第 3 章

代数学のあれこれ

この章では，主に代数学に関する内容を雑多にまとめる．詳細は [?] や，加群については [?] を参照されるのが良いと思う．

まず，部分群の定義と判定法を書いておく：

定義 3.1: 部分群

$(G, \cdot, 1_G)$ を群とする．部分集合 $H \subset G$ が G の**部分群** (subgroup) であるとは，H が演算 $\cdot$ によって群になることを言う．

命題 3.1: 部分群であることの判定法

群 G の部分集合 H が G の部分群になるための必要十分条件は，以下の 3 条件が満たされることである：

(SG1) $1_G \in H$

(SG2) $x, y \in H \implies x \cdot y \in H$

(SG3) $x \in H \implies x^{-1} \in H$

群の生成を定義しておく：

定義 3.2: word

$(G, \cdot, 1_G)$ を群，$S \subset G$ を部分集合とする．

S の有限部分集合 $\{x_1, \dots, x_n\} \subset S$ によって

$$x_1^{\pm 1} \cdot x_2^{\pm 1} \cdots x_n^{\pm 1} \qquad \text{w/} \quad x_i^{\pm 1} \text{ は } x_i \text{ か } x_i^{-1} \text{ のどちらでも良い}$$

と書かれる G の元を **S の元による語** (word) と呼ぶ．ただし $n = 0$ のときは単位元 1_G を表すものとする．

命題 3.2: 部分加群の生成

S の元による word 全体の集合を $\langle S \rangle$ と書く．

(1) $\langle S \rangle$ は G の部分群である．これを **S によって生成された部分群**と呼び，S のことを**生成系** (generator)，S の元を**生成元**と呼ぶ．

(2) G の部分群 H が $S \subset H$ を充たすならば $\langle S \rangle \subset H$ である．i.e. $\langle S \rangle$ は S を含む最小の部分群である．

証明 (1) 命題 3.1 の 3 条件を充していることを確認する．$x_1, \ldots, x_n, y_1, \ldots, y_m \in S$ とする．

(SG1) $n = 0$ の場合から $1_G \in \langle S \rangle$

(SG2) $x_1, \ldots, x_n, y_1, \ldots, y_m \in S$ とする．

$$(x_1^{\pm 1} \cdots x_n^{\pm 1}) \cdot (y_1^{\pm 1} \cdots y_m^{\pm 1}) = x_1^{\pm 1} \cdots x_n^{\pm 1} \cdot y_1^{\pm 1} \cdots y_m^{\pm 1} \in \langle S \rangle$$

(SG3) 複号同順で

$$(x_1^{\pm 1} \cdots x_n^{\pm 1}) \cdot (x_n^{\mp 1} \cdots x_1^{\mp 1}) = 1_G$$

かつ $x_n^{\mp 1} \cdots x_1^{\mp 1} \in \langle S \rangle$ なので良い．

(2) $1_G \in H$ なので $n = 0$ のときは良い．$n > 0$ として $x_1, \ldots, x_n \in S$ を任意にとると，仮定より $x_1, \ldots, x_n \in H$ である．故に命題 3.1 から $x_1^{\pm 1}, \ldots, x_n^{\pm 1} \in H$ であり，H が席について閉じていることから $x_1^{\pm 1} \cdots x_n^{\pm 1} \in H$ である．i.e. $\langle S \rangle \subset H$.

■

定義 3.3: 巡回群

G を群とする．一つの元 $x \in G$ で生成される群 $\langle x \rangle$ を**巡回群** (cyclic group) と言う．G の部分群であって，巡回群でもあるものを**巡回部分群**と呼ぶ．

3.1 群の準同型

3.1.1 定義

定義 3.4: 群準同型

$(G_1, \cdot, 1_{G_1})$, $(G_2, *, 1_{G_2})$ を群とする．写像 $\phi\colon G_1 \to G_2$ が（群の）**準同型写像** (homomorphism) であるとは，

$$\phi(x \cdot y) = \phi(x) * \phi(y), \quad \forall x, y \in G_1$$

が成り立つことを言う．

ϕ が準同型写像であって逆写像 ϕ^{-1} を持ち，かつ ϕ^{-1} もまた準同型写像であるとき，ϕ は**同型写像** (isomorphism) と呼ばれる．このとき G_1, G_2 は同型 (isomorphic) であるといい，$G_1 \cong G_2$ と書く．

いちいち群の演算を明記するのは大変なので，以降では余程紛らわしくない限り省略する．

命題 3.3:

$\phi\colon G_1 \to G_2$ を群の準同型とするとき，以下が成立する：

(1) $\phi(1_{G_1}) = 1_{G_2}$
(2) $\phi(x^{-1}) = \phi(x)^{-1}, \quad \forall x \in G_1$

証明　(1) $\phi(1_{G_1}) = \phi(1_{G_1}1_{G_1}) = \phi(1_{G_1})\phi(1_{G_1})$ より $\phi(1_{G_1}) = 1_{G_2}$
(2) (1) より $\phi(1_{G_1}) = \phi(x^{-1}x) = \phi(x^{-1})\phi(x) = 1_{G_2}$

■

標語的には「準同型写像 $\phi\colon G_1 \to G_2$ は群の演算，単位元，逆元の全てを保つ」ということになる．特に ϕ が全単射である，i.e. 同型写像であるならば，G_1 と G_2 の群論的な性質は同じである．この意味で G_1 と G_2 は同一視できる．

3.1.2　核と像

定義 3.5: 準同型の核・像

G_1, G_2 を群，$\phi\colon G_1 \to G_2$ を準同型写像とする．

(1) ϕ の**核** (kernel) $\operatorname{Ker}\phi \subset G_1$ を次のように定義する：

$$\operatorname{Ker}\phi := \left\{ x \in G_1 \,\middle|\, \phi(x) = 1_{G_2} \right\}$$

