{-1}A$ のイデアルである．

[証明].

(1) (a) $t(as - as) = 0$ より $(a,s) \sim (a,s)$.
  (b) $(a,s) \sim (a',s') \Rightarrow (a',s') \sim (a,s)$.
  (c) $(a,s) \sim (a',s'), (a',s') \sim (a'',s'')$ とする．すなわち，$\exists_{t,t' \in S}\ t(as' - a's) = t'(a's'' - a''s') = 0$. すなわち，$tas' = ta's, t'a's'' = t'a''s'$. 第二式の両辺に ts を乗じて，$t'' := tt's$ とおくと，A が可換であることに注意して，
$$tst'a's'' = tst'a''s' \iff (ta's)t's'' = (tt's')a''s \iff tas't's'' = t''as'' = t''a''s.$$
(2) 加法は結合的で，$\frac{0}{1}$ を単位元とし，$\frac{a}{s}$ の逆元は $\frac{-a}{s}$ である．積も結合的で可換で，$\frac{1}{1}$ を単位元とする．最後に分配法則も成り立つ．

[†13] A が整域であり，$0 \notin S$ ならば，この関係は $as' = a's$ と同値．また，$0 \in S$ の時は潰れた同値関係 $A \times S$ を定める．

■

要諦 2.6.4. 分数とは「比が同じ」という同値類である．しかし，その関係は S が正則元のみからなるとは限らない場合は非自明で，$\dfrac{a}{s} = \dfrac{a'}{s'} \Leftrightarrow \exists_{t\in S}\ tas' = ta's$ となる．

注 2.6.5. $0 \in S \Leftrightarrow S^{-1}A = \{0\}$.

命題 2.6.6 (局所化の普遍性).

(1) 写像 $\iota : A \to S^{-1}A; a \mapsto \dfrac{a}{1}$ は環準同型である．また，S が A の正則元のみからなるとき，そしてその時に限り，単射である．特に，A が整域であり，$0 \notin S$ であるとき，単射である．

(2) 任意の環準同型 $f : A \to B$ に対して，$f(S) \subset B^\times$ ならば，環準同型 $g : S^{-1}A \to B$ であって次を可換にするものが一意的に存在する：

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle\iota}\downarrow & \nearrow_{g} & \\ S^{-1}A & & \end{array}$$

また，このときの $g : S^{-1}A \to B$ とは，$g\left(\dfrac{a}{s}\right) = f(s)^{-1}f(a)$ で定まる写像である．

[証明].

(1) $S^{-1}A$ の加法・乗法の定め方より，ι は演算を明らかに保ち，環準同型となる．$\iota(a) = 0$ とは $\dfrac{a}{1} = 0$ すなわち $\exists_{s\in S}\ as = 0$ ということであるから，S が A の正則元のみからなるときこれは $a = 0$ を意味し，ι は単射である．

(2) 写像 $g : S^{-1}A \to B$ を $\dfrac{a}{s} \mapsto f(s)^{-1}f(a)$ と定めると，これは写像として well-defined であり，環の準同型であり，図式を可換にし，一意的であることを示す．

well-definedness　任意の $a, a' \in A, s, s' \in S$ について，$\dfrac{a}{s} = \dfrac{a'}{s'}$ を満たすと仮定し，$f(s)^{-1}f(a) = f(s')^{-1}f(a')$ を導く．仮定より，$\exists_{t\in S}\ tas' = ta's$．したがって，$f(t)f(a)f(s') = f(t)f(a')f(s)$ であるが，仮定の $f(s), f(s'), f(t) \in \operatorname{Im} f \subset B^\times$ より，$f(s)^{-1}f(a') = f(s')^{-1}f(a)$ が従う．

準同型　環準同型の 3 公理は次のように示される：

$$\begin{aligned} g\left(\frac{a}{s} + \frac{a'}{s'}\right) = g\left(\frac{as' + a's}{ss'}\right) &= f(ss')^{-1}f(as' + a's) \\ &= f(s)^{-1}f(a) + f(s')^{-1}f(a') = g\left(\frac{a}{s}\right) + g\left(\frac{a'}{s'}\right) \\ g\left(\frac{a}{s} \cdot \frac{a'}{s'}\right) = g\left(\frac{aa'}{ss'}\right) = f(ss')^{-1}f(aa') &= g\left(\frac{a}{s}\right) \cdot g\left(\frac{a'}{s'}\right) \\ g\left(\frac{1}{1}\right) = f(1)^{-1}f(1) &= 1. \end{aligned}$$

図式の可換性　$g(\iota(a)) = g\left(\dfrac{a}{1}\right) = f(1)^{-1}f(a) = f(a)$ より．

一意性　$g' : S^{-1}A \to B$ も $g' \circ \iota = f$ を満たすとして，$g' = g$ を導く．任意の $a \in A, s \in S$ に対して，$sa = sa \cdot 1$ より，$\dfrac{s}{1} \cdot \dfrac{a}{s} = \dfrac{sa}{s} = \dfrac{a}{1}$ が成り立つから，

$$\begin{aligned} g'\left(\frac{s}{1}\right) g'\left(\frac{a}{s}\right) = g'\left(\frac{a}{1}\right) &= g'(\iota(a)) = f(a), \\ g'\left(\frac{s}{1}\right) &= g'(\iota(s)) = f(s), \end{aligned}$$

より，$f(s)g'\left(\dfrac{a}{s}\right) = f(a)$ であるから，$g'\left(\dfrac{a}{s}\right) = f(s)^{-1}f(a) = g\left(\dfrac{a}{s}\right)$ が従う．よって，$g = g'$.

■

要諦 2.6.7. 局所化も大きな空間を作ってから割っているので，テンソル積の普遍性と似ている．

2.6.2　局所化の性質と普遍性の利用

局所化の構成 $\iota : A \to S^{-1}A$ とは，積閉集合を $S^{-1}A$ の単元に「埋め込む」．積閉集合 S は，$S^{-1}A$ で可逆になる：$\iota(S) \subset (S^{-1}A)^\times$．$\iota(s) = \frac{s}{1}$ の逆元は $\frac{1}{s}$ である．一般に $\frac{1}{s} \in \iota(S)$ ではない．[a] S が A の正則元のみからなるとき，単射になる．$A = \mathbb{Z}, S = \mathbb{Z}\backslash\{0\}$ とした場合が $\mathbb{Z} \hookrightarrow \mathbb{Q} = \mathrm{Frac}\,\mathbb{Z}$ の構成に当たる．

[a] $1/2$ などは整数としては表せないということ．

命題 2.6.8 (局所化の局所化). $S, S' \subset A$ を積閉集合で，$S \subset S'$ を満たすものとする．$\iota : A \to S^{-1}A$ による S' の像も S' と表すと，$S'^{-1}A \simeq S'^{-1}(S^{-1}A)$ が成り立つ．

$$\begin{array}{ccc} A & & \\ {\scriptstyle\iota}\downarrow & \overset{\sim}{\searrow} & \\ S^{-1}A & \xrightarrow[\iota']{} & S'^{-1}(S^{-1}A) \end{array}$$

[証明].

互いに逆な射の構成　合成 $\iota' \circ \iota : A \to S'^{-1}(S^{-1}(A))$ による S' の像は $(S'^{-1}(S^{-1}A))^\times$ に含まれるので，局所化の普遍性 2.6.6 より，準同型

$$\begin{array}{ccc} f : S'^{-1}A & \longrightarrow & S'^{-1}(S^{-1}A) \\ \cup & & \cup \\ \frac{a}{s'} & \longmapsto & \iota'(\iota(s))^{-1}\iota'(\iota(a)) = \frac{a/1}{s'/1} \end{array}$$

が引き起こされる．また，仮定 $S \subset S'$ より，$\iota'' : A \to S'^{-1}A$ による S の像も $(S'^{-1}A)^\times$ に含まれるから，局所化の普遍性 2.6.6 より，

$$\begin{array}{ccc} g : S^{-1}A & \longrightarrow & S'^{-1}A \\ \cup & & \cup \\ \frac{a}{s} & \longmapsto & \iota''(s)^{-1}\iota''(a) = \frac{a}{s} \end{array}$$

が引き起こされ，さらに g による S' の像も，$\iota''(S')$ に等しいから $(S'^{-1}A)^\times$ に含まれ，局所化の普遍性 2.6.6 より，

$$\begin{array}{ccc} h : S'^{-1}(S^{-1}A) & \longrightarrow & S'^{-1}A \\ \cup & & \cup \\ \frac{a/s}{s'/1} & \longmapsto & g\left(\frac{s'}{1}\right)^{-1} g\left(\frac{a}{s}\right) = \frac{a}{ss'} \end{array}$$

が引き起こされる．

互いに逆であることの証明　$h \circ f = \mathrm{id}_{S'^{-1}A}, f \circ h = \mathrm{id}_{S'^{-1}(S^{-1}A)}$ が成り立つ．

■

要諦 2.6.9. これは $S \hookrightarrow S'$ のとき $S'^{-1}A \hookrightarrow S^{-1}A$ という描像ではないのか？それで準同型定理を使ったらどうなる？

命題 2.6.10 (局所化と剰余環の関係). $S \subset A$ を積閉集合，$I \subset A$ をイデアルとする．$\pi : A \twoheadrightarrow A/I$ による S の像も S と表すと，$S^{-1}A/S^{-1}I \simeq S^{-1}(A/I)$ が成り立つ．

$$\begin{array}{ccc} A & \xrightarrow{\pi} & A/I \\ {\scriptstyle\iota}\downarrow & & \downarrow{\scriptstyle\iota'} \\ S^{-1}A & \xrightarrow{\pi'} & S^{-1}A/S^{-1}I \simeq S^{-1}(A/I) \end{array}$$

[証明]. 合成 $\iota' \circ \pi : A \to S^{-1}(A/I)$ について，$\iota' \circ \pi(S) \subset (S^{-1}(A/I))^\times$ より（記号の混用に注意），局所化の普遍性 2.6.6 から

$$\begin{array}{ccc} \pi'' : S^{-1}A & \longrightarrow & S^{-1}(A/I) \\ \cup & & \cup \\ \dfrac{a}{s} & \longmapsto & \dfrac{\pi(a)}{\pi(s)} (= \iota'\pi(s)^{-1}\iota'\pi(a)) \end{array}$$

が引き起こされる．$\pi : A \twoheadrightarrow A/I$ が全射だから，$\pi'' : S^{-1}A \to S^{-1}(A/I)$ も全射に定まっている[†14]．$S^{-1}I = \operatorname{Ker} \pi''$ を示す．

(1) $S^{-1}I \subset \operatorname{Ker} \pi''$：任意の $\dfrac{a}{s} \in S^{-1}I$ について，$\pi''\left(\dfrac{a}{s}\right) = \dfrac{\pi(a)}{\pi(s)} = \dfrac{0}{\pi(s)} = 0$.

(2) $S^{-1}I \supset \operatorname{Ker} \pi''$：$\dfrac{a}{s} \in \operatorname{Ker} \pi''$ とする．$\dfrac{\pi(a)}{\pi(s)} = 0$ より，$\exists_{t \in S}\ \pi(t)\pi(a) = \pi(ta) = 0$．すなわち，$ta \in \operatorname{Ker} \pi = I$．よって，$\dfrac{a}{s} = \dfrac{ta}{ts} \in S^{-1}I$ が従う．

よって準同型定理より，$\overline{\pi''} : S^{-1}A/S^{-1}I \xrightarrow{\sim} S^{-1}(A/I)$ を得る． ■

要諦 2.6.11. 剰余環を取る操作と局所化を取る操作は，同型を除いて可換であるという関手的消息．具体例は，$S = \{f^n \in A \mid n \in \mathbb{N}, f \in A\}$ の場合がわかりやすい．f の冪を分母に持つ数同士の分数は，f の冪を括り出せる．

2.6.3　局所化に於けるイデアルの対応

- A の素イデアルであって S と交わらないもの
- $S^{-1}A$ の素イデアル

が，包含関係を保って対応する．まさに「割り算」に対する「素数」のような振る舞い $\dfrac{a}{s} \in S^{-1}\mathfrak{p} \Leftrightarrow a \in \mathfrak{p}$ をする（$S \cap \mathfrak{p} = \varnothing$ のとき，分母を払える）．

補題 2.6.12 (イデアルの表現). $\iota : A \to S^{-1}A$ を局所化とする．

(1) A のイデアル I に対し，対応する $S^{-1}A$ のイデアルは $S^{-1}I = \iota(I)S^{-1}A$（$\iota(I)$ で生成されるイデアル 2.4.1）と表せる．

(2) $S^{-1}A$ のイデアル J に対し，$J = S^{-1}(\iota^{-1}(J))$ が成り立つ．この意味で「対応」する．

[証明].

(1) $S^{-1}I \subset \iota(I)S^{-1}A$　$S^{-1}I$ の任意の元は，任意の $x \in I, s \in S$ を用いて $\dfrac{x}{s} \in S^{-1}I$ と表せる．$\dfrac{x}{s} = \iota(x) \cdot \dfrac{1}{s} \in \iota(S) \cdot S^{-1}A$.
$S^{-1}I \supset \iota(I)S^{-1}A$　任意の $x \in I, a \in A, s \in S$ に対して，$\iota(x) \cdot \dfrac{a}{s} = \dfrac{ax}{s} \in S^{-1}I$.

(2) $S^{-1}(\iota^{-1}(J)) \subset J$　$a \in \iota^{-1}(J), s \in S$ に対して，$\dfrac{a}{s} = \dfrac{1}{s}\iota(a) \in J$.
$S^{-1}(\iota^{-1}(J)) \supset J$　任意の $\dfrac{a}{s} \in J$ に対して，$\iota(a) = \dfrac{a}{1} = \dfrac{s}{1} \cdot \dfrac{a}{s} \in J$ より $a \in \iota^{-1}(J)$ だから，$\dfrac{a}{s} \in S^{-1}(\iota^{-1}(J))$.

■

注 2.6.13. (2) の逆の主張 $I = \iota^{-1}(S^{-1}(I))$ が任意の A のイデアル I について成り立つとは限らない．が，これが失敗する場合は，$S \cap \mathfrak{p} \neq \varnothing$ であるために，$S^{-1}\mathfrak{p}$ が $1 \in S^{-1}\mathfrak{p}$ となって $S^{-1}A$ 全体に拡散してしまう場合に限る．

要諦 2.6.14. $S^{-1}I = \iota(I)S^{-1}A$ は，分母の I を $I = IA$ と表せるのを利用しているように思える．

命題 2.6.15 (素イデアルの対応).

(1) A の素イデアル $\mathfrak{p}$ が $S \cap \mathfrak{p} = \varnothing$ を満たすならば，$S^{-1}\mathfrak{p}$ は $S^{-1}A$ の素イデアルである．

(2) $\mathfrak{q}$ を $S^{-1}A$ の素イデアルとするとき，$\iota^{-1}(\mathfrak{q})$ は A の素イデアルであり，$S \cap \iota^{-1}(\mathfrak{q}) = \varnothing$ が成り立つ．

(3) すなわち，A の素イデアルであって S と交わらないものと $S^{-1}A$ の素イデアルが，包含関係を保って対応する．

[†14] ι' はどうやっても単射なので，図式を可換にするに当たっては全射ではないが，準同型自体は全射に定まっているという状況……！？

[証明].

(1) (a) 補題より，$\frac{1}{1} \notin S^{-1}\mathfrak{p} \iff 1 \notin \mathfrak{p}$ なので，$S^{-1}\mathfrak{p} \neq S^{-1}A$ が成り立つ．

(b) 任意の $a, a' \in A, s, s' \in S$ について，$\frac{aa'}{ss'} \in S^{-1}\mathfrak{p} \iff aa' \in \mathfrak{p}$ が成り立つと仮定する．$\mathfrak{p}$ は素イデアルだから，$a \in \mathfrak{p} \vee a' \in \mathfrak{p}$．したがって再び補題より，$\frac{a}{s} \in S^{-1}\mathfrak{p} \vee \frac{a'}{s'} \in S^{-1}\mathfrak{p}$.

(2) $\iota^{-1}(\mathfrak{q})$ は素イデアルである 2.5.6．$s \in S \cap \iota^{-1}(\mathfrak{q})$ が取れると仮定して矛盾を導く．$\frac{s}{1} = \iota(s) \in \mathfrak{q}$ より，$1 = \frac{1}{s} \cdot \frac{s}{1} \in \mathfrak{q}$ が従い，$\mathfrak{q}$ が素イデアルであることに矛盾．

(3) $S^{-1}(\iota^{-1}(\mathfrak{q})) = \mathfrak{q}$ は前の補題に含意される．$\iota^{-1}(S^{-1}\mathfrak{p}) = \mathfrak{p}$ は，$S \cap \mathfrak{p} = \varnothing$ のとき，補題より，$a \in \iota^{-1}(S^{-1}\mathfrak{p}) \Leftrightarrow \frac{a}{1} \in S^{-1}\mathfrak{p} \Leftrightarrow a \in \mathfrak{p}$ より従う．$\mathfrak{p} \mapsto S^{-1}\mathfrak{p}, \mathfrak{q} \mapsto \iota^{-1}(\mathfrak{q})$ は明らかに包含関係を保つ．

■

補題 2.6.16．A の素イデアル $\mathfrak{p}$ が $S \cap \mathfrak{p} = \varnothing$ を満たすとき，$\forall_{a \in A}\, \forall_{s \in S}\, \frac{a}{s} \in S^{-1}\mathfrak{p} \iff a \in \mathfrak{p}$.

[証明]. $\Rightarrow$ を示せば良い．$\frac{a}{s} \in S^{-1}\mathfrak{p}$ のとき，$\frac{a}{s} = \frac{a'}{s'}$ を満たす $a' \in \mathfrak{p}, s' \in S$ が存在するから，$\exists_{t \in S}\, t(as' - a's) = 0$．このとき，$tas' = ta's \in \mathfrak{p}$ である．S は積閉集合であるから $ts' \in S$ であり，$S \cap \mathfrak{p} = \varnothing$ の仮定より $ts' \notin \mathfrak{p}$ を得る．よって，$\mathfrak{p}$ は素イデアルだから $a \in \mathfrak{p}$ が従う．■

要諦 2.6.17. おそらく，$S \cap \mathfrak{p} = \varnothing$ ならば，分子に $\mathfrak{p}$ 以外の元がこないこと，$\frac{\mathfrak{p}}{\mathfrak{p}} = \frac{1}{1}$ のようなことが起こらないことを言っている．

2.6.4　商体・局所環

局所環の例に商体がある．整域の局所化において，商体はある種の終対象である（一番大きい）．そこで，単射 $A \hookrightarrow \operatorname{Frac} A$ を用いて，A の元を $\operatorname{Frac} A$ の中に埋め込んで $\operatorname{Frac} A$ での式として考える手法が多々用いられる．一意分解整域において単項分数イデアルを考えること 2.8.20 など．

定義 2.6.18 (field of fractions / field of quotients). A を可換環とする．

(1) A が整域であるとき，A の $A\backslash\{0\}$ による局所化は体になる．これを A の**商体**とよび，$\operatorname{Frac} A$ と表す．

(2) $\mathfrak{p}$ を A の素イデアルとするとき，A の $A\backslash\mathfrak{p}$ による局所化 $A_{\mathfrak{p}}$ は局所環であり，その極大イデアルは $\mathfrak{p}A\mathfrak{p}$ である．また，$A_{\mathfrak{p}}/\mathfrak{p}A\mathfrak{p} \simeq \operatorname{Frac} A/\mathfrak{p}$ が成り立つ．$A_{\mathfrak{p}}$ を A **の** $\mathfrak{p}$ **に於ける局所化**と呼ぶ．

[証明].

(1) $S := A\backslash\{0\}$ と交わらないようなイデアルは 0 のみであり，A が整域であるという仮定から 0 は素イデアルである 2.4.4．よって，素イデアルの対応 2.6.15 より，$0 = S^{-1}0$ は $S^{-1}A$ の唯一の素イデアルである．特に 0 は $S^{-1}A$ の極大イデアルである必要があるから，$S^{-1}A$ は体である．

(2) $S := A\backslash\mathfrak{p}$ とする．

(a) S に含まれない素イデアルのうち最大であるものが $\mathfrak{p}$ だから，$S^{-1}\mathfrak{p} = \mathfrak{p}A_{\mathfrak{p}}$（イデアルの表示 2.6.12）[†15]は $A_{\mathfrak{p}}$ の素イデアルであり，$A_{\mathfrak{p}}$ の任意の素イデアルは $\mathfrak{p}A_{\mathfrak{p}}$ に含まれる．（$A_{\mathfrak{p}}$ は素イデアル $\mathfrak{p}A_{\mathfrak{p}}$ を持つので零でないから）極大イデアル $\mathfrak{m}$ を任意に取ると，$\mathfrak{m}$ も素イデアルであり，$\mathfrak{m} \subset \mathfrak{p}A_{\mathfrak{p}}$ が従う．よって，$\mathfrak{m} = \mathfrak{p}A_{\mathfrak{p}}$ が従い，$\mathfrak{p}A_{\mathfrak{p}}$ は $A_{\mathfrak{p}}$ の唯一の極大イデアルである．

(b) イデアルの表現 2.6.12 と局所化と剰余環の関係 2.6.10 より，$A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} = S^{-1}A/S^{-1}\mathfrak{p} \simeq S^{-1}(A/\mathfrak{p})$．$\pi : A \twoheadrightarrow A/\mathfrak{p}$ による $S = A\backslash\mathfrak{p}$ の像は $\pi(S) = (A/\mathfrak{p})\backslash\{0\}$ であるから，$S^{-1}(A/\mathfrak{p}) = \operatorname{Frac} A/\mathfrak{p}$ である．

■

例 2.6.19 (商体の例).

[†15] 任意の $\mathfrak{p}$ の元は $\mathfrak{p}A$ とかけることから，$S^{-1}\mathfrak{p} = \mathfrak{p}A_{\mathfrak{p}} = \mathfrak{p}S^{-1}A$

(1) $\mathbb{Z}$ の商体が $\mathbb{Q} = \operatorname{Frac}\mathbb{Z}$ である．
(2) F 係数多項式環 $F[X_1, \cdots, X_r]$ $(r \geqslant 1)$ は整域であり，この商体を**有理関数体**という：$\operatorname{Frac} K[X] = K(X)$.
(3) 形式冪級数環 $K[[X]]$ も整域であり，この商体を**形式 Laurent 級数体** $K((X))$ と表す．

□

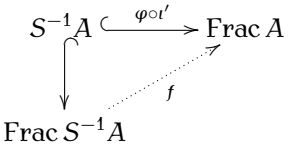
命題 2.6.20 (整域の局所化に於ける商体の立ち位置). A を整域，S をその積閉集合とする．$0 \notin S$ ならば $S^{-1}A$ も整域であり，単射準同型 $S^{-1}A \hookrightarrow \operatorname{Frac} A$ が存在する．さらに，$\operatorname{Frac} S^{-1}A \simeq \operatorname{Frac} A$ が成り立つ．

[証明].

$S^{-1}A$ も整域　A は整域であるから，0 は A の素イデアルであり 2.4.4，仮定 $0 \notin S$ より $0 \cap S = \varnothing$．よって素イデアルの対応 2.6.15 により，$0 = S^{-1}0$ は $S^{-1}A$ の素イデアルである．よって，$S^{-1}A$ は整域．

単射の存在　$S' := A\backslash\{0\}$ とおくと，$\operatorname{Frac} A = S'^{-1}A$ 及び $S \subset S'$ が成り立つから，命題 2.6.8 より，$\varphi : S'^{-1}(S^{-1}A) \xrightarrow{\sim} S'^{-1}A = \operatorname{Frac} A$ が存在する．一方，$\iota : A \hookrightarrow S^{-1}A$ は単射で $0 \notin S'$ だから，S' の $S^{-1}A$ における像 $\iota(S')$ も 0 を含まず，したがって $\iota' : S^{-1}A \hookrightarrow S'^{-1}(S^{-1}A)$ も単射である（局所化の普遍性 2.6.6）．よって，$\varphi \circ \iota' : S'A \hookrightarrow \operatorname{Frac} A; \dfrac{a}{s} \mapsto \dfrac{a}{s}$ は単射．

局所化の商体と同型　$S'' := (S^{-1}A)\backslash\{0\}$ とおくと，$\operatorname{Frac} S^{-1}A = S''^{-1}(S^{-1}A)$ と表せる．単射 $\varphi \circ \iota' : S^{-1}A \hookrightarrow \operatorname{Frac} A$ による S'' の像は $(\operatorname{Frac} A)^\times = \operatorname{Frac}\backslash\{0\}$ に含まれるから，局所化の普遍性 2.6.6 より，環準同型 $f : \operatorname{Frac} S^{-1}A \to \operatorname{Frac} A$ が引き起こされる．



任意の $\dfrac{a}{b} \in \operatorname{Frac} A$ $(a \in A, b \in A\backslash\{0\})$ に対して，$\dfrac{b}{1} \in S'' = (S^{-1}A)\backslash\{0\}$ であるから，$\dfrac{a/1}{b/1} \in f^{-1}\left(\dfrac{a}{b}\right)$ が見つかり，f は全射．また，$\operatorname{Frac} S^{-1}A$ は体であり，$\operatorname{Frac} A$ は零でないから，f は単射 2.4.12.

■

2.6.5　冪零根基

幂零根基は，全ての素イデアルの共通部分である．すごい，極めて非自明だ．

補題 2.6.21 (冪零根基の元の特徴付け). $f \in A$ に対し，A の積閉集合 $\{f^n \in A \mid n \in \mathbb{N}\}$ による局所化を A_f と表す．このとき，$f \in \sqrt{0} \iff A_f = 0$.

[証明].

$$A_f = 0 \iff \frac{1}{1} = \frac{0}{1} \overset{def}{\iff} \exists_{n\in\mathbb{N}}\, f^n \cdot 1 = f^n = 0.$$

というより，$0 \in S \Leftrightarrow S^{-1}A = 0$ より．■

系 2.6.22 (冪零根基の表現). A を可換環とするとき，$\displaystyle\bigcap_{\mathfrak{p}:A \text{ の素イデアル}} \mathfrak{p} = \sqrt{0}$.

[証明].

$\cap\mathfrak{p} \supset \sqrt{0}$　任意の A の素イデアル $\mathfrak{p}$ について $\mathfrak{p} \supset \sqrt{0}$ が成り立つことを示せば良い．任意に $a \in \sqrt{0}$ を取ると，$\exists_{n\in\mathbb{N}}\, a^n = 0 \in \mathfrak{p}$ であるから，$a \in \mathfrak{p}$ が従う．

$\cap\mathfrak{p} \subset \sqrt{0}$　$f \in \displaystyle\bigcap_{\mathfrak{p}:A \text{ の素イデアル}} \mathfrak{p}$ を任意に取る．すると，A の素イデアルは必ず f を含むから，A_f は素イデアルを持たない（素イデアルの対応 2.6.15）．よって，素イデアルの存在 2.5.10 の対偶より，$A_f = 0 \iff f \in \sqrt{0}$.

■

2.7　単項イデアル整域

体 ↪ (ユークリッド整域) ↪ 単項イデアル整域 ↪ 一意分解整域 ↪ 整域 ↪ 可換環

$\mathbb{Z}, F[X]$ は Euclid 整域である．一意分解整域係数の多項式環は一意分解整域であるが，単項イデアル整域係数の多項式は単項イデアル整域とは限らない．体係数多項式環は単項イデアル整域である．体係数の多変数多項式環は一意分解整域である．

2.7.1　定義と例

定義 2.7.1 (PID: principal ideal domain). 整域 A について，A の任意のイデアルが単項イデアルであるとき，A を**単項イデアル整域**という．

定義 2.7.2 (degree function, Euclidean ideal).