(2) ϕ の**像** (image) $\operatorname{Im}\phi \subset G_2$ を次のように定義する：

$$\operatorname{Im}\phi := \left\{ \phi(x) \,\middle|\, x \in G_1 \right\}$$

命題 3.4:

G_1, G_2 を群，$\phi\colon G_1 \to G_2$ を準同型写像とする．このとき $\operatorname{Ker}\phi$, $\operatorname{Im}\phi$ はそれぞれ G_1, G_2 の部分群である．

証明　命題 3.1 の 3 条件を充していることを確認すれば良い．

(SG1)　命題 3.3-(1) より $1_{G_1} \in \operatorname{Ker}\phi$, $1_{G_2} \in \operatorname{Im}\phi$
(SG2)　$\operatorname{Ker}\phi$ に関しては

$$\begin{aligned} x,\, y \in \operatorname{Ker}\phi \quad &\Longrightarrow \quad \phi(xy) = \phi(x)\phi(y) = 1_{G_2}1_{G_2} = 1_{G_2} \\ &\Longrightarrow \quad xy \in \operatorname{Ker}\phi \end{aligned}$$

よりよい．
$\operatorname{Im}\phi$ に関しては ϕ が準同型であることから自明．

(SG3) $\mathrm{Ker}\,\phi$ に関しては命題 3.3-(2) から

$$\begin{aligned} x \in \mathrm{Ker}\,\phi &\implies \phi(x^{-1}) = \phi(x)^{-1} = 1_{G_2}^{-1} = 1_{G_2} \\ &\implies x^{-1} \in \mathrm{Ker}\,\phi \end{aligned}$$

よりよい．

$\mathrm{Im}\,\phi$ に関しても命題 3.3-(2) から

$$\begin{aligned} y \in \mathrm{Im}\,\phi &\implies \exists x \in G_1,\ y = \phi(x) \\ &\implies y^{-1} = \phi(x)^{-1} = \phi(x^{-1}) \\ &\implies y^{-1} \in \mathrm{Im}\,\phi \end{aligned}$$

ただし，3 行目で G_1 が群であるために $x \in G_1 \implies x^{-1} \in G_1$ であることを使った．

■

命題 3.4 より，$\mathrm{Ker}\,\phi$ や $\mathrm{Im}\,\phi$ による剰余類を考えることができる．

命題 3.5: 準同型の単射性判定

準同型写像 $\phi\colon G_1 \to G_2$ に対して以下が成立する：

$$\phi\ \text{が単射} \iff \mathrm{Ker}\,\phi = \{1_{G_1}\}$$

<u>**証明**</u> $(\implies)$ ϕ は単射と仮定する．命題 3.3-(1) より $1_{G_1} \in \mathrm{Ker}\,\phi$ である．このとき $\forall x \in G_1$ に対して

$$x \in \mathrm{Ker}\,\phi \implies \phi(x) = 1_{G_2} = \phi(1_{G_1})$$

であり，仮定から $x = 1_{G_1}$ とわかる．

$(\impliedby)$ $\mathrm{Ker}\,\phi = \{1_{G_1}\}$ と仮定する．このとき $\forall x, y \in G_1$ に対して

$$\begin{aligned} \phi(x) = \phi(y) &\implies \phi(xy^{-1}) = \phi(x)\phi(y)^{-1} = \phi(x)\phi(x)^{-1} = 1_{G_2} \\ &\implies xy^{-1} \in \mathrm{Ker}\,\phi \end{aligned}$$

が成立し，仮定より $xy^{-1} = 1_{G_1}$ とわかる．故に $x = y$ であり，$\phi(x) = \phi(y) \implies x = y$ が示された． ■

3.1.3 剰余類

群 G の部分群 H は G 上の同値関係を誘導する：

命題 3.6: 部分群による同値関係

群 $(G, \cdot, 1_G)$ の部分群 $(H, \cdot, 1_H)$ を与える．このとき，次のようにして定義される集合 $\sim_{\mathrm{L}}, \sim_{\mathrm{R}} \subset G \times G$ は同値関係である[a]：

$$\begin{aligned} \sim_{\mathrm{L}} &:= \left\{ (x, y) \in G \times G \,\middle|\, x^{-1}y \in H \right\} \\ \sim_{\mathrm{R}} &:= \left\{ (x, y) \in G \times G \,\middle|\, yx^{-1} \in H \right\} \end{aligned}$$

[a] 群 G は可換とは限らない!

証明 同値関係の公理??を充していることを確認すればよい．ほぼ同じ議論なので，$\sim_{\mathrm{L}}$ についてのみ示す．

(1) 命題 3.1-(1) より $x^{-1}x = 1_G = 1_H \in H$ であるから $x \sim_{\mathrm{L}} x$.

(2) 命題 3.1-(3) より部分群 H は逆元をとる操作について閉じている．故に

$$\begin{aligned} x \sim_{\mathrm{L}} y &\implies x^{-1}y \in H \\ &\implies y^{-1}x = (x^{-1}y)^{-1} \in H \\ &\implies y \sim_{\mathrm{L}} x. \end{aligned}$$

(3) 命題 3.1-(2) より部分群 H は演算 $\cdot$ について閉じている．故に

$$\begin{aligned} x \sim_{\mathrm{L}} y \quad \text{かつ} \quad y \sim_{\mathrm{L}} z &\implies x^{-1}y \in H \quad \text{かつ} \quad y^{-1}z \in H \\ &\implies x^{-1}z = x^{-1}(yy^{-1})z = (x^{-1}y)(y^{-1}z) \in H \\ &\implies x \sim_{\mathrm{L}} z. \end{aligned}$$

■

つまり，同値関係 $\sim_{\mathrm{L}}$, $\sim_{\mathrm{R}}$ の気持ちは

- 反射律 $\leftrightarrow$ 単位元
- 対称律 $\leftrightarrow$ 逆元をとる操作
- 推移律 $\leftrightarrow$ 群の演算