(1) 整域 A について，写像 $H : A\backslash\{0\} \to \mathbb{N}$ が **Euclid 関数**であるとは，次が成り立つことをいう：$\forall_{a\in A}\ \forall_{b\in A\backslash\{0\}}\ \exists_{q,r\in A}\ a = qb + r \wedge (r = 0 \vee H(r) < H(b))$.
(2) Euclid 関数を少なくとも 1 つ持つような整域 A を **Euclid 整域**という．

例 2.7.3 (Euclid 整域)**.**

(1) $A = \mathbb{Z}$ に対し，$H : \mathbb{Z}\backslash\{0\} \to \mathbb{N}$ を $H(-) = |-|$ と定めると，これは Euclid 関数である．
(2) F を体とする．$A = F[X]$ に対し，$H : F[X]\backslash\{0\} \to \mathbb{N}$ を $H = \deg$ と定めると，これは Euclid 関数である（この主張を剰余定理という）．

□

命題 2.7.4 . Euclid 整域は単項イデアル整域である．

[証明]. Euclid 整域 A 上の Euclid 関数 $H : A\backslash\{0\} \to \mathbb{N}$ を任意に取る．$I \subset A$ を任意のイデアルとし，これが単項生成可能であることを示せば良い．

構成　$I = 0$ のときは $I = (0)$ であるから，$I \neq 0$ の場合を考える．$\{H(a) \in \mathbb{N} \mid a \in I\backslash\{0\}\}$ を最小にする $a_0 \in I\backslash\{0\}$ を 1 つ取ると，$I = (a_0)$ であることを示す．

証明　$a \in I$ を任意に取ると，$a = qa_0 + r$ かつ $r = 0 \vee H(r) < H(a_0)$ を満たす $q, r \in A$ が存在する．$r \neq 0$ ならば，$r = a - qa_0 \in I\backslash\{0\}$ より，a_0 の定め方より $H(a_0) \leqslant H(r)$ が必要だが，これは矛盾を起こすから $r = 0$ が必要．すなわち，$a = qa_0 \in (a_0)$ である．

■

要諦 2.7.5. 抽象化された剰余計算である．

2.7.2　素イデアルの消息

素イデアルは 2 階層になっていて，$\mathfrak{p} = 0$ であるか，極大イデアルであるかのいずれかである．さらに単項イデアル整域は一意分解整域でもあるから，素元と既約元は一致し，既約元が生成する単項イデアルは（既約元は零でないので）極大イデアルである．

命題 2.7.6 (PID の極大イデアルの特徴付け). A を体でない単項イデアル整域とする．次の 2 条件は同値．

(1) 素イデアル $\mathfrak{p}$ が極大である．

(2) $\mathfrak{p} \neq 0$.

[証明].

(1)⇒(2)　$A/0 = A$ は体ではないので，0 は極大イデアルではない．よって，$\mathfrak{p} \neq 0$.

(2)⇒(1)　$\mathfrak{p} \subsetneq I$ を満たす任意のイデアル I に対し，$A = I$ を導く．A は単項イデアル整域であるから，$\mathfrak{p} \neq 0$ であるとき，ある $a \in A\backslash\{0\}$ が存在して $\mathfrak{p} = (a)$ となり，$x \in A$ が存在して $I = (x)$ となる．仮定 $\mathfrak{p} \subset I$ は $\exists_{y \in A}\ a = xy$ を含意する．すると特に $xy \in (a) = \mathfrak{p}$ より，$x \in \mathfrak{p} \vee y \in \mathfrak{p}$ が従う．

$x \in \mathfrak{p}$ ならば $I = (x) \subset \mathfrak{p}$ となるから，仮定に反する．$y \in \mathfrak{p}$ のとき，$\exists_{z \in A}\ y = az$ であり，$a = xy$ と併せて $a = xaz \Leftrightarrow a(xz - 1) = 0$. A は整域で $a \neq 0$ としたから，$xz = 1 \in (x) = I$ が従う．よって，$I = A$.

■

2.7.3　局所化についての閉性

命題 2.7.7 . A を単項イデアル整域とし，S をその積閉集合とする．$0 \notin S$ ならば，$S^{-1}A$ は再び単項イデアル整域である．

[証明]. $0 \notin S$ のとき，整域の局所化は整域である 2.6.20 から，$S^{-1}A$ は整域である．J を $S^{-1}A$ の任意のイデアルとし，これが単項生成であることを示せば良い．単射 $\iota : A \hookrightarrow S^{-1}A$ について，$\iota^{-1}(J)$ も A のイデアル 2.3.8 であり，したがって単項生成である．イデアルの表現 2.6.12(1)(2) より，$J = \iota(\iota^{-1}(J)) \cdot S^{-1}A$ より，J も単項イデアルである．■

2.8　一意分解整域

単項イデアル性も大きな性質であったが，より中間的な性質である $\mathbb{Z}$ の素因数分解の一意性に迫る．これは単項イデアル整域よりも広いクラスとなる．

2.8.1　整域の元の性質

$\mathbb{Z}$ の単元は 2 つであること $\mathbb{Z}^\times = \{\pm 1\}$ を念頭におく．$\mathbb{Z}^\times$ の作用により同じ軌道の属する元を同伴という．この性質を，イデアルに注目することで一般の整域に適用する．$\mathbb{Z}$ の既約元とは，素数とその -1 倍をいう．$\mathbb{Z}$ や $\mathbb{Z}[X_1, \cdots, X_n]$ などの一意分解整域においては既約元と素元が一致する．既約元の見つけ方は素イデアルに注目するのがよく，素イデアルを生成する零でない元を素元という．

定義 2.8.1 (associated element, irreducible element, prime element). A を整域とする．

(1) $a, b \in A$ が**同伴**であるとは，次が成り立つことをいう：$\exists_{u \in A^\times}\ b = ua$.
(2) $a \in A$ が**既約元**であるとは，$a \notin A^\times \cup \{0\}$ かつ $\forall_{b,c \in A}\ a = bc \Rightarrow b \in A^\times \vee c \in A^\times$ が成り立つことをいう．
(3) $a \in A$ が**素元**であるとは，$a \neq 0$ かつ (a) が素イデアルであることをいう．[†16]

例 2.8.2 (多項式環の既約元と素元). 多項式環 $F[X]$ の部分環 $F[X^2, X^3]$ において，X^2 は既約元であるが素元ではない．

実際，$f, g \in F[X^2, X^3]$ が $X^2 = fg$ を満たすとき，いずれかは 0 次式，すなわち単元である必要がある．しかし，$(X^3)^2 = (X^2)^3 \in (X^2)$ であるが，$X^3 \notin (X^2)$ であるので，素イデアルを生成しない．□

補題 2.8.3 (同伴性の特徴付け・素元は既約). A を整域とする．

(1) $a, b \in A$ が同伴であることは，同じイデアルを生成すること $(a) = (b)$ に同値．
(2) A の任意の素元は既約元である．
(3) 同伴な元の既約性はすべて同値．

[†16] 後者の条件が $a \notin A^\times$ も含んでいることに注意．

[証明].

(1) (a) $a,b\in A$ が同伴であるとき，$\exists_{u\in A^\times}\ a=ub$ より，$x\in(a)\Leftrightarrow\exists_{u\in A}x=ya=yub\in(b)$ より，$(a)=(b)$ が従う，
(b) 逆に，$(a)=(b)$ であるとき，$a,b\in A$ が同伴であることを示す．$(a)=(b)=0$ ならば $a=b=0$ より，$u=1\in A^\times$ とすれば $b=ua$ が成り立つ．$0\subsetneq(a)=(b)$ のとき，$ab\neq0$．特に $b\in(a)$ より，$\exists_{u\in A}\ b=ua$ で，$a\in(b)$ より，$\exists_{u'\in A}\ a=u'b$．併せて，$a=u'b=u'ua$ 及び $a\neq0$ から，A が整域なので $uu'=1$ すなわち $u\in A^\times$ が従う．

(2) $p\in A$ を素元とする．
(a) (p) は素イデアルなので，$(p)\subsetneq A$ より，p は単元ではない．
(b) 任意に $a,b\in A$ をとり，$p=ab\in(p)$ を満たすとすると，$a\in(p)\vee b\in(p)$ が従う．$a\in(p)$ のとき，$\exists_{c\in A}\ a=pc$ より，$p=ab=pcb$ で，$p\neq0$ から，A が整域なので $cb=1$ となって $b\in A^\times$ が従う．同様に，$b\in(p)$ の時は $a\in A^\times$ が従う．

(3) $\exists_{u\in A^\times}\ b=ua$ であるとき，u の定める左移動は全単射である．[†17] したがって，条件 $b(=ua)=xy\Rightarrow x\in A^\times\vee y\in A^\times\vee$ の $x,y\in A$ それぞれについて，$u^{-1}x,y$ についての条件を考えれば良い．

■

要諦 2.8.4. 単項イデアル整域の極大イデアルの特徴付け 2.7.6 で (2)(b) と同様の議論をした．

2.8.2　定義と例

定義 2.8.5 (UFD: unique factorization domain). 整域 A に対して，任意の元 $a\in A\backslash\{0\}$ に対する次の 3 条件は同値である．

(1) (**既約元分解**と一意性) $a=up_1\cdots p_r$ $(a\in A^\times,p_1,\cdots,p_r:$ 既約元$,r\in\mathbb{N})$ と順番と同伴の別を除いて一意に表せる．ただし，$r=0$ の時は $p_1\cdots p_r=1$ と約束する．すなわち，$a=up_1\cdots p_r=vq_1\cdots q_s$ ならば，$r=s$ かつ $\exists_{\sigma\in S_r}\ \forall_{i\in[r]}\ p_i$ と $q_{\sigma(i)}$ は同伴 が成り立つ．
(2) (既約元分解と既約元と素元の一致) 既約元分解を持ち，かつ，A の任意の既約元は素元である．
(3) (**素元分解**) $a=up_1\cdots p_r$ $(a\in A^\times,p_1,\cdots,p_r:$ 素元$,r\in\mathbb{N})$ と表せる．ただし，$r=0$ の時は $p_1\cdots p_r=1$ と約束する．

整域 A がこの同値な条件を満たすとき，**一意分解整域**という．特に，素元分解は既約元分解だから，一意分解整域において，任意の元 $a\in A\backslash\{0\}$ に素元分解は存在して順番を除いてと同伴の別を除いて一意である．

[証明].

(1)⇒(2)　任意の既約元 $p\in A$ を取り，これが素元であることを示せば良い．p は既約元だから $p\neq0$．あとは (p) が素イデアルであることを示せば良い．特に p は単元ではないから，$p\subsetneq A$．よって，あとは $ab\in(p)\Rightarrow a\in(p)\vee b\in(p)$ を示せば良い．$ab=0$ の時は，A が整域であることから従うから，$ab\neq0$ の場合を考える．仮定 $ab\in(p)$ より，$\exists_{c\in A}\ ab=pc$．すると $a,b,c(\neq0)$ の既約元分解とその一意性により，a または b の既約元分解に，p と同伴な既約元が現れる．これより特に，$a\in(p),b\in(p)$.

(2)⇒(3)　この場合は任意の既約元分解が素元分解を与える．

(3)⇒(2)　素元は既約元 2.8.3(2) であるから，任意の $a\in A\backslash\{0\}$ は既約元分解を持つ．そこで，任意の既約元 $a\in A$ について，これが素元であることを示せば良い．素元分解 $a=up_1\cdots p_r$ を考えると，$a\notin A^\times$ より $r\geqslant1$ である．p_1 は素元なので，特に単元ではなく，$up_1\notin A^\times$．よって，$p_2\cdots p_r\in A^\times\Rightarrow p_2\in A^\times\wedge\cdots p_r\in A^\times$ が従う．これは不合理なので，$r=1$ で $a=up_1$，すなわち $(a)=(p_1)$ であることがわかった．(p_1) は素イデアルであるから，a は素元である．

(2)⇒(1)　任意の $a\in A\backslash\{0\}$ を取り，既約元分解を 2 つ $a=up_1\cdots p_r=vq_1\cdots q_s$ $(r\leqslant s)$ と取り，一意性を示せば良い．$r=0$ ならば，$a=u\in A^\times$ となり，$s=0$ が必要．よって成立．残った $r\geqslant1$ の場合を考える．
特に $vq_1\cdots q_s\in(p_1)$ で，p_1 は既約元より，仮定から素元だから，(p_1) は素イデアルで，$v\notin(p_1)$ と併せるとある $i\in[s]$ が存在して，$q_i\in(p_1)$ が必要．q_i は既約元であり，$p_1\notin A^\times$ なので，p_1 と q_i は同伴である：$\exists_{u_1\in A}\ q_i=u_1p_1$ かつ $u_1\in A^\times$．このとき，$up_2\cdots p_r=u_1vq_1\cdots q_{i-1}q_{i+1}\cdots q_s$．これを繰り返すことで，$u=v'($ 残った q_jが $s-r$ 個 $)\in A^\times$ となるから，$r=s$ が必要．こうして，全単射 $\sigma:[r]\xrightarrow{\sim}[r]$ であって，$\forall_{i\in[r]}\ q_{\sigma(i)}=u_ip_i$ を満たすものが定まる．

[†17] さらに言えば，これが A の自己同型だからであろう．

■

要諦 2.8.6. $p_2\cdots p_r\in A^\times \iff p_2\in A^\times\cdots p_r\in A^\times$ などの単元の性質を何度か使った．単元と不可逆元との積は不可逆である．

命題 2.8.7 . 単項イデアル整域は一意分解整域である．

[証明]. 条件 (3) を用いて，ある元 $a\in A\backslash\{0\}$ が素元分解を持たないとして矛盾を導く．$a\in A^\times$ ならば $r=0$ の場合が素元分解となるから，$a\notin A^\times$ の場合を考える．A の極大イデアル $\mathfrak{m}$ が存在して，$(a)\subset\mathfrak{m}$ が成り立つ（系 2.5.12）．A は単項イデアル整域なので，$\exists_{p_1\in A}\ (p_1)=\mathfrak{m}$ である．$p_1=0\Rightarrow\mathfrak{m}=0\Rightarrow a=0$ が従うから，$p_1\neq 0$ かつ (p_1) は特に素イデアルより，p_1 は素元である．したがって，$(a)\subset(p_1)=\mathfrak{m}$ は $\exists_{a_1\in A\backslash\{0\}}\ a=a_1p_1$ を意味する．$a_1\in A^\times$ ならばこれが素元分解を与えるから，$a_1\in A\backslash(A^\times\cup\{0\})$ とする．同様の条件を得たから，この議論は繰り返すことができ，$\exists_{p_2:\text{ 素元}}\ \exists_{a_2\in A\backslash\{0\}}\ a_1=a_2p_2$ となり，$a_2\notin A^\times$．これを繰り返すと，素元の列 (p_i) と $A\backslash(A^\times\cup\{0\})$ の列 (a_j) であって，$a_i=a_{i+1}p_{i+1}\ (i\geqslant 1)$ を満たすものを得る：$(a_1)\subset(a_2)\subset\cdots$．$I:=\cup_{i\geqslant 1}(a_i)$ は A のイデアルであるから（極大イデアルの存在 2.5.10 の証明抽出），$\exists_{x\in A}\ I=(x)$ が必要．すると，ある $i\in I$ について，$x\in(a_i)$ であるから，$(x)\subset(a_i)\subset(a_{i+1})\subset I=(x)$ を含意する．これは $(a_i)=(a_{i+1})$ を意味する．よって補題 2.8.3(1) より，a_i と a_{i+1} は同伴．$a_i=a_{i+1}p_{i+1}$ と併せると，$a_{i+1}\neq 0$ より $p_{i+1}\in A^\times$ だが，これは p_{i+1} が素元であることに矛盾．■

要諦 2.8.8 (単項イデアル整域は Noether 環である)**.** 単項イデアル整域が $A=\mathbb{Z}$ の時は，イデアルの任意の昇鎖列 $\{(a_i)\}_{i\in\mathbb{N}}$ があった時，$|a_i|$ という値が減少するので，必ず有限停止をする．同じことを，一般の単項イデアル整域で議論した．この性質が，一意分解性を導く．

定義 2.8.9 (Noetherian ring). イデアルの包含関係が整礎的であるような環を**ネーター環**という．これはイデアルの上で帰納法が使えることを意味する．

2.8.3　局所化についての閉性

補題 2.8.10 . A を一意分解整域，S をその積閉集合，$p\in A$ を素元であるとする．

(1) $(p)\cap S=\varnothing$ ならば $\dfrac{p}{1}=\iota(p)$ は $S^{-1}A$ の素元である．
(2) $(p)\cap S\neq\varnothing$ ならば $\dfrac{p}{1}=\iota(p)$ は $S^{-1}A$ の単元である．

[証明].