という対応を定式化したものと言える．

さて，集合 G の上に同値関係ができたので同値類を考えることができる：

定義 3.6: 剰余類

群 $(G, \cdot, 1_G)$ の部分群 $(H, \cdot, 1_H)$ を与える．

(1) G 上の同値関係 $\sim_{\mathrm{L}}$ による $x \in G$ の同値類を**左剰余類** (left coset) と呼び，xH と書く．あからさまには以下の通り：

$$xH := \{ y \in G \mid x^{-1}y \in H \}$$

同値関係 $\sim_{\mathrm{L}}$ による G の商集合を $\boldsymbol{G/H}$ と書く：

$$\boldsymbol{G/H} := G/\sim_{\mathrm{L}} \ = \{ xH \mid x \in G \}$$

(2) G 上の同値関係 $\sim_{\mathrm{R}}$ による $x \in G$ の同値類を**右剰余類** (right coset) と呼び，Hx と書く．あからさまには以下の通り：

$$Hx := \{ y \in G \mid yx^{-1} \in H \}$$

同値関係 $\sim_{\mathrm{R}}$ による G の商集合を $\boldsymbol{H\backslash G}$ と書く：

$$\boldsymbol{H\backslash G} := G/\sim_{\mathrm{R}} \ = \{ Hx \mid x \in G \}$$

左/右剰余類は H が G の部分群ならば**必ず**作ことができる．

命題 3.7: 剰余類の位数

H が G の部分群ならば以下が成り立つ（位数は ∞ でも良い）：

(1) $|G/H| = |H\backslash G|$
(2) $|xH| = |Hx| = |H|, \quad \forall x \in G$

証明 (1) 集合の濃度が等しいことを示すには，G/H から $H\backslash G$ への全単射が存在することを示せば良い．

写像 $\alpha\colon G/H \to H\backslash G$ を $\alpha(xH) := Hx^{-1}$ と定義する．α が well-defined であることを示す．実際，$\forall x \in G$ を一つ固定したとき xH の勝手な元は xh $(h \in H)$ と書かれるが，$(xh)^{-1} = h^{-1}x^{-1} \in Hx^{-1}$ なので，写像 α の xH への作用は xH の代表元の取り方によらない．i.e. α は well-defined である．

同様な議論から，写像 $\beta\colon H\backslash G \to G/H$ を $\beta(Hx) := x^{-1}H$ として定義すると β も well-defined であることがわかる．このとき $(\beta\circ\alpha)(xH) = \beta(Hx^{-1}) = xH$, $(\alpha\circ\beta)(Hx) = Hx$ が成立するので $\beta\circ\alpha = \mathrm{id}_{G/H}$，$\alpha\circ\beta = \mathrm{id}_{H\backslash G}$ であり，α, β は両方とも全単射である．

(2) 写像 $\phi\colon H \to xH$ を $\phi(h) := xh$ と定義する．このとき，$\forall h_1, h_2 \in H$ に対して

$$\phi(h_1) = \phi(h_2) \implies xh_1 = xh_2 \implies h_1 = x^{-1}xh_1 = x^{-1}xh_2 = h_2$$

が成立するので ϕ は単射である．ϕ が全射であることは明らかなので全単射である．故に $|xH| = |H|$. $|Hg| = |H|$ も同様に示される．

■

同値類全体の集合は商集合を非交和 (disjoint union) に分割することを考えると，次の定理が即座に従う：

定理 3.1: Lagrange の定理

集合 G/H, $H\backslash G$ の濃度を $\boldsymbol{(G : H)}$ と書く[a]と，

$$|G| = (G : H)|H|.$$

[a] G における H の**指数** (index) と呼ぶ．

3.1.4 両側剰余類

命題 3.8:

群 $(G, \cdot, 1_G)$ およびその部分群 $(H, \cdot, 1_H)$, $(K, \cdot\ 1_K)$ を与える．このとき，次のようにして定義される集合 $\sim_{\mathrm{D}} \subset G\times G$ は同値関係である：

$$\sim_{\mathrm{D}} := \left\{\, (x, y) \;\middle|\; \exists h \in H,\, \exists k \in K,\; x = h\cdot y\cdot k \,\right\}$$

証明 同値関係の公理??を充していることを確認すればよい．ほぼ同じ議論なので，$\sim_{\mathrm{L}}$ についてのみ示す．

(1) 命題 3.1-(1) より $1_G = 1_H = 1_K$ であるから $x = 1_H x 1_K$.

(2) 命題 3.1-(3) より部分群は逆元をとる操作について閉じている．故に

$$\begin{aligned} x \sim_{\mathrm{D}} y &\implies \exists h \in H,\ \exists k \in K,\ x = hyk \\ &\implies \quad y = h^{-1} x k^{-1} \\ &\implies \quad y \sim_{\mathrm{D}} x. \end{aligned}$$

(3) 命題 3.1-(2) より部分群は演算 $\cdot$ について閉じている．故に

$$\begin{aligned} x \sim_{\mathrm{D}} y \quad \text{かつ} \quad y \sim_{\mathrm{D}} z &\implies \exists h_1,\ h_2 \in H,\ \exists k_1,\ k_2 \in K,\ x = h_1 y k_1 \ \text{かつ}\ y = h_2 z k_2 \\ &\implies \quad x = (h_1 h_2) z (k_2 k_1) \\ &\implies \quad x \sim_{\mathrm{D}} z. \end{aligned}$$

■

定義 3.7: 両側剰余類

命題 3.8 において，同値関係 $\sim_{\mathrm{D}}$ による G の商集合 $G/\sim_{\mathrm{D}}$ を $\boldsymbol{H\backslash G/K}$ と書く．$H\backslash G/K$ の元を $H,\ K$ による**両側剰余類** (double coset) と呼ぶ．$x \in G$ の両側剰余類をあからさまに書くと以下の通り：

$$HxK = \left\{ hxk \;\middle|\; h \in H,\ k \in K \right\}$$

3.1.5 正規部分群

定義 3.6 において右剰余類と左剰余類を定義したが，補題 3.1 より部分群 H が正規部分群ならば両者は一致する．そしてこのとき商集合 G/H と $H\backslash G$ が同一視され，自然に群構造が入る．

定義 3.8: 正規部分群

H を G の部分群とする．H が G の**正規部分群** (normal subgroup) であるとは，$\forall g \in G,\ \forall h \in H$ に対して $ghg^{-1} \in H$ であることを言い[a]，記号として $H \lhd G$，あるいは $G \rhd H$ と書く．

[a] このことを H は**内部自己同型** (inner automorphism) の下で不変だ，とか言う

命題 3.9: Ker は正規部分群

G_1, G_2 を群，$\phi\colon G_1 \to G_2$ を準同型写像とすると，$\operatorname{Ker}\phi \lhd G_1$ である．

<u>**証明**</u> $\forall g \in G_1,\ h \in \operatorname{Ker}\phi$ に対して

$$\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g^{-1}) = \phi(g)\phi(g)^{-1} = 1_{G_2}$$

なので $ghg^{-1} \in \operatorname{Ker}\phi$ である．i.e. $\operatorname{Ker}\phi \lhd G_1$ である． ■

補題 3.1:

群 G およびその部分群 N を与える．このとき以下が成り立つ：

$$N \lhd G \iff \forall g \in G,\ gN = Ng$$

証明 ($\Longrightarrow$)

- ($\subset$)　$\forall x \in gN$ を一つとると，ある $n \in N$ が存在して $x = gn$ と書ける．仮定より $N \lhd G$ だから $gng^{-1} \in N$ である．ゆえに

$$x = gn = gn(g^{-1}g) = (gng^{-1})g \in Ng.$$

  $x \in gN$ は任意だったから $gN \subset Ng$.
- ($\supset$)　g を g^{-1} に置き換えて同じ議論をすれば良い．

($\Longleftarrow$)　$\forall g \in G,\ \forall n \in N$ をとる．仮定より $\exists n' \in N,\ gn = n'g$ が言える．従って

$$gng^{-1} = n'gg^{-1} = n' \in N.$$

■

定理 3.2: 剰余群

群 G とその正規部分群 N を与える．このとき，左剰余類による商集合（定義 3.6）G/N 上の二項演算 $\cdot : G/N \times G/N \to G/N$ を

$$gN \cdot hN := (gh)N \tag{3.1.1}$$

と定義するとこれは well-defined であり，かつ $\boldsymbol{(G/N, \cdot, N)}$ **は群を成す**．この群を G の N による**剰余群** (quotient group) と呼ぶ．

証明 **well-definedness**

要するに式 (3.1.1) の右辺が引数 gN, hN の代表元の取り方によらずに定まることを示せば良い．$\forall g, h \in G$ を固定する．このとき左剰余類 gN, hN の勝手な元 $x \in gN, y \in hN$ は $x = gn,\ y = hn'$ $(n, n' \in N)$ と書ける．故に

$$xy = (gn)(hn') = g(hh^{-1})nhn' = (gh)(h^{-1}nh)n'$$

だが，**N が G の正規部分群であることにより** $h^{-1}nh \in N$ が言える．よって $xy \in (gh)N$ であり，式 (3.1.1) の右辺が gN, hN の代表元の取り方によらないことが示された．

群であること

演算 $\cdot$ の well-definedness が示されたので，後は群の公理を充していることを確認すれば良い．

単位元　G/N の任意の元は gN の形をしている．このとき

$$gN \cdot N = N \cdot gN = (g1_G)N = gN$$

なので $1_{G/N} = N$ である．

結合則　G/N の任意の元を 3 つとってきて，それらを $gN,\ hN,\ kN\ (g,\ h,\ k \in G)$ と書く．このとき

$$gN \cdot (hN \cdot kN) = gN \cdot (hk)N = (ghk)N = \bigl((gh)k\bigr)N = (gh)N \cdot kN = (gN \cdot hN) \cdot kN$$

なので良い．

逆元　G/N の任意の元を 1 つとってきてそれを $gN\ (g \in G)$ と書く．このとき $g^{-1} \in G$ なので $g^{-1}N \in G/N$ であり，

$$gN \cdot g^{-1}N = (gg^{-1})N = N = 1_{G/N}$$

とわかる．i.e. $(gN)^{-1} = g^{-1}N$ である．

■

系 3.3: 標準射影と剰余群

群 G とその正規部分群 N を与える．このとき標準射影（定義??）$\pi\colon G \to G/N,\ g \mapsto gN$ は $\boldsymbol{G/N}$ **を剰余群だと思うと全射準同型写像になる**．また，$\mathrm{Ker}\,\pi = N$ である．

証明 $\mathrm{Im}\,\pi = G/N$ は π の定義から明らか．

剰余群 G/N の積の定義 (3.1.1) より

$$\pi(gh) = (gh)N = gN \cdot hN = \pi(g) \cdot \pi(h)$$

であり，π は準同型である．

剰余群 G/N の単位元は N なので，$\forall g \in G$ に対して $\pi(g) = gN = 1_{G/N} \iff g \in N$． ■

系 3.3 より，標準射影 $\pi\colon G \twoheadrightarrow G/N$ のことを**自然な全射準同型**と呼ぶ場合がある．

3.1.6　直積・半直積

部分群の「割り算」を定義できたので，ついでに「積」も定義しておこう．まず群 G の**部分集合**の積が自然に定まることを見る．以下の定義 3.9 は**部分群を作っているわけではないので注意**.

定義 3.9: 群 G の部分集合の積

$S_1,\ S_2$ を群 $(G,\ \cdot\ ,\ 1_G)$ の部分集合とする[a]．集合

$$S_1S_2 \coloneqq \left\{\, x \cdot y \;\middle|\; x \in S_1,\ y \in S_2 \,\right\}$$

を部分集合の**積**と呼ぶ.