(1) $(p)\cap S=\varnothing$ ならば，素イデアルの対応 2.6.15 より，(p) に対応するイデアル $S^{-1}(p)=\iota((p))S^{-1}A=(\iota(p))$（$\iota(p)$ が生成するイデアル 2.6.12(1)）は素イデアルである．$p\neq 0$ より $\dfrac{p}{1}\neq 0$ で，$\iota(p)\in S^{-1}A$ も素元である．
(2) $(p)\cap S\neq\varnothing$ のとき，$ap\in S$ を満たす $a\in A$ が存在する（(p) の任意の元は ap と表せる 2.2.12 ため）．このとき，$1=\dfrac{p}{1}\cdot\dfrac{a}{ap}$ より，$\iota(p)$ は $S^{-1}A$ の単元である．

■

命題 2.8.11 . A を一意分解整域とし，S をその積閉集合とする．$0\notin S$ ならば，$S^{-1}A$ は再び一意分解整域である．

[証明]. $S^{-1}A$ は整域である（命題 2.6.20）．$S^{-1}A\backslash\{0\}$ の任意の元は $a\in A\backslash\{0\}, s\in S$ を用いて $\dfrac{a}{s}$ と表せる．これが素元分解を持つことを示す．

A は一意分解整域としたから，素元分解 $a=up_1\cdots p_r$ が取れる．$p_1,\cdots,p_r$ は，ある $1\leqslant k\leqslant r$ について，

$$\begin{cases}(p_i)\cap S\neq\varnothing, & 1\leqslant i\leqslant k,\\ (p_i)\cap S=\varnothing, & k+1\leqslant i\leqslant r\end{cases}$$

を満たすように取る．すると，補題より，

$$\frac{a}{s}=\underbrace{\frac{u}{s}\cdot\frac{p_1}{1}\cdots\frac{p_k}{1}}_{\in(S^{-1}A)^\times}\frac{p_{k+1}}{1}\cdots\frac{p_r}{1}$$

は $\dfrac{a}{s}$ の素元分解となっている．■

2.8.4　単項分数イデアル

分数イデアル：分母が許されたイデアルの拡張を商体の部分 A 加群に注目して定義する

一意分解整域では,「最大公約数」「最小公倍数」の概念が定義できる．単元倍の任意性のある概念である ($\gcd(6,9)=\pm 3$？) から，元の代わりにそれが生成する単項イデアルについて定義した方が明快になる．しかし，単項イデアルの積は再び単項イデアルであるが，逆元が存在するとは限らない．それが Abel 群の構造を定めるように，議論の場所を商体に移し，概念を拡張する．$\mathrm{Frac}\,A$ **上での部分** A **加群として概念を拡張すれば良い**のである．すると，単項分数イデアル全体は，A の単項素イデアル全体の積で表せる（まさに素因数分解への引き戻し）．そしてこの演算について，単項分数イデアルの「最大公約数」「最小公倍数」を考えるのである．すると，A の商体の零でない元全てについて最小公倍数と最大公約数の概念が定まる．イデアルの演算というこれ以上無いほどに複雑な構造に仮託しているが，どうしてイデアルの方が概念として安定なのだろうか？

定義 2.8.12 (principal fractional ideal). A を一意分解整域，$F:=\mathrm{Frac}\,A=(A\backslash\{0\})^{-1}A$ をその商体とする．商体の単元 $x\in F^\times(\overset{def}{=}F\backslash\{0\})$ に対し，$(x)=\{ax\in F\mid a\in A\}$ とおくと，これは F の部分 A-加群になり，$y\in(x)\wedge a\in A\Rightarrow ay\in(x)$ を満たす．この形で表せる F の部分集合を，A の**単項分数イデアル**といい，x をその**生成元**という．

注 2.8.13 (fractional ideal).

(1) 単項イデアル（の F への埋め込み）は単項分数イデアルである．
(2) $x,y\in F^\times$ について，$(x)=(y)\ \Leftrightarrow\ xy^{-1}\in A^\times$ が成り立つ．この条件も，単元の軌道分解による同値類に入るから，x と y は**同伴**であるという．[†18]
(3) A の単項分数イデアル全体は，体の上で考えているから，積を $(x)\cdot(y):=(xy)$ として Abel 群となる．単位元は $A=(1)$ で，逆元は (x^{-1}) である．
(4) 一般に，体 F の部分 A-加群 I で $\exists_{r\in A\backslash\{0\}}\ rI\subset A$ を満たすものを**分数イデアル**という．A が Noether 環であるとき，この定義は，部分 A-加群 I が有限生成であることと同値になる．[†19]代数的整数論で大事になる概念で，「分母が許されたイデアルの概念拡張」のようなものである．

補題 2.8.14 (単項分数イデアルの Abel 群の構造：単項素イデアルへの注目). A を一意分解整域，$F:=\mathrm{Frac}\,A=(A\backslash\{0\})^{-1}A$ をその商体とする．A の 0 でない単項素イデアル全体の集合を P_A とする．

(1) Abel 群 $\mathbb{Z}$ の添字 $\mathfrak{p}\in P_A$ による直和から A の単項分数イデアルのなす Abel 群への写像

$$\begin{array}{ccc}\Phi:\bigoplus_{\mathfrak{p}\in P_A}\mathbb{Z} & \longrightarrow & \{A\text{ の単項分数イデアル全体}\}\\ \cup & & \cup\\ (m_\mathfrak{p})_{\mathfrak{p}\in P_A} & \longmapsto & \prod_{\mathfrak{p}\in P_A}\mathfrak{p}^{m_\mathfrak{p}}\end{array}$$

は全単射な群準同型（したがって同型 1.1.7）である．[†20]Φ の逆写像を $I\mapsto(m_\mathfrak{p}(I))_{\mathfrak{p}\in P_A}$ と表す．
(2) A の単項分数イデアル I,J に対して，$I\subset J\ \Leftrightarrow\ \forall_{\mathfrak{p}\in P_A}\ m_\mathfrak{p}(I)\geqslant m_\mathfrak{p}(J)$ が成り立つ．すなわち，$\bigoplus_{\mathfrak{p}\in P_A}\mathbb{Z}$ にそのような順序を入れると，Φ は単調（減少）写像である．[†21]

[証明].

(1) 積の構造は確かに保たれ，Φ は群準同型である．[†22]
全射性　$I=(x)$ $(x\in F^\times)$ を任意の単項分数イデアルとし，Φ による逆像の元を構成すれば良い．

[†18] $xy^{-1}\in H\ \Leftrightarrow\ \exists_{h\in H}\ x=hy$ が部分群の特徴付なのであった．
[†19] $I=A\frac{1}{2}+A\frac{1}{3}$ などは 2 元生成の $\mathbb{Z}$ の分数イデアルである．
[†20] ただし，$\mathfrak{p}^0=A$ とする．整数環における事象 $n^0=1$ に当たる．
[†21] この逆転構造はなんだ？
[†22] $\mathfrak{p}^0=A$ と約束したとき，確かに単位元は単位元に写り，Φ は群準同型である．

(a)　特に $x \in A\backslash\{0\}$ の場合を考える．A は一意分解整域だから，素元分解 $x = up_1 \cdots p_r$ が取れる．任意の $\mathfrak{p} \in P_A$ に対して，$m_\mathfrak{p}(I) := |\{i \in [r] \mid (p_i) = \mathfrak{p}\}|$ とおくと，$(m_\mathfrak{p}(I))_{\mathfrak{p}\in P_A} \in \bigoplus_{\mathfrak{p}\in P_A} \mathbb{Z}$ で（素元分解 (p_i) は有限列なので，$m_\mathfrak{p}(I) \neq 0$ を満たす $\mathfrak{p} \in P_A$ は有限個），$I = \prod_{\mathfrak{p}\in P_A} \mathfrak{p}^{m_\mathfrak{p}(I)} = \Phi((m_\mathfrak{p})_\mathfrak{p})$ である．このとき，$m_\mathfrak{p}(I) \geqslant 0$ であることに注意．

(b)　一般の $x \in F^\times$ の場合については，任意の元は $x = \dfrac{a}{b}$ $(a, b \in A\backslash\{0\})$ と表せる．$m_\mathfrak{p}(I) := m_\mathfrak{p}((a)) - m_\mathfrak{p}((b))$ と定めると，$\Phi((m_\mathfrak{p}(I))_{\mathfrak{p}\in P_A}) = (a)(b)^{-1} = (x) = I$ となる．

単射性　$(m_\mathfrak{p})_{\mathfrak{p}\in P_A} \in \bigoplus_{\mathfrak{p}\in P_A} \mathbb{Z}$ が $\prod_{\mathfrak{p}\in P_A} \mathfrak{p}^{m_\mathfrak{p}} = A$ を満たすと仮定し，$\forall_{\mathfrak{p}\in P_A}\ m_\mathfrak{p} = 0$ を示す．$P_+ := \{\mathfrak{p} \in P_A \mid m_\mathfrak{p} > 0\}, P_- := \{\mathfrak{p} \in P_A \mid m_\mathfrak{p} < 0\}$ とおいて，$P_+ = P_- = \varnothing$ を示せば良い．このとき，$\prod_{\mathfrak{p}\in P_+} \mathfrak{p}^{m_\mathfrak{p}} = \prod_{\mathfrak{p}\in P_-} \mathfrak{p}^{-m_\mathfrak{p}}$ が成り立つ．[†23]ただし，$P_\pm = \varnothing$ ならば，$\prod_{\mathfrak{p}\in P_\pm} \mathfrak{p}^{m_\mathfrak{p}} = A$ とする．よって，各単項素イデアル $\mathfrak{p} \in P_A$ の生成元 $p_\mathfrak{p}$ を考えると，両辺の生成元は $\prod_{\mathfrak{p}\in P_+} p_\mathfrak{p}^{m_\mathfrak{p}}$ と $\prod_{\mathfrak{p}\in P_-} p_\mathfrak{p}^{-m_\mathfrak{p}}$ になり，これらは同伴になる（注 2.8.13）．[†24]A は一意分解整域だから，素元分解の一意性より，$P_+ \neq \varnothing$ ならば，$\mathfrak{p}_1 \in P_+$ を取ると，$\mathfrak{p}_1' \in P_-$ であって，$p_{\mathfrak{p}_1}$ と $p_{\mathfrak{p}_1'}$ とが同伴であるものが存在するが，このとき $\mathfrak{p}_1 = (p_{\mathfrak{p}_1}) = (p_{\mathfrak{p}_1'}) = \mathfrak{p}'$ が従い，$P_+ \cap P_- = \varnothing$ に矛盾する．よって，$P_+ = \varnothing$ である．同様に，$P_- = \varnothing$ が導ける．

(2) $\Rightarrow$　$I = (x), J = (y)$ となる $x, y \in F^\times$ が存在する．$I \subset J \Leftrightarrow (x) \subset (y)$ のとき，特に $x \in (y)$ で，$\exists_{z\in A\backslash\{0\}}\ x = yz$ が成り立つから，$J' := (z)$ とおくと，$I = JJ'$．よって，$\forall_{\mathfrak{p}\in P_A}\ m_\mathfrak{p}(I) = m_\mathfrak{p}(JJ') = m_\mathfrak{p}(J) + m_\mathfrak{p}(J')$．このとき，$z \in A\backslash\{0\}$ より，全射性の証明の (b) での議論の通り $m_\mathfrak{p}(J') \geqslant 0$ なので，$m_\mathfrak{p}(I) \geqslant m_\mathfrak{p}(J)$ が示された．

$\Leftarrow$　$\forall_{\mathfrak{p}\in P_A}\ m_\mathfrak{p}(I) \geqslant m_\mathfrak{p}(J)$ のとき，$I = \prod_{\mathfrak{p}\in P_A} \mathfrak{p}^{m_\mathfrak{p}(I)} \subset \prod_{\mathfrak{p}\in P_A} \mathfrak{p}^{m_\mathfrak{p}(J)} = J$ が従う．$\mathfrak{p}^0 = A$ なので，零でない $m_\mathfrak{p}$ が多いほど，積の結果得るイデアルは小さくなることに注意．

■

要諦 2.8.15 (素元ではなく単項素イデアルに注目する)**.** A の単項分数イデアルを，素イデアルの（負冪も含めた）積でみたとき，素因数分解のように使えるという補題である．これによって，整数で慣れ親しんだ概念を，一般の一意分解整域に素イデアルの言葉を通して流入させることができる．

定義 2.8.16 (最大公約イデアル・最小公倍イデアル).