[a] 部分群ではない！

命題 3.10: 部分集合の積が部分群になる必要十分条件

群 $(G,\, \cdot\,,\, 1_G)$ とその部分群 $H_1,\, H_2$ を与える．このとき，以下が成り立つ：

(1) $H_1H_2 \subset G$ が G の部分群 $\iff$ $H_1H_2 = H_2H_1$
(2) $H_1 \lhd G$ かつ $H_2 \lhd G$ $\implies$ $H_1H_2 \lhd G$

証明 (1) ($\implies$) H_1H_2 が G の部分群であると仮定する．H_1H_2 の勝手な元は $x = h_1h_2$ $(h_i \in H_i)$ と書ける．このとき仮定より $x^{-1} \in H_1H_2$ だが，H_i が部分群なので

$$x^{-1} = h_2^{-1}h_1^{-1} \in H_2H_1$$

でもある．よって $H_1H_2 = H_2H_1$.
($\impliedby$) $H_1H_2 = H_2H_1$ と仮定する．命題 3.1 の 2 条件を充していることを確認する．

(SG1) H_i が部分群なので $1_G = 1_G1_G \in H_1H_2$.

(SG2) H_1H_2 の勝手な 2 つの元は $h_1h_2,\, k_1k_2$ $(h_i,\, k_i \in H_i)$ と書ける．仮定より $\exists h_1' \in H_1,\, \exists k_2' \in H_2,\ h_2k_1 = h_1'k_2'$ が成立するから，

$$(h_1h_2)(k_1k_2) = h_1(h_2k_1)k_2 = (h_1h_1')(k_2'k_2) \in H_1H_2.$$

(SG3) $h_1h_2 \in H_1H_2$ を任意にとる．仮定から $\exists k_1' \in H_1,\, \exists k_2' \in H_2,\ h_2^{-1}h_1^{-1} = k_1'k_2'$ が成立するから

$$(h_1h_2)^{-1} = h_1'h_2' \in H_1H_2.$$

(2) 仮定と補題 3.1 より $\forall g \in G$ に対して $gH_2 = H_2g$ である．故に

$$H_1H_2 = \bigcup_{h_1 \in H_1} h_1H_2 = \bigcup_{h_1 \in H_1} H_2h_1 = H_2H_1.$$

よって (1) から H_1H_2 は G の部分群である．
$h_1h_2 \in H_1H_2$ を任意にとる．仮定より $\forall g \in G$ に対して $gh_ig^{-1} \in H_i$ である．

$$g(h_1h_2)g^{-1} = (gh_1g^{-1})(gh_2g^{-1}) \in H_1H_2.$$

i.e. $H_1H_2 \lhd G$.

■

次に，群の直積集合を群にする方法を定める．

定義 3.10: 群の直積

- $G_1,\, G_2$ を群とする．直積集合 $G_1 \times G_2$ に以下のように二項演算 $\cdot : G_1 \times G_2 \to G_1 \times G_2$ を定義すれば，$\bigl(G_1 \times G_2,\, \cdot\,,\, (1_{G_1},\, 1_{G_2})\bigr)$ は群になる：

$$(g_1,\, g_2) \cdot (h_1,\, h_2) := (g_1h_1,\, g_2h_2)$$

-

証明 **結合律** $G_1,\, G_2$ それぞれの結合則から明らか．

単位元　$\forall(g_1,\, g_2) \in G_1 \times G_2$ に対して

$$(g_1,\, g_2)\cdot(1_{G_1},\, 1_{G_2}) = (g_1,\, g_2) = (1_{G_1},\, 1_{G_2})\cdot(g_1,\, g_2)$$

逆元　$\forall(g_1,\, g_2) \in G_1 \times G_2$ に対して

$$(g_1,\, g_2)\cdot(g_1^{-1},\, g_2^{-1}) = (1_{G_1},\, 1_{G_2}) = 1_{G_1\times G_2}$$

i.e. $(g_1,\, g_2)^{-1} = (g_1^{-1},\, g_2^{-1})$ である．

■

命題 3.11: 群の直積の特徴付け

(1) G_1, G_2 を群とし，包含写像 $\iota_i\colon G_i \hookrightarrow G_1 \times G_2 \quad (i = 1,\, 2)$ を

$$\iota_1(g_1) := (g_1,\, 1_{G_2}), \quad \iota_2(g_2) := (1_{G_1},\, g_2)$$

と定義する．このとき $\iota_1(G_1)$ の元と $\iota_2(G_2)$ の元は互いに可換であり，$\iota_i(G_i) \triangleleft G_1 \times G_2$ が成り立つ．

(2) G を群，$H, K \subset G$ を部分群とする．このとき $H \triangleleft G$ かつ $K \triangleleft G$ かつ $H \cap K = \{1_G\}$ かつ $HK = G$ ならば $G \cong H \times K$ である．

証明　(1) 可換であることは

$$(g_1,\, 1_{G_2})(1_{G_1},\, g_2) = (g_1,\, g_2) = (1_{G_1},\, g_2)(g_1,\, 1_{G_2})$$

より従う．

$\forall g_1 \in G_1,\ \forall(h_1,\, h_2) \in G_1 \times G_2$ をとる．

$$(h_1,\, h_2)\iota_1(g_1)(h_1,\, h_2)^{-1} = (h_1 g_1 h_1^{-1},\, 1_{G_2}) \in \iota_1(G_1)$$

なので $\iota_1(G_1) \triangleleft G_1 \times G_2$ である．全く同様にして $\iota_2(G_2) \triangleleft G_1 \times G_2$ もわかる．

(2) 写像 $\phi\colon H \times K \to G$ を

$$\phi\big((h,\, k)\big) := hk$$

と定義する．仮定より $G = HK$ だから（部分集合の積）ϕ は全射．

まず $\forall h \in H, \forall k \in K$ に対して $hk = kh$ であることを示す．

$$hk(kh)^{-1} = (hkh^{-1})k^{-1} = h(kh^{-1}k^{-1})$$

だが，仮定より $K, H \triangleleft G$ なので $hkh^{-1} \in K$，$kh^{-1}k^{-1} \in H$ であり，$hk(kh)^{-1} \in K \cap H = \{1_G\}$ が言える．i.e. $hk = kh$.

従って $\forall(h,\, k), (h',\, k') \in H \times K$ に対して

$$\phi\big((h,\, k)\big)\phi\big((h',\, k')\big) = h(kh')k' = h(h'k)k' = (hh')(kk') = \phi\big((h,\, k)\cdot(h',\, k')\big)$$

が成り立つから ϕ は群の準同型である．また，

$$(h,\, k) \in \operatorname{Ker}\phi \quad\Longrightarrow\quad hk = 1_G \quad\Longrightarrow\quad h = k^{-1} \in H \cap K = \{1_G\}$$

だから $\operatorname{Ker}\phi = \{1_G\}$ であり，命題 3.5 から ϕ は単射．よって ϕ は同型写像である．

■

最後に群の半直積を定義しておこう．

定義 3.11: 外部半直積

$N,\ H$ を群とし，$\phi\colon H \to \mathrm{Aut}\,N,\ h \mapsto \phi_h$ を準同型写像とする[a]．このとき，集合 $N \times H$ は次の二項演算 $\cdot : N \times H \to N \times H$ に関して群を成す：

$$(n_1,\ h_1) \cdot (n_2,\ h_2) \coloneqq \big(n_1 \phi_{h_1}(n_2),\ h_1 h_2\big)$$

この群 $\big(N \times H,\ \cdot\ ,\ (1_N,\ 1_H)\big)$ のことを $N,\ H$ の（外部）**半直積** (semidirect product) と呼び，$\boldsymbol{H \ltimes_\phi N}$ または $\boldsymbol{N \rtimes_\phi H}$ と書く．

[a] $\mathrm{Aut}\,N$ は，N から N 自身への同型写像全体の集合に，写像の合成を群の演算として群構造を入れたもので，**自己同型群** (automorphism group) と呼ばれる．

証明 **結合律**　$\phi\colon H \to \mathrm{Aut}\,N$ は準同型写像であるから $\phi_{h_1 h_2} = \phi(h_1 h_2) = \phi(h_1) \circ \phi(h_2) = \phi_{h_1} \circ \phi_{h_2}$ である．

$$\begin{aligned}
\big((n_1,\ h_1) \cdot (n_2,\ h_2)\big) \cdot (n_3,\ h_3) &= \Big(n_1 \phi_{h_1}(n_2) \phi_{h_1 h_2}(n_3),\ h_1 h_2 h_3\Big) \\
&= \Big(n_1 \phi_{h_1}(n_2) \phi_{h_1}\big(\phi_{h_2}(n_3)\big),\ h_1 h_2 h_3\Big) \\
&= \Big(n_1 \phi_{h_1}\big(n_2 \phi_{h_2}(n_3)\big),\ h_1 (h_2 h_3)\Big) \\
&= (n_1,\ h_1) \cdot \big(n_2 \phi_{h_2}(n_3),\ h_2 h_3\big) \\
&= (n_1,\ h_1) \cdot \Big((n_2,\ h_2) \cdot (n_3,\ h_3)\Big)
\end{aligned}$$

単位元　$\phi\colon H \to \mathrm{Aut}\,N$ は準同型写像であるから $\phi_{1_H} = \mathrm{id}_N$ である．故に $\forall n \in N,\ \forall h \in H$ に対して

$$(n,\ h) \cdot (1_N,\ 1_H) = (n \phi_h(1_N),\ h 1_H) = (n,\ h) = (1_N \phi_{1_H}(n),\ 1_H h) = (1_N,\ 1_H) \cdot (n,\ h)$$

逆元　$\phi\colon H \to \mathrm{Aut}\,N$ は準同型写像であるから，命題 3.4 より $\phi_{h^{-1}} = \phi(h^{-1}) = \phi(h)^{-1} = \phi_h^{-1}$ である．故に $\forall n \in N,\ \forall h \in H$ に対して

$$\begin{aligned}
(n,\ h) \cdot \big(\phi_{h^{-1}}(n^{-1}),\ h^{-1}\big) &= \Big(n \phi_h\big(\phi_{h^{-1}}(n^{-1})\big),\ 1_H\Big) = (n n^{-1},\ 1_H) = 1_{N \rtimes_\phi H} \\
\big(\phi_{h^{-1}}(n^{-1}),\ h^{-1}\big) \cdot (n,\ h) &= \Big(\phi_{h^{-1}}(n^{-1}) \phi_{h^{-1}}(n),\ 1_H\Big) = (\phi_{h^{-1}}(n)^{-1} \phi_{h^{-1}}(n),\ 1_H) = 1_{N \rtimes_\phi H}
\end{aligned}$$

i.e. $\boldsymbol{(n,\ h)^{-1} = \big(\phi_{h^{-1}}(n^{-1}),\ h^{-1}\big)}$.