(1) A を一意分解整域とし，$I_1, \cdots, I_n$ を A の単項分数イデアルとする．
  (a) 単項分数イデアル $\prod_{\mathfrak{p}\in P_A} \mathfrak{p}^{\max_{1\leqslant i\leqslant n} m_\mathfrak{p}(I_i)}$ を $I_1, \cdots, I_n$ の**最小公倍イデアル**という．
  (b) 単項分数イデアル $\prod_{\mathfrak{p}\in P_A} \mathfrak{p}^{\min_{1\leqslant i\leqslant n} m_\mathfrak{p}(I_i)}$ を $I_1, \cdots, I_n$ の**最大公約イデアル**という．

(2) $a_1, \cdots, a_n \in F^\times$ に対し，
  (a) 単項分数イデアル $(a_1), \cdots, (a_n)$ の最小公倍イデアルの生成元を，**最小公倍数**という．
  (b) 単項分数イデアル $(a_1), \cdots, (a_n)$ の最大公約イデアルの生成元を，**最大公約数**という．
  これらは，同伴の別を除いて定まる．[†25]

(3) $a, b \in A$ の最大公約数が A の単元となる（したがって，単項イデアル $(a), (b)$ の最大公約イデアルが A である）とき，これらを**互いに素**という．

例 2.8.17 (整数環での例)**.** $\mathbb{Z}$ の単項分数イデアル $I = \left(\dfrac{48}{25}\right), J = \left(-\dfrac{28}{125}\right)$ を考える．$I = (2)^4(3)(5)^{-2}, J = (2)^2(5)^{-3}(7)$ である．よって，最小公倍イデアルは $(2)^4(3)(5)^{-2}(7) = \left(\dfrac{336}{25}\right)$ であり，最大公約イデアルは $(2)^2(5)^{-3} = \left(\dfrac{4}{125}\right)$ である．よって，$\dfrac{48}{25}, -\dfrac{28}{125}$ の最小公倍数は $\pm\dfrac{336}{25}$ で，最大公約数は $\pm\dfrac{4}{125}$．分母の最小公倍は，あくまで $-3 < -2$ のとき -2 を採用する．　□

要諦 2.8.18. 最大公約数が小さいとき，対応する最大公約イデアルは大きいことに注意．

[†23] $\prod_{\mathfrak{p}\in P_A} \mathfrak{p}^{m_\mathfrak{p}} = A$ の分母を払ったことに当たる．この後は，両辺の素元分解を考えれば良い．

[†24] $P_\pm$ が一般の濃度の場合に，これらの A の元が well-defined であるか不安になる．

[†25] おそらく単元 u の左移動による作用が A の自己同型を定めるからであろう．

2.8.5　互いに素

互いに素であるということは，同伴でない素元を 2 つ含むイデアルは必ず自明であることで捉えられる．2 つの主イデアルの和が主イデアルになる整域で必ず Bézout の補題は成立するから，このようなクラスを Bézout 整域という．単項分数イデアルの全体はある種の Bézout 整域である．

命題 2.8.19 (最小公倍・最大公約イデアルの特徴付け). A を一意分解整域とし，$I_1,\cdots,I_n$ をその単項分数イデアルとする．

(1) $I_1,\cdots,I_n$ の最小公倍イデアルは，$\forall_{i\in[n]}\ J\subset I_i$ を満たす単項分数イデアル J のうち最大のものである．
(2) $I_1,\cdots,I_n$ の最大公約イデアルは，$\forall_{i\in[n]}\ I_i\subset J$ を満たす単項分数イデアル J のうち最小のものである．
(3) 任意の単項分数イデアル J について，$J\gcd(I_1,\cdots,I_n)=\gcd(JI_1,\cdots,JI_n), J\operatorname{lcm}(I_1,\cdots,I_n)=\operatorname{lcm}(JI_1,\cdots,JI_n)$ である．

[証明]. 補題 2.8.14 の写像 Φ^{-1} によって，$\bigoplus_{\mathfrak{p}\in P_A}\mathbb{Z}$ での議論に還元すれば明らか．■

命題 2.8.20 (互いに素の特徴付け？). A を一意分解整域とする．$a,b\in A$ について，次の 3 条件は同値か？

(1) a と b は互いに素．
(2) (Bézout's lemma) $\exists_{x,y\in A}\ ax+by=1$.
(3) a も b も素元で，互いに同伴でない．

A が単項イデアル整域ならば (3)⇒(2) が明らかなのでこれらは同値である．問題は，一意分解整域でも並行な議論が成り立つかどうかだ．

[証明].

(1)⇒(2)　仮定より，$(a)\subset I,(b)\subset I$ を満たす最小の単項分数イデアル I について $I=A$ である 2.8.19．このとき I の任意の元は $ax+by$ $(x,y\in A)$ と表される 2.2.12 から[†26]，$(a)+(b)=I=A$ が成り立つ．特に $\exists_{x,y\in A}\ ax+by=1$.

(2)⇒(1)　(2) の仮定は，a,b を含む（単項分数）イデアルは必ず A になることを含意する．これは，$(a),(b)$ の最大公約イデアルについても例外ではない．

(3)⇒(1)　一意分解整域について，これは成り立つはず．逆は自信がない．

2 つの同伴でない素元 a,b が生成する素イデアルについて，$(a)\subsetneq I,(b)\subsetneq I$ を満たす最小の単項分数イデアル I は，$I=A$ であるという，単項イデアル整域の消息 2.7.6 に似たことを示せば良い（a,b が同伴でないことは $(a)\neq(b)$ に同値 2.8.3 で，$(a),(b)\subsetneq I$ に注意）．I は単項分数イデアルなので，$\exists_{x\in F^\times}\ I=(x)$ と表せる．仮定 $(a)\subsetneq I$ は，$\exists_{y\in A}\ a=xy$ を含意する．特に $xy\in(a)$ ヨリ，$x\in(a)\vee y\in(a)$ が従う．$x\in(a)$ ならば $I\subset(a)$ が必要だから仮定に反する．したがって $y\in(a)$ であるが，このとき $\exists_{z\in A}\ y=za$ であり，$a=xy$ と併せて $a=xza\Leftrightarrow a(1-xz)=0$．これは商体 $F=\operatorname{Frac}A$ 上の等式とみなせて，特に整域だから，$xz=1\in I$ が必要．したがって，$I=A$ である．

■

要諦 2.8.21 (同伴でない素元を 2 つ含むイデアルは必ず自明である)**.** 単項分数イデアルの言葉で互いに素であることを定義した．すると，ある種の単項イデアル整域に議論領域が限定されるため，素イデアルの様子が単項イデアル整域の場合 2.7.6 に類似する．これが整数論で有名な「a と b が互いに素 $\Leftrightarrow$ $\exists_{x,y\in A}\ ax+by=1$」である．

注 2.8.22. 一意分解整域 $k[X]$ での Bézout の補題が非自明である．互いに素な $f_1(x),f_2(x)$ について，$g_1(x)f_1(x)+g_2(x)f_2(x)=1$ とできる．

[†26] というより，I は A 加群なので，I の最小性から $I\subset Aa+Ab$ が必要．

2.8.6　一意分解整域上の多項式環は一意分解整域

一意分解整域上の n 変数多項式環は一意分解整域である

$\mathbb{Z}$ は一意分解整域だから，$\mathbb{Z}[X]$ も一意分解整域である．任意の体 K について，$K[X]$ は Euclid 整域 2.7.4 であり，多変数多項式 $K[X_1,\cdots,X_n]$ は一意分解整域である．
原始多項式はある種の正規化された対象である．単項分数イデアルの概念を引き継ぎ，$F:=\operatorname{Frac}A$ 係数多項式上に拡張して捉える視点が肝要になる．

定義 2.8.23 (primitive polynomials). A を一意分解整域とし，$F=\operatorname{Frac}A$ をその商体とする．多項式 $f=a_nX^n+\cdots+a_1X+a_0\in F[X]\backslash\{0\}$ に対し，その係数が定める単項分数イデアル $(a_0),\cdots,(a_n)$ のうちの 0 でないものの最大公約イデアルを $I(f)$ とおく．

(1) $I(f)=A$ を満たすような $f\in F[X]\backslash\{0\}$ を**原始多項式**と呼ぶ.[†27] $a_i\in A$（特に $a_i\in A^\times$）でないと $A\subset(a_i)$ を満たさないので，特に $A[X]\backslash\{0\}$ の元である．
(2) 単項分数イデアル $I(f)$ の生成元を $c(f)$ と書き，f の**内容**という．これは同伴を除いて一意に定まる．

補題 2.8.24 (I の関手性と内容-原始成分分解). A を一意分解整域，$F=\operatorname{Frac}A$ をその商体，$f,g\in F[X]\backslash\{0\}$ を多項式とする．

(1) f,g が原始多項式ならば fg も原始多項式である．
(2) $a\in F^\times$ に対し，$I(af)=(a)I(f)$ が成り立つ．特に，a を $I(f)$ の生成元とすると，$a^{-1}f$ は原始多項式である．
(3) $I(fg)=I(f)I(g)$ である．
(4) 任意の $A[X]$ の元は，内容と原始多項式の積に，A の単元倍を除いて一意的に分解できる．

[証明].

(1) f,g は原始多項式だから，特に $f,g\in A[X]$ である．A が整域であることより $A[X]$ も整域 2.4.5 だから，$f,g\neq0$ の仮定より $fg\neq0$ が従う．ここで，$fg\in A[X]\backslash\{0\}$ が原始多項式ではない，すなわち $I(fg)\subsetneq A$ と仮定して矛盾を導く（$a_i\in A$ のとき，$(a_i)\subset A$ に注意）．
$I(fg)\subsetneq A$ のとき，$I(fg)\subset(p)\subsetneq A$ を満たす素元 $p\in A$ が存在する．これは $I(fg)$ の生成元の素元分解に現れる素元を任意に取れば良い.[†28] このような p を 1 つ取ると，fg の係数は全て p で割り切れるということであるから，全射準同型 $p:A[X]\to A/(p)[X]$ の像 $\overline{f}:=p(f),\overline{g}:=p(g)$ について，$\overline{f}\cdot\overline{g}=0$ が成り立つ．$p\in A$ は素元より (p) は素イデアルで $A/(p)$ は整域，したがって $A/(p)[X]$ も整域 2.4.5 だから，$\overline{f}=0\vee\overline{g}=0$ が従う．$\overline{f}=0$ のとき，f の係数が全て p で割り切れるということだから，$I(f)\subset(p)\subsetneq A$ が成り立ち，f が原始多項式であることに矛盾．$\overline{g}=0$ の場合も同様．
(2) 最大公約イデアルの性質 2.8.19 より，

$$I(af)\overset{def}{=}\gcd((aa_0),\cdots,(aa_n))=(a)\gcd((a_0),\cdots,(a_n))=(a)I(f).$$

また，a が $I(f)$ の生成元であるとき，$(a)=I(f),(a^{-1})=(a)^{-1}=I(f)^{-1}$ より，$I(a^{-1}f)=I(f)^{-1}I(f)=(1)=A$ より，$a^{-1}f$ は原始多項式である．
(3) $a\in I(f),b\in I(g)$ をそれぞれの生成元とすると，(2) より $a^{-1}f,b^{-1}g$ は原始多項式である．よって，(1) より，$(a^{-1}f)(b^{-1}g)$ は原始多項式である．よって，(2) より，

$$\begin{aligned}I(fg)&=I(ab(a^{-1}f)(b^{-1}g))=(ab)I((a^{-1}f)(b^{-1}g))\\&=(ab)A=(ab)=(a)(b)=I(f)I(g).\end{aligned}$$

■

定理 2.8.25 (Gauss の補題：既約元の特徴付け). A を一意分解整域，$F=\operatorname{Frac}A$ をその商体とする． 1 次以上の多項式 $f\in A[X]\backslash A$ に対して，次の 2 条件は同値．

[†27] すなわち，内容＝係数の最大公約数が ±1 であるような多項式である．
[†28] 単項分数イデアル全体は Abel 群をなすので，$I(fg)$ も単項分数イデアルであることに注意．

(1) f は $A[X]$ の既約元である．
(2) f は原始多項式であり，かつ，$F[X]$ の既約元である．

[証明].

(1)⇒(2)　**f は原始多項式である**　$I(f)(\neq\varnothing)$ の生成元 $a\in F^\times=F\backslash\{0\}$ をとる．補題 2.8.24(2) より，$a^{-1}f$ は原始多項式だから，特に $a^{-1}f\in A[X]$ で，また $f\in A[X]$ より $I(f)\subset A$ より特に $a\in A$．よって，$f=a(a^{-1}f)$on $A[X]$ であるが，f の $A[X]$ での既約性から，$a\in A[X]^\times=A^\times$ または $a^{-1}f\in A[X]^\times=A^\times$ が従う 2.4.5．仮定より $a^{-1}f$ は 1 次以上の多項式だから，前者が成り立ち，$I(f)=(a)=A$ を得る．

既約元である　まず f は一次以上という仮定より，零ではなく，$f\notin F^\times=F[X]^\times$ である．よって，あとは，任意の $f=gh$ を満たす $g,h\in F[X]$ について，$g\in F^\times\vee h\in F^\times$ を導けば良い．

$a,b\in F^\times$ をそれぞれ $I(g),I(h)$ の生成元とすると，補題 2.8.24(3) より，$A=I(f)=I(gh)=I(g)I(h)=(ab)$ となるので，$ab\in A^\times$ が成り立つ．$u:=ab$ とおくと，$f=(a^{-1}\cdot ub^{-1})gh=(a^{-1}g)(ub^{-1}h)$ である．$a^{-1}g,b^{-1}h$ は原始多項式であるから，$a^{-1}g,ub^{-1}h\in A[X]$ より，f が $A[X]$ の既約元という仮定から $a^{-1}g\in A[X]^\times\vee ub^{-1}h\in A[X]^\times$，特に $a^{-1}g\in F[X]^\times\vee ub^{-1}h\in F[X]^\times$ が従う．$a,b\in F^\times$ より $a^{-1},ub^{-1}\in F^\times$ だから，$g\in F[X]^\times,h\in F[X]^\times$ がわかった．

(2)⇒(1)　f が $F[X]$ の既約元より $f\notin F[X]^\times$ なので，$f\notin A[X]^\times$ は明らか．あとは $g,h\in A[X]$ が $f=gh$ を満たすと仮定して，$g\in A[X]^\times\vee h\in A[X]^\times$ を導けば良い．

f は $F[X]$ の既約元としたから，$g\in F[X]^\times\vee h\in F[X]^\times$ である．$F[X]^\times=F^\times$2.4.5 より，$g,h\in A[X]$ と併せると，$F^\times\cap A=A\backslash\{0\}$ より $g\in A\backslash\{0\}\vee h\in A\backslash\{0\}$ が解る．このとき前者が成り立つと仮定しても一般性を失わない．$I(f)=I(g)I(h)=(g)I(h)\subset(g)A=(g)$ より（$h\in A[X]$ より $I(h)\subset A$ に注意 2.8.19），$I(f)=A$ という仮定と合わせると，$(g)=A$ が必要．したがって，$g\in A^\times$ である．

■

要諦 2.8.26. (1)⇒(2) の考え方が肝要で，定理 2.8.27 の証明でも使われる．

定理 2.8.27 . A が一意分解整域であるとき，多項式環 $A[X]$ も一意分解整域である．すなわち，次の 2 条件が成り立つ．

(1) A を一意分解整域とするとき，$A[X]\backslash\{0\}$ の任意の元は既約元分解を持つ．
(2) A を一意分解整域とするとき，$A[X]$ の任意の既約元は素元である．

[証明].

(1) $f\in A[X]\backslash\{0\}$ を任意に取る．f を商体 $F:=\operatorname{Frac}A$ 上の多項式と見ると，体上の多項式環 $F[X]$ は Euclid 整域より単項イデアル整域 2.7.4 で，したがって一意分解整域 2.8.7 であるから，$F[X]$ 内で既約元分解

$$f=ug_1\cdots g_r\qquad(u\in F^\times,g_1,\cdots,g_r:F[X]\text{ の既約元 })$$

をもつ．

(a) $a\in A\backslash\{0\},b_1,\cdots,b_r\in F^\times$ をそれぞれ $I(f),I(g_1),\cdots,I(g_r)\subset F$ の生成元とすると，補題 2.8.24 より，

$$(a)=I(f)=(u)I(g_1)\cdots I(g_r)=(ub_1\cdots b_r)$$

が成り立つ．よって，$u':=a^{-1}ub_1\cdots b_r$ と定めると，$(u')=(1)$ より，$u'\in A^\times$ である．

(b) $A[X]$ 上の等式 $f=au'(b_1^{-1}g_1)\cdots(b_r^{-1}g_r)$ をよく考えると，実はこれは既約元分解を与えている．まず，項 $b_i^{-1}g_i\in A[X]$ は $F[X]$ において既約元 g_i と同伴であるから $F[X]$ の既約元で 2.8.3(3)，また原始多項式であるから，Gauss の補題 2.8.25 より，$b_i^{-1}g_i$ は $A[X]$ の既約元である．続いて，A は一意分解整域だから，$au'\in A\backslash\{0\}$ は A において既約元分解 $au'=u''p_1\cdots p_s$ を持つ．$A[X]^\times=A^\times$ も考え合わせると，A の既約元は $A[X]$ でも既約元だから，これは $A[X]$ 上での既約元分解でもある．以上より，等式 $f=au'(b_1^{-1}g_1)\cdots(b_r^{-1}g_r)$ は $A[X]$ 上の既約元分解を与える．

(2) $f\in A[X]$ を任意の既約元とする．あとは $(f)\subset A[X]$ が素イデアルであることを示せば良い．

$f\in A$ のとき　$A^\times=A[X]^\times$ より，f は A の既約元でもあるから，A が一意分解整域であることより，f は A の素元である．したがって $A/(f)$ は整域で $A/(f)[X]$ も整域だから，$A[X]/(f)\simeq A/(f)[X]$ より，(f) は $A[X]$ の整域でもある（素イデアルの特徴付け 2.5.2）．

$f \notin A$ **のとき**　(a)　f は一次以上の多項式であるから，Gauss の補題 2.8.25 より，f は $F[X]$ の既約元であるような原始多項式である．いま $F[X]$ は一意分解整域であるから，f は $F[X]$ の素元でもある．すなわち，単項イデアル $(f)_{F[X]}$ は素イデアルである．したがって，素イデアルの逆像は素イデアルだから 2.5.6，$i : A[X] \hookrightarrow F[X]$ について，$i^{-1}((f)_{F[X]}) = A[X] \cap (f)_{F[X]} = (f)_{A[X]}$ を示せば十分．

(b)　$A[X] \cap (f)_{F[X]} \supset (f)_{A[X]}$ は $f \in A[X]$ と $(f)_{A[X]} = f \cdot A[X]$2.2.12 より明らかだから，$A[X] \cap (f)_{F[X]} \subset (f)_{A[X]}$ を示せば良い．任意に $g \in A[X] \cap (f)_{F[X]}$ を取ると，$\exists_{h \in F[X] \setminus \{0\}}\ g = fh$．補題 2.8.24 より，$I(g) = I(f)I(h) = AI(h) = I(h)$ であるから，$g \in A[X]$ より $I(g) \subset A$ である（最大公約イデアルの特徴付け 2.8.19）ことと併せて，$I(h) \subset A$ を得る．これより $h \in A[X]$ が従うので，[†29] $g \in (f)_{A[X]}$ である．

■

系 2.8.28．F を体とし，$n \geqslant 1$ を整数とする．$F[X_1, \cdots, X_n]$ は一意分解整域である．

[証明]．

(1) Euclid 整域 $F[X_1]$ は単項イデアル整域である 2.7.4 から，一意分解整域である 2.8.7．
(2) $F[X_1, \cdots, X_n] \simeq (F[X_1, \cdots, X_{n-1}])[X_n]$ であるから，定理 2.8.27 より，帰納的に $F[X_1, \cdots, X_n]$ は一意分解整域である．

■

2.8.7　Eisenstein の既約判定法

引き続き多項式環の研究で，Gauss の補題 2.8.25 からさらに踏み込んで，既約元を特徴づける結果を考える．monic な多項式は $A[X]$ の中で乗法についてモノイドをなす（モニック多項式の積はモニック）．体の拡大の理論で方程式の既約性の判定が肝要になってくる．

定理 2.8.29 (Eisenstein の既約判定法)．A を整域とする．A 係数のモニックな多項式 $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in A[X]$ $(n \geqslant 1)$ に対して，素イデアル $\mathfrak{p} \subset A$ が存在して次の 2 条件を満たすならば，f は $A[X]$ の既約元である．

(a) $\forall_{i \in n}\ a_i \in \mathfrak{p}$.
(b) $a_0 \notin \mathfrak{p}^2$.

特に A が一意分解整域である場合は，$F = \operatorname{Frac} A$ とおくと f は $F[X]$ の元としても既約である（Gauss の補題 2.8.25）．[†30]

[証明]．$f = 1 \in A^\times$ の場合，条件 (a),(b) を満たす素イデアル $\mathfrak{p}$ は存在しないから，確かに f は $A[X]$ の既約元ではない．そこで，$\deg f \geqslant 1$ の場合のみを考えれば良い．したがって，あとは $f = gh$ を満たす $g, h \in A[X]$ について，$g \in A^\times \vee h \in A^\times$ を導けば良い．

(1)

$$g = b_r X^r + \cdots + b_1 X + b_0, \qquad h = c_s X^s + \cdots + c_1 X + c_0,$$

とおく $(b_r c_s \neq 0)$．すると gh の最高次項は $b_r c_s X^{r+s}$ であり，$b_r c_s = 1 . r + s = n$ が必要．特に $b_r, c_s \in A^\times$．

(2) この g, h の係数に関しても $\forall_{i \in r, j \in s}\ b_i, c_j \in \mathfrak{p}$ であることを示す．

$$i_0 := \min\{i \in r \mid b_i \notin \mathfrak{p}\}, \qquad j_0 := \min\{j \in s \mid c_j \notin \mathfrak{p}\},$$

とおいて，$i_0 = r, j_0 = s$ を示せば良い．いま $i_0 \leqslant r, j_0 \leqslant s$ なので，$i_0 + j_0 = r + s$ を示せば十分．そこで，$i_0 + j_0 < r + s$ と仮定して矛盾を導く．等式 $f = gh$ の $X^{i_0 + j_0}$ の項の係数を比較することで，

$$a_{i_0 + j_0} = \sum_{i,j \geqslant 0, i+j = i_0 + j_0} b_i c_j \in b_{i_0} c_{j_0} + \mathfrak{p}$$

[†29] $I(h) \subset A$ とは，最大公約イデアルの特徴付け 2.8.19 より，h の係数の生成する単項分数イデアル $(a_i) \subset F$ が全て A 以外の元を含まないことを意味するから．

[†30] この場合は，$\mathfrak{p}$ として単項イデアルを取る場合が多い．

を得る．仮定より，$a_{i_0+j_0} \in \mathfrak{p}$ であるから，$b_{j_0}c_{j_0} \in \mathfrak{p}$ でもあるが，これは b_{j_0}, c_{j_0} の取り方に矛盾する．よって，$b_i, c_j \in \mathfrak{p}$ $(i \in r, j \in s)$.

(3) もし $r \geqslant 1 \wedge s \geqslant 1$ ならば，(2) より $b_0, c_0 \in \mathfrak{p}$ なので，$f = gh$ の定数項について比較することで，$a_0 = b_0c_0 \in \mathfrak{p}^2$ が従うが，これは仮定 (b) に矛盾．よって，$r = 0 \vee s = 0$ である．すなわち，$g \in A^\times \vee h \in A^\times$.

■

要諦 2.8.30. 係数比較と係数の積についての整域の性質による議論を繰り返すのみで得られる性質であり，あまりにも精密機械のような証明の仕組みに呆れた．

例 2.8.31 (既約多項式)**.** 素数 p について，$f(X) = X^{p-1} + X^{p-2} + \cdots + X + 1 \in \mathbb{Z}[X]$ は $\mathbb{Q}[X]$ の既約元である．

このままでは全ての係数が 1 なので，素イデアル $\mathfrak{p}$ は見つからない．$\mathbb{Q}[X]$ の商体 $\mathbb{Q}(X)$ において，

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

が成り立ち，最左辺と最右辺との等式は $\mathbb{Z}[X]$ 上においても成り立つ．

- $0 \leqslant i \leqslant p-2$ に対して，X^i の係数は $\binom{p}{i+1}$ であるから p の倍数である．
- $f(X+1)$ の定数項 p は p^2 の倍数ではない．

よって，Eisenstein の既約判定法 2.8.29 より，$f(X+1)$ は $\mathbb{Z}[X]$ の既約元であり，したがって $f(X)$ も $\mathbb{Z}[X]$ の既約元である．[†31]Gauss の補題 2.8.25 より，$f(X)$ は $\mathbb{Q}[X]$ の既約元でもある． □

2.9　中国剰余定理

可換環の剰余環の形は，剰余を互いに素なイデアルについて分解すれば決定できる

一意分解整域上 2.8.16 だけでなく，一般の可換環にも互いに素の概念が定義できる．これは特に単項整域イデアルでは，一意分解整域での定義と同値になるが，より一般の場合はそれより強い（一般に互いに素ならば，一意分解整域の意味でも互いに素である）．すると，イデアルの演算について更なる美しい性質が成り立つ．$A/(I_1 \cdots I_n)$ は，$I_1, \cdots, I_n$ が「互いに素」なとき，分解しても同型である．

2.9.1　互いに素

定義 2.9.1 (coprime).

(1) 可換環 A のイデアル I, J が**互いに素**であるとは，$I + J = A$ が成り立つことをいう．

(2) イデアルの有限列 $I_1, \cdots, I_n$ が互いに素であるとは，$\forall_{1 \leqslant i < j \leqslant n}$ について I_i と I_j が互いに素であることをいう．

補題 2.9.2. A を一意分解整域とし，$a, b \in A \backslash \{0\}$ とする．一般に (1)⇒(2) が成り立ち，A が単項イデアル整域であるとき，(2)⇒(1) も成り立つ．後者の主張を Bézout の補題ともいう．

(1) 2 つのイデアル (a) と (b) が互いに素である．

(2) 2 つの元 a, b は互いに素である（定義 2.8.16）．

[証明].

(1)⇒(2)　(a) と (b) の最大公約イデアル I について，$I = A(= (1))$ を示せば良い．

最大公約イデアルの特徴付け 2.8.19(2) より，$I \subset A$ は $(a) \subset I, (b) \subset I$ を満たす最小の単項分数イデアルであり，定義 2.8.16 より，$(a), (b)$ がいずれも単項イデアルであるから I もイデアルである（(a) も (b) も A の素イデアルの正冪で表さ

[†31] $X \mapsto X + 1$ は $\mathbb{Z}[X]$ の自己同型を定め，整域の自己同型について元の既約性は保たれるため．

れるから，I の素イデアルへの分解も正冪しか現れない）．したがって，$(a)+(b)\subset I$ が必要だが，(a) と (b) が互いに素であることより，これは $A\subset I$ を意味する．

(2)⇒(1)　A は単項イデアル整域であるから，$\exists_{x\in A}\ (a)+(b)=(x)$．すると，特に $(a)+0=(a)\subset(x), 0+(b)=(b)\subset(x)$ より，(x) は $(a),(b)$ を共に含み，かつ，最小のイデアルである（イデアルの表示 2.2.12 より，$\{a,b\}$ で生成されるイデアルは $Aa+Ab=(a)+(b)$ という形をしている）から，最大公約イデアルの特徴付け 2.8.19(2) より，これが (a) と (b) の最大公約イデアルに他ならず，a,b が互いに素という仮定よりこれは A に等しい：$(x)=A$．よって，$(a)+(b)=(x)=A$ を得る．

■

反例 2.9.3. 一般の一意分解整域における (2)⇒(1) の反例は，$F[X,Y]$ における $(X),(Y)$ である．$X,Y\in F[X,Y]$ の最大公約イデアルは $F[X,Y]$ であるから互いに素であるが，$(X)+(Y)=(X,Y)\neq F[X,Y]$ より（$F[X,Y]^\times$ を含まない），2 つのイデアル $(X),(Y)$ は互いに素ではない．

補題 2.9.4 . 可換環 A のイデアル I,J が互いに素であるとき，$IJ=I\cap J$ が成り立つ．

[証明].