■

3.1.7　準同型定理

群の準同型写像 $\phi\colon G \to H$ が与えられると，命題 3.9 より $\mathrm{Ker}\,\phi \lhd G$ であるから $G/\mathrm{Ker}\,\phi$ は剰余群 3.2 になる．そして系 3.3 により，G と $G/\mathrm{Ker}\,\phi$ は自然に全射準同型 π で結ばれることもわかる．では，群 $G/\mathrm{Ker}\,\phi$ と群 H の関係はどうなっているのだろうか？

定理 3.4: 準同型定理 (第一同型定理)

群の準同型写像 $\phi\colon G \to H$ を与える．$\pi\colon G \to G/\operatorname{Ker}\phi$ を自然な準同型とする．このとき，図 3.1 が可換図式となるような準同型 $\psi\colon G/\operatorname{Ker}\phi \to H$ がただ一つ存在し，$\psi\colon G/\operatorname{Ker}\phi \to \operatorname{Im}\phi$ は同型写像になる．

$$\begin{tikzcd} G \arrow[r, "\phi"] \arrow[d, two heads, "\pi"] & H \\ G/\operatorname{Ker}\phi \arrow[ur, dashed, "\exists!\psi"'] & \end{tikzcd}$$

図 3.1: 準同型定理

<u>**証明**</u> $N = \operatorname{Ker}\phi$ とおく．$\forall g \in G$ に対して

$$\psi(gN) \coloneqq \phi(g) \tag{3.1.2}$$

と定義する．

$\forall x \in gN$ はある $n \in N = \operatorname{Ker}\phi$ を使って $x = gn$ と書くことができるから

$$\psi(xN) = \phi(x) = \phi(gn) = \phi(g)\phi(n) = \phi(g)1_G = \psi(gN)$$

が成立する．i.e. (3.1.2) によって定義される写像 $\psi\colon G/N \to H$ は well-defined である．

ψ は準同型写像で，図 3.1 は可換図式である

$\forall g, h \in G$ に対して

$$\psi\big((gN)(hN)\big) = \psi\big((gh)N\big) = \phi(gh) = \phi(g)\phi(h) = \psi(gN)\psi(hN)$$

であるから ψ は準同型写像.

また，定義 (3.1.2) から明らかに写像の等式として $\psi \circ \pi = \phi$ が成り立つ．i.e. 図 3.1 は可換図式である．

ψ は単射である

$\forall g \in G$ に対して

$$\psi(gN) = 1_H \quad \Longrightarrow \quad \phi(g) = 1_H \quad \Longleftrightarrow \quad g \in \operatorname{Ker}\phi = N$$

なので $\operatorname{Ker}\psi = \{N\}$ とわかる．$N = 1_{G/N}$ なので，命題 3.4 から ψ は単射である．

$\operatorname{Im}\psi = \operatorname{Im}\phi$ である

$\forall g \in G$ に対して $\phi(g) = \psi(gN)$ なので $\operatorname{Im}\phi \subset \operatorname{Im}\psi$．$G/N$ の勝手な元は $gN \quad (g \in G)$ の形をしているので $\psi(gN) = \phi(g)$ であり，$\operatorname{Im}\psi \subset \operatorname{Im}\phi$ とわかる．よって $\operatorname{Im}\psi = \operatorname{Im}\phi$ である．ψ は単射だから $\psi\colon G/N \to \operatorname{Im}\phi$ は全単射であり，$G/N \cong \operatorname{Im}\phi$ が言える．

ψ は一意的に定まる

図 3.1 が可換図式であるとき，i.e. $\psi \circ \pi = \phi$ が成り立つとき，$\forall x = gN \in G/N$ に対して $\psi(x) = \psi(gN) = (\psi \circ \pi)(g) = \phi(g)$ として値が定まり，定義 (3.1.2) と一致する．従って ψ は一意に定まる．

■

定理 3.5: 準同型定理 (第二同型定理)

G を群，H を G の部分群，N を G の正規部分群とするとき，次が成り立つ：

(1) $H \cap N \lhd H$

(2) $\boldsymbol{HN/N \cong H/H \cap N}$

証明 写像 $\phi\colon H \to HN/N,\ h \mapsto hN/N$ は剰余群への自然な全射準同型と同様に well-defined な準同型写像である．

$\forall y \in HN/N$ に対して

$$\exists h \in H, \exists n \in N,\ y = (hn)N = hN = \phi(h)$$

が成立するから $\operatorname{Im}\phi = HN/N$ である．また，$h \in H$ に対して

$$\phi(h) = 1_{HN/N} \quad \Longleftrightarrow \quad hN = N \quad \Longrightarrow \quad h \in H \cap N$$

だから $\operatorname{Ker}\phi = H \cap N$ である．

(1) 命題 $prop.ker_group - 1$ より $H \cap N \lhd H$ である．

(2) 準同型定理（第一同型定理）3.17 より，ϕ によって $HN/N \cong H/H \cap N$ である．

■

定理 3.6: 準同型定理 (第三同型定理)

G を群，$N \subset M$ を G の正規部分群とするとき，次が成り立つ：

$$\boldsymbol{(G/N)/(M/N) \cong G/M}$$

証明 $\forall x \in G, \forall y \in N$ をとる．$N \subset M$ なので $(xy)M = xM$ である．従って，写像 $\phi\colon G/N \to G/M$ を

$$\phi(xN) := xM$$

とおくと ϕ は well-defined な準同型写像である．

また，$x \in G$ に対して

$$\phi(xN) = 1_{G/M} \quad \Longleftrightarrow \quad xM = M \quad \Longrightarrow \quad x \in M$$

だから $\operatorname{Ker}\phi = M/N$ である．よって準同型定理（第一同型定理）3.17 を使うことで $(G/N)/(M/N) \cong G/M$ がわかる． ■

3.2 群の作用

定義 3.12: 群の作用

G を群，X を集合とする．

- G の X への**左作用** (left action) とは写像

$$\phi\colon G \times X \to X,\ (g,\, x) \mapsto \phi(g,\, x)$$

であって以下の性質を充たすものを言う：

(1) $\phi(1_G,\, x) = x$

(2) $\phi\bigl(g,\, \phi(h,\, x)\bigr) = \phi(gh,\, x)$

- G の X への**右作用** (right action) とは写像

$$\phi\colon X \times G \to X,\ (x,\, g) \mapsto \phi(x,\, g)$$

であって以下の性質を充たすものを言う：

(1) $\phi(x,\, 1_G) = x$

(2) $\phi\bigl(\phi(x,\, h),\, g\bigr) = \phi(hg,\, x)$

! よく左作用 ϕ は $g \cdot x,\ gx \coloneqq \phi(g,\, x)$ と略記される．右作用 ϕ は $x \cdot g,\ xg,\ x^g \coloneqq \phi(g,\, x)$ などと略記される．

命題 3.12:

群 G が集合 X に左（右）から作用するとする．$\forall g \in G$ を一つ固定すると，写像

$$\alpha\colon X \to X,\ x \mapsto g \cdot x$$

は全単射になる．

証明 **左作用**　$\forall x \in X$ に対して $y \coloneqq g \cdot x$ とおく．

$$g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = 1_G \cdot x = x = g^{-1} \cdot y$$

なので写像 $\beta\colon X \to X,\ x \mapsto g^{-1} \cdot x$ が α の逆写像である．

右作用　左作用のときとほぼ同様に $y \coloneqq x \cdot g$ とおくと，

$$(x \cdot g) \cdot g^{-1} = x \cdot (gg^{-1}) = x \cdot 1_G = y \cdot g^{-1}$$

であることから，α^{-1} の逆写像の存在が示される．

■

3.2.1 種々の作用

定義 3.13: 剰余群への自然な作用

H を群 G の部分群とする．このとき $\forall g, \forall xH \in G/H$ に対して

$$g \cdot (xH) \coloneqq (gx)H \tag{3.2.1}$$

と定義すれば G の G/H への左作用が得られる．これを ***G* の *G/H* への自然な作用**と呼ぶ.
同様に $\forall g, \forall Hx \in H\backslash G$ に対して

$$(Hx) \cdot g \coloneqq H(xg)$$

と定義すれば G の $H\backslash G$ への右作用が得られる．これも自然な作用と呼ぶ.

証明 well-definedness を確認する．実際 xH の勝手な元 y は $h \in H$ を使って $y = xh$ と書かれるから

$$gy = gxh \in (gx)H$$

であり，式 (3.2.1) の右辺は剰余類 xH の代表元の取り方によらない．右作用に関しても同様である． ■

定義 3.14: 随伴作用

G を群とし，$\forall g \in G$ をとる．このとき，写像 $\mathrm{Ad}(g)\colon G \to G$ を

$$\mathrm{Ad}(g)(h) \coloneqq ghg^{-1}, \quad \forall h \in G$$

と定義すれば，$\mathrm{Ad}\colon G \times G \to G$ は G の G 自身への左作用になる．これを**随伴作用**[a] (adjoint action) と呼ぶ.

[a] **共役作用** (conjugation) とも言う.

証明 定義 3.12 の 2 条件を充していることを確認する.

(1) $\mathrm{Ad}(1_G)(h) = h$ より明らか.
(2) $\forall g_1, g_2 \in G$ に対して

$$\mathrm{Ad}(g_1g_2)(h) = (g_1g_2)h(g_1g_2)^{-1} = g_1(g_2hg_2^{-1})g_1^{-1} = \mathrm{Ad}(g_1)\bigl(\mathrm{Ad}(g_2)(h)\bigr)$$

よりよい.

■

3.2.2 群の作用に関する諸定義

以下，断らなければ作用は左作用であるとする.

定義 3.15: 軌道，等質空間，安定化群

群 G が集合 X に作用するとする．

(1) $x \in X$ に対して，集合 $\boldsymbol{G \cdot x} := \left\{ g \cdot x \;\middle|\; g \in G \right\}$ を x の G による**軌道** (orbit) と呼ぶ．
(2) $x \in X$ に対して，集合 $\boldsymbol{G_x} := \left\{ g \in G \;\middle|\; g \cdot x = x \right\}$ を x の**安定化群** (stabilizer subgroup) と呼ぶ．
(3) $\exists x \in X,\ G \cdot x = X$ であるとき，この作用は**推移的**[a] (transitive) であると言う．このとき X は G の**等質空間** (homogeneous space) であると言う．
(4) $\forall x \in X,\ G_x = \{1_G\}$ であるとき，この作用は**自由**[b] (free) であると言う．
(5) $\exists x \in X,\ G_x = \{1_G\}$ であるとき，この作用は**効果的**[c] (effective) であると言う．

---

[a] **可移**と言うこともある．
[b] **半正則** (semiregular) とも言う．
[c] **忠実** (faithful) とも言う．

命題 3.13:

群 G が X に作用するとする．$\forall x \in X$ を一つ固定する．このとき写像

$$\alpha \colon G/G_x \to G \cdot x,\ gG_x \mapsto g \cdot x$$

は全単射である．従って

$$|G \cdot x| = (G : G_x).$$

証明 gG_x の勝手な元 h は $g_1 \in G_x$ を用いて $h = gg_1$ と書かれるから $h \cdot x = (gg_1) \cdot x = g \cdot (g_1 \cdot x) = g \cdot x$ であり，α は well-defined である．

$\forall g_1, g_2 \in G$ をとる．

$$\begin{aligned} g_1 \cdot x = g_2 \cdot x \quad &\Longleftrightarrow \quad (g_2^{-1} g_1) \cdot x = x \\ &\Longleftrightarrow \quad g_2^{-1} g_1 \in G_x \\ &\Longleftrightarrow \quad g_1 \in g_2 G_x \\ &\Longrightarrow \quad g_1 G_x = g_2 G_x \end{aligned}$$

だから α は単射である．全射性は明らか． ■

定義 3.16: 正規化群，中心化群

H を群 G の部分群とする．

(1) G の部分群 $\mathrm{N}_G(H) := \left\{ g \in G \;\middle|\; gHg^{-1} = H \right\}$ を H の**正規化群** (normalizer) と呼ぶ．
(2) G の部分群 $\mathrm{Z}_G(H) := \left\{ g \in G \;\middle|\; \forall h \in H,\ gh = hg \right\}$ を H の**中心化群** (centralizer) と呼ぶ．
(3) $\mathrm