$IJ\subset I\cap J$　イデアルの定義より，$IJ\subset I$ かつ $IJ\subset J$ であるから，$IJ\subset I\cap J$ である．

$IJ\supset I\cap J$　任意に $a\in I\cap J$ を取る．I と J が互いに素であるとしたから，$I+J=A$ より，特に $\exists_{x\in I,y\in J}\ x+y=1$．これを用いて，$a=a(x+y)=ax+ay=JI+IJ=IJ$.

■

2.9.2　中国剰余定理

定理 2.9.5 (Chinese remainder theorem). A を可換環とし，$I_1,\cdots,I_n$ を互いに素なイデアルとする．このとき，次が成り立つ．

(1) $I_1\cap\cdots\cap I_n=I_1\cdots I_n$.
(2) $A/I_1\cdots I_n=A/(I_1\cap\cdots\cap I_n)\xrightarrow{\sim}A/I_1\times\cdots\times A/I_n$.

[証明].

(1) $I_1,\cdots,I_n$ が互いに素なイデアルであるという仮定の下で，任意の $1\leqslant i\leqslant n-1$ に対して，I_i と $I_{i+1}\cdots I_n$ が互いに素であることを示せば，補題を繰り返し適用することにより，

$$I_1\cdots I_n=I_1\cap I_2\cdots I_n=I_1\cap I_2\cap I_3\cdots I_n=\cdots=I_1\cap I_2\cap\cdots\cap I_n$$

が従う．

$i<j\leqslant n$ を満たす任意の j に対して，仮定より $I_i+I_j=A$ であるから特に $\exists_{a_j\in I_i,b_j\in I_j}\ a_j+b_j=1$ だから，$\prod_{j=i+1}^{n}(a_j+b_j)=1$. ここで左辺は，$b_{i+1}b_{i+2}\cdots b_n\in I_{i+1}\cdots I_n$ を除いてその他の項は I_i の元だから，$1\in I_i+I_{i+1}\cdots I_n$ となる．よって，$I_i+I_{i+1}\cdots I_n=A$ が従う．

(2) 標準全射 $\pi_i:A\twoheadrightarrow A/I_i\ (i\in[n])$ について，$\pi:=(\pi_1,\cdots,\pi_n):A\to A/I_1\times\cdots\times A/I_n$ が定まる．$\operatorname{Ker}\pi=I_1\cap\cdots\cap I_n$ であるから，π が全射であることを示せば，準同型定理 2.3.11 より $A/(I_1\cap\cdots\cap I_n)\xrightarrow{\sim}\operatorname{Im}\pi=A/I_1\times\cdots\times A/I_n$ が従う．これを帰納法によって示す．

$n=2$ のとき　$(x_1,x_2)\in A/I_1\times A/I_2$ を任意に取る．$y_1\in\pi_1^{-1}(x_1), y_2\in\pi_2^{-1}(x_2)$ を取る．仮定より $I_1+I_2=A$ だから，特に $a+b=1$ を満たす $a\in I_1, b\in I_2$ を取れる．これらに対して $z:=by_1+ay_2$ と定めると，$a\in I_1=\operatorname{Ker}\pi_1, b\in I_2=\operatorname{Ker}\pi_2$ より，

$$\pi_1(z)=\pi_1(by_1+ay_2)=\pi_1(y_1-ay_1+ay_2)=\pi_1(y_1)=x_1,$$
$$\pi_2(z)=\pi_2(by_1+ay_2)=\pi_2(by_1+y_2-by_2)=\pi_2(y_2)=x_2.$$

よって，$z\in\pi^{-1}(x_1,x_2)$.

$n > 2$ **のとき**　帰納法の仮定より，$\pi' := (\pi_2, \cdots, \pi_n) : A \twoheadrightarrow A/I_2 \times \cdots \times A/I_n$ は全射だから，$\overline{\pi'} : A/(I_2 \cap \cdots \cap I_n) \xrightarrow{\sim} A/I_2 \times \cdots \times A/I_n$ を定める．$\pi'' := (\pi_1, \pi_{2\cdots n}) : A \twoheadrightarrow A/I_1 \times A/(I_2 \cdots I_n)$ と定めると，I_1 と $I_2 \cdots I_n$ は互いに素であったから（(1) の証明抽出），$n = 2$ の場合より π'' も全射．

$$A \xrightarrow{\pi''} A/I_1 \times A/(I_2 \cdots I_n) \overset{(1)}{=\!=} A/I_1 \times A/(I_2 \cap \cdots \cap I_n) \xrightarrow[\sim]{\mathrm{id}_{A/I_1} \times \overline{\pi'}} A/I_1 \times A/I_2 \times \cdots \times A/I_n$$

より，$\pi = (\mathrm{id}_{A/I_1} \times \overline{\pi'}) \circ \pi''$ と全射の合成で表せるから，π も全射である．

■

要諦 2.9.6. 互いに素であることの定義って，大体 $a + b = 1$ となるものを選び出すために使うんだね．そしてこれがパズルの極めて肝心なピースとなる．命題 2.8.20 で考察したが，$(a), (b) \subset I$ を満たす I は $Aa + Ab = I$ という表示を持つから，$(a) + (b) = I$ ならば a, b は互いに素である．なお，$(a) + (b) = I$ は $\exists_{x,y \in A}\ ax + by = 1$ と同値（命題 2.8.20）．この逆が言えるかが問題になるが，任意の単項イデアル整域で正しい（これが Bézout の補題）．単項（分数でない）イデアルの最大公約イデアルが再び単項イデアルになるか？という問いの答えは常に真だろうが，単項イデアルの和が単項イデアルになるかは Bézout 整域というクラスを定めるようだ．

注 2.9.7. $\mathbb{Z}/(m_1 \cdots m_r) \simeq \mathbb{Z}/(m_1) \times \cdots \times \mathbb{Z}/(m_r)$ の場合が特に有名である．互いに素な $m_1, \cdots, m_r$ について，それぞれの剰余を指定されれば，$m_1 \cdots m_r$ までの中に対応する数がただ一つ見つかる．

2.9.3　構造決定

例 2.9.8 (多項式の生成するイデアルによる剰余環の構造決定)**.**

$$\mathbb{R}[X]/(X^3 - 1) \simeq \mathbb{R} \times \mathbb{C}$$

である．

(1) $X^3 - 1 = (X - 1)(X^2 + X + 1)$ は既約元分解を与えている．例 2.8.31 より分かるが，$X^2 + X + 1$ が既約でない，したがって一次式の積として書けたとすると，実数解を持つこととなり矛盾する．$\mathbb{C}[X]$ の既約元は一次式のみという主張が代数学の基本定理なのであるな．

(2) $X - 1, X^2 + X + 1$ は同伴でない素元であるから，互いに素である 2.8.20．$\mathbb{R}[X]$ は Euclid 整域 2.7.3 であるから特に単項イデアル整域であること 2.7.4 に注意すると，補題 2.9.2 より，$(X - 1), (X^2 + X + 1)$ も互いに素である．または，$\mathbb{R}[X]$ は Euclid 整域であるから特に $(X - 1) + (X^2 + X + 1) = \mathbb{R}[X]$ に同値であるが，これはたしかに満たされる：$(X + 2)(X - 1) - (X^2 + X + 1) = -3$.

(3) 中国剰余定理 2.9.5 より，

$$\mathbb{R}[X]/(X^3 - 1) = \mathbb{R}[X]/(X - 1)(X^2 + X + 1) \xrightarrow{\sim} \mathbb{R}[X]/(X - 1) \times \mathbb{R}[X]/(X^2 + X + 1).$$

(4) $\mathrm{ev}_1 : \mathbb{R}[X] \twoheadrightarrow \mathbb{R}$ は全射準同型であり，その核はイデアル $(X - 1)$ であるから，準同型定理より $\mathbb{R}[X]/(X - 1) \xrightarrow{\sim} \mathbb{R}$.

(5) $\omega := \dfrac{-1 + \sqrt{3}}{2} \in \mathbb{C}$ について $\mathrm{ev}_\omega : \mathbb{R}[X] \twoheadrightarrow \mathbb{C}$ は全射準同型であり，$\mathrm{Ker}\ \mathrm{ev}_\omega = (X^2 + X + 1)$ である．実際，$\mathrm{Ker}\ \mathrm{ev}_\omega \supset (X^2 + X + 1)$ は分かる．$(X^2 + X + 1)$ は素イデアルであるから，単項イデアル整域 $\mathbb{R}[X]$ の極大イデアルである 2.7.6．よって，$\mathrm{Ker}\ \mathrm{ev}_\omega = (X^2 + X + 1) \vee \mathrm{Ker}\ \mathrm{ev}_\omega = \mathbb{R}[X]$ であるが，後者は $1 = 0$ が必要であるため，$\mathbb{C}$ が零環でないことに矛盾．よって，準同型定理から，$\mathbb{R}[X]/(X^2 + X + 1) \simeq \mathbb{C}$.

□

2.10　体の拡大

体の消息を群論で調べる

Galois 理論とは，F の有限次拡大体 E に対して，$F \subset M \subset E$ を満たす**中間体**を，群論に写し取って記述する理論である．S_n の可解性から n 次方程式の解の公式の存在，また Sylow の定理と p-群の可解性から代数学の基本定理を導く架け橋となる．代数的整数論ではこの架け橋を頻繁に往復する．

定義 2.10.1 .

(1) 体 F を部分環として含む体 E を，F の**拡大体**という．
(2) E は乗法について F-線型空間となる．この時の次元を $[E:F]$ で表し，体拡大 $F \hookrightarrow E$ の**拡大次元**という．
(3) $[E:F] < \infty$ のとき，E は F の**有限次拡大体**という．

定義 2.10.2 . 任意の $f \in F[X] \backslash F$ に対して，$\{a \in F \mid f(a) = 0\} \neq \varnothing$ となるとき，F を**代数閉体**という．

定理 2.10.3 . 任意の F について，F の拡大体であって代数閉体であるものが存在する．

定義 2.10.4 . F を体，$\overline{F}$ を F の拡大体であって代数閉体であるものとする．

(1) $f \in F[X] \backslash F$ が**分離多項式**であるとは，f が $\overline{F}$ において重根を持たないことをいう．
(2) 分離多項式 $f \in F[X] \backslash F$ に対し，根を $\{a \in \overline{F} \mid f(a) = 0\} =: \{\alpha_1, \cdots, \alpha_d\}$ $(d := \deg f)$ と表し，$F_f = F(\alpha_1, \cdots, \alpha_d)$ とおく[†32]．この F_f を f の**分解体**という．
(3) ある分離多項式 $f \in F[X]$ を用いて F_f の形で表せる F の有限次拡大体の F を **Galois 拡大体**という．[†33]

例 2.10.5. $F = \mathbb{Q}, \overline{F} = \mathbb{C}$ とする．

(1) $f(X) = X^2 - 2$ ならば，$\mathbb{Q}_f = \mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$.
(2) $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[4]{2})$ は $\mathbb{Q}$ の有限次拡大体だが，重根を持ってしまうので，Galois 拡大体ではない．

□

定義 2.10.6 . F の Galois 拡大体 E に対して，F 上恒等であるような E の体自己同型からなる集合 $\mathrm{Gal}(E/F) = \{f \in \mathrm{Aut}_{\mathrm{Ring}}(E) \mid \forall_{a \in F}\, f(a) = a\}$ を $F \hookrightarrow E$ の **Galois** 群と呼ぶ．[†34]

定理 2.10.7 (Galois 理論の基本定理). E を F の Galois 拡大体とする．部分群 $H \hookrightarrow \mathrm{Gal}(E/F)$ に対し，$E^H := \{a \in E \mid \forall_{f \in H}\, f(a) = a\}$ とおく．これは $F \subset E$ の中間体である．この構成の定める対応 $H \mapsto E^H$ は，$\mathrm{Gal}(E/F)$ の部分群と $F \subset E$ の中間体の間に全単射を引き起こす．逆写像は $M \mapsto \mathrm{Gal}(E/M)$ で定まる．また，この写像は包含関係を逆転させる単調写像である．

要諦 2.10.8. $\mathrm{Gal}(E/F)$ に対応する中間体は F 自身である：$E^{\mathrm{Gal}(E/F)} = F$.

[†32] F 上で $\alpha_1, \cdots, \alpha_d$ で生成されるような $\overline{F}$ の部分体を表す．これは分数も含むということを意味するが，実は生成される部分環 $F[\alpha_1, \cdots, \alpha_n]$ に一致することも証明できる．
[†33] Galois 理論は Galois 拡大体についてのみ適用可能である．
[†34] $[E:F] = |\mathrm{Gal}(E/F)|$ なので，必ず有限になる．

第 3 章

組み合わせ論

具体例を見るとき特に位数が大事.

3.1 2021 年度期末試験

問題 1

(1) $|Gx| = \dfrac{|G|}{|\mathrm{Stab}_G(x)|}$. Lagrange の定理より $\dfrac{|G|}{|\mathrm{Stab}_G(x)|} = |G/\mathrm{Stab}_G(x)|$ であるから，写像

$$\begin{array}{ccc} \varphi : G/\mathrm{Stab}_G(x) & \longrightarrow & Gx \\ \cup & & \cup \\ g\mathrm{Stab}_G(x) & \longmapsto & gx \end{array}$$

が全単射であることを示せば良い.

(2) S_3 は生成元 $\{\tau := (1\,2), \sigma := (1\,2\,3)\}$ と関係式 $\left\{\sigma^3 = \tau^2 = \tau\sigma\tau\sigma = e\right\}$ によって定まる群であるから, $\left\{(a,b) \in S^4 \times S^4 \mid a^3 = b^2 \right.$ の元の個数を数えれば良い．a は長さ 3 の巡回置換，b は長さ 2 の巡回置換（互換）しかあり得ない．$baba = e$ を満たすためには，b が動かす 2 つの要素がいずれも a に含まれていなければならない．そのようなものは，39 個.

(3) $p = q$ **のとき**　$\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ の部分群は，位数 p^3 のものが 1 つ，p^2 のものが $\langle(1,-)\rangle$ $(- = 0, 1, \cdots, p-1)$ という形の p 個と $p\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, 位数 p のものが $\langle(0,1)\rangle$,$\langle(p,-)\rangle$ という形の $p+1$ 個，位数 1 のものが 1 個で合計 $2p+4$ 個.
$p \neq q$ **のとき**　$\mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ の部分群は，巡回群であることに注意すると単元生成される部分群に注目すればよく，位数 p^2q のものが 1 つ，p^2 のものが $\langle(1,0)\rangle$ の 1 つ，pq のものが $\langle(p,1)\rangle$ の 1 つ，p のものが 1 つ，q のものが 1 つ，1 のものが 1 つなので合計 6 個.

(4) 成り立つ．有限 Abel 群の構造定理より，同型 $f : M \xrightarrow{\sim} \mathbb{Z}/p_1^{m_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{m_r}\mathbb{Z}$ が存在するが，これが $f(N) = \mathbb{Z}/p_1^{m_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{m_s}\mathbb{Z}$ を満たすように取ることができることを示す．N の位数は $p_1^{m_1} \cdots p_s^{m_s}$ であるが，$f(N)$ は上述の形を満たさないとする．すると，ある $1 \leqslant i \leqslant s$ が存在して，位数 $p_i^{m_i}$ の元 $(0, \cdots, 0, 1, 0, \cdots, 0)$ は N に含まれない．これに対応する元 $\overline{(0, \cdots, 0, 1, 0, \cdots)} \in M/N$ の位数は p_i の倍数である．これは矛盾．このとき，同じ同型は $N \times M/N \simeq M$ を引き起こす.

(5) $\mathrm{Im}\ f = \{0, 2, 4, 6\}$ より，$\mathrm{Im}\ f \simeq \mathbb{Z}/4\mathbb{Z}$. $\mathrm{Ker}\ f = \langle(1,3)\rangle$ という巡回群であるから，有限巡回群の基本定理より，$\mathrm{Ker}\ f \simeq \mathbb{Z}/8\mathbb{Z}$.

(6) $\mathbb{C}[X]$ が単項イデアル整域であることとイデアルの対応より，$\mathbb{C}[X]$ のイデアルで $(X^3 + X^2)$ を含むものを考えれば良い．$\mathbb{C}[X]^\times = \mathbb{C}^\times$ が単元で，単元同士で写り合う同伴元は同じイデアルを生成することと同値であることに注意すると，$(X^3 + \alpha X^2 + \beta X + \gamma)$ $(\alpha, \beta, \gamma \in \mathbb{C}, \alpha \neq 1)$ となる．$\mathbb{C}[X]$ は特に一意分解整域で，素元と既約元は一致するから，素イデアルは既約元が生成するイデアルである．$\mathbb{C}[X]$ の既約元は一次式に限る．また，一次式による $\mathbb{C}[X]$ の商は $\mathbb{C}$ に同型だから，極大でもある.

(7) $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in I$ ならば，各

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & d \end{pmatrix}$$

も I に含まれ，また，$(00;10)$ を左からかけることと $(01;00)$ を右からかけることとその両方を考えることより，$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in I$ ならば $\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ a & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix} \in I$ より，$(10;00), (20;00), (30;00)$ のうちいくつかが生成する両側イデアルを考えれば十分．$(10;00), (30;00)$ は $M_2(\mathbb{Z}/4\mathbb{Z})$ を生成し，$(20;00)$ は $M_2(2\mathbb{Z}/4\mathbb{Z})$ を生成する．2 元生成されるイデアルは全て $M_2(\mathbb{Z}/4\mathbb{Z})$.

(8) $\mathbb{F}_7/(X^3-1)$ は，$1, X$ が生成し，関係式 $X^3 = 1$ が定める環である．1 の行き先は 1 だから，あとは X の行き先を定めれば良い．よって，$\{a \in \mathbb{F}_7/(X^4-X^2) \mid a^3 = 1\}$ の元の個数を求めれば良い．中国剰余定理より $\mathbb{F}_7[X]/(X^4-X^2) \simeq \mathbb{F}_7[X]/(X^2) \times \mathbb{F}_7 \times \mathbb{F}_7$ である．$\mathbb{F}_7$ の元で位数が 3 の約数であるのは，$1^3 = 1, 2^3 = 1, 4^3 = 1$．$\mathbb{F}_7[X]/(X^2)$ は，$1, 2, 4$ に加えて，$(X^2 + a)$ $(a = 1, 2, 4)$ の 6 つが存在する．実際，$(X^2 + aX + b)^3 = (X^2) + 3ab^2X + b^3$ より，$a = 0, b = 1, 2, 4$ が必要．以上より，$3^2 \cdot 6 = 54$ 個.

(9) $\mathbb{Z}[X]_{X^2-1} = \{(X^2-1)^m \in \mathbb{Z}[X] \mid m \in \mathbb{N}\}^{-1}\mathbb{Z}[X]$ である．$\mathbb{Z}[X]$ は整域で，$0 \notin \{(X^2-1)^m \in \mathbb{Z}[X] \mid m \in \mathbb{N}\}^{-1}$ より，

$$\frac{f(X)}{(X^2-1)^m}\frac{g(X)}{(X^2-1)^n} = 1 \Leftrightarrow f(X)g(X) = (X+1)^{m+n}(X-1)^{m+n} \quad (m, n \in \mathbb{N}).$$

$\mathbb{Z}[X]$ は一意分解整域だから，$f \in (\mathbb{Z}[X]_{X^2-1})^\times \Leftrightarrow f \in \left\{a(X+1)^i(X-1)^j \in \mathbb{Z}[X]_{X^2-1} \mid a \in \mathbb{Z}^\times, 0 \leqslant i, j \leqslant n+m\right\}$．ここで，

$$\begin{array}{ccc} \varphi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} & \longrightarrow & \mathbb{Z}[X]_{X^2-1} \\ \cup & & \cup \\ (a, i, j) & \longmapsto & (-1)^a(X+1)^i(X-1)^j \end{array}$$

と定めると，これが群準同型写像であることを示す．まず，写像として全単射である．そして，指数法則より $\varphi(a+b, i+i', j+j') = \varphi(a, i, j) \cdot \varphi(b, i', j')$.

(10) まず (6) からのインスピレーションで $\mathbb{R} \times \mathbb{R}$ などが思いつくが，これは整域ではない．$\mathbb{Z} \times \mathbb{Z}$ も整域にはならない.

(11) $6\mathbb{Z}$ を含むイデアルは $2\mathbb{Z}, 3\mathbb{Z}$ の二つであるが，肝心の $\mathbb{Z}/6\mathbb{Z}$ は整域ではない．$0 \notin S$ のとき，整域の局所化は整域であることを使う．$(\mathbb{Z}\backslash 2\mathbb{Z} \cap \mathbb{Z}\backslash 3\mathbb{Z})^{-1}\mathbb{Z}$ は極大イデアルを 2 つもつ．単項イデアル整域の局所化は再び単項イデアル整域であることに注意すると，$(2/1), (3/1)$ は極大イデアルであり，これ以外の素イデアルは存在しないことから極大イデアルは以上の 2 つである.

問題 2

(1) $[(1,1,0,\sigma), (0,0,0,\tau)] = (1,0,1,\sigma^2) \in [G,G]$ や $[(1,1,0,\sigma), (0,0,0,\sigma)] = (1,0,1,e)$ などの観察と対称性より，

$$\underbrace{\{(0,0,0), (1,1,0), (1,0,1), (0,1,1)\}}_{=:B} \rtimes A_3 \subset [G,G].$$

$B \rtimes A_3$ は位数 12 の正規部分群である．これは，この群 G における共役変換は，

$$\begin{aligned} (a,b,c)f(1,1,0)\sigma^i f^{-1}(a,b,c) &= (a,b,c) \cdot f\sigma^i f^{-1} \cdot f\sigma^{2i}(1,1,0) \cdot (a,b,c) \\ &= f\sigma^i f^{-1} \cdot f\sigma^i f^{-1}(a,b,c) \cdot f\sigma^{2i}(1,1,0) \cdot (a,b,c) \end{aligned}$$

となり，第一引数については任意の $(\mathbb{Z}/3\mathbb{Z})^3$ の元自身とその置換とを足す操作となるが，これは 1 の個数の偶奇を変えない操作であることがわかる．また第二引数についても，A_3 が S_3 の正規部分群であることから，$B \rtimes A_3$ は確かに正規である．すると，$G/B \rtimes A_3$ の位数は 4 であるが，位数 4 の群は Abel 群である．よって，$[G,G] \subset B \rtimes A_3$ もわかる．よって，$[G,G] = B \rtimes A_3$.

$G/[G,G]$ は $\{(0,0,0), (1,1,0)\} \rtimes \{e, \tau\}$ と表せて，この群の任意の元の位数は 2 であるから，$G/[G,G] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(2) $|G| = 48$ であるから，G の p-Sylow 部分群の位数は 16．Sylow の定理より，p-Sylow 部分群の個数は 1 または 3 である．いま，$(\mathbb{Z}/3\mathbb{Z})^2 \times \{e, (1,2)\}, (\mathbb{Z}/3\mathbb{Z})^2 \times \{e, (1,3)\}, (\mathbb{Z}/3\mathbb{Z})^2 \times \{e, (2,3)\}$ は部分群を定め，いずれも位数は 16 であるから，これらが p-Sylow 部分群である.

(3) $B \times S_3$ が定める部分群が条件を満たす．これは正規部分群 B をもち，最初の 2 成分への射影によって $B \simeq \mathbb{Z}/2\mathbb{Z}$ である．また，$(B \times S_3)/B \simeq S_3$ である.

要諦 3.1.1 (半直積の計算)**.** $G \rtimes H$ は，任意の元を G の元と H の元の積に分解し，交換法則を見つける方向で対処すると計算がしやすい．そして交換子部分群の計算が一番難しい．生成元に注目することと，正規部分群になることと，割ったら可換になることを使って決定していく．そして半直積と交換子には綺麗な関係がある．$gh = [g,h](hg)$ となる．

問題 3：局所化 $A_{\overline{X}}$ は一意分解整域であるが，本人 A は一意分解整域ではない整域 A.

(1) $\mathbb{C}[X,Y,Z]$ は一意分解整域で，素元と既約元は一致するから，$Z^2 - XY$ が既約であることを示せば良い．$Z^2 - XY \in (\mathbb{C}[X,Y])[Z]$ について Eisenstein の既約判定法より，素イデアル (X) が存在して $-XY \in (X), -XY \notin (X^2)$ を満たすから，これは $(\mathbb{C}[X,Y])[Z]$ の既約元，したがって $\mathbb{C}[X,Y,Z]$ の既約元である．

(2) $A_{\overline{X}} \simeq \mathbb{C}[X,Y,Z]_X/(Z^2-XY)_X \simeq (\mathbb{C}[X,Z]_X)[Y]/(X^{-1}Z^2 - Y)$．ここで，評価写像 $\mathrm{ev}_{Z^2/X} : (\mathbb{C}[X,Y]_X)[Y] \to \mathbb{C}[X,Z]_X$ を考えると，$\mathrm{Ker}\ \mathrm{ev}_{Z^2/X} = (Z^2 - XY)_X$．準同型定理より，$(\mathbb{C}[X,Z]_X)[Y]/(X^{-1}Z^2 - Y) \simeq \mathbb{C}[X,Z]_X \simeq (\mathbb{C}[X]_X)[Z]$．$\mathbb{C}[X]$ は一意分解整域だから $\mathbb{C}[X]_X$ も一意分解整域．よって，$A_{\overline{X}} \simeq (\mathbb{C}[X]_X)[Z]$ も一意分解整域である．
これより，$(A_{\overline{X}})^\times = \overline{\mathbb{C}[X]_X \backslash \{0\}}$．$\overline{X}^{-1} \notin A$ なので，$(A_{\overline{X}})^\times \cap A = \overline{\mathbb{C}[X]\backslash\{0\}}$．$A$ は $\overline{X}$ の逆元を持たないことは，$\mathbb{C}[X,Y,Z]$ に引き戻して考えると $Z^2 - XY$ が既約元であることからわかる．

(3) $\overline{Z} \in A_{\overline{X}}$ は，一変数多項式環の元と同一視できるので，既約元である．$\overline{Z} = fg$ $(f,g \in A)$ と表せると仮定する．このとき，$f \in (A_{\overline{X}})^\times \cap A$ または $g \in (A_{\overline{X}})^\times \cap A$ である．$f \in \overline{\mathbb{C}[X]\backslash\{0\}}$ として一般性を失わない．しかし，(X) の元は可逆でないから，$Z = fg$ に矛盾するため，$f \in \mathbb{C}^\times$．特に，$f \in A^\times$．
$A/(\overline{Z})$ が整域でないことを示せば良い．$\overline{XY} = \overline{Z}^2 \in A$ であるが，$X, Y \neq 0$ かつ $XY = 0 \in A/(\overline{Z})$．よって，$A/(\overline{Z})$ は整域ではない．

3.2　群の演習問題

(1) $\mathbb{R}$ の affine 変換群は群になる．

(2) Möbius 群の確認．

(3) 右の単位元と右の逆元の存在と結合律を仮定する $gg' = e, ge = g$ だけで，g の右単位元 g' の右単位元を g'' とすると，

$$g'g = g'g(g'g'') = g'g'' = e$$

より，$g = g''$ を得る．したがって，右逆元と左逆元は一致．すると，$eg = gg'g = ge = g$ より左単位元と右単位元も一致する．

(4) G に無限位数の群があるとき，部分群の特徴付け $SS \subset S$ は必要十分ではない．

(5) 1.3.15

(6) $\mathbb{R}$ を群と呼ぶときは加法群だから，自明でない有限部分群はない．なるほど！半直積だ．行列の群も半直積に分解できれば，交換条件も整理され，随分簡単になるのではないか？

(7) (7)

(8) やはり群の決定は位数から攻めるんだな．

(9) (9)

(10) $\mathrm{SL}_2(\mathbb{Z})$ は $(11;01), (01;-10)$ の二元で生成される．証明は極めて組み合わせ論的．

3.2.1　準同型の決定

命題 3.2.1 . 群準同型 $f : G \to H$ の，$g \in G$ の値 $f(g) \in H$ の位数は g の位数の約数である．

参考文献

[1] Reinhard Diestel "Graph Theory" 5th ed. (2016).
[2] Chris Godsil and Gordon Royle (2001), Algebraic Graph Theory, Springer.
[3] Michael "Toposes, Triples and Theories" (Springer, 1983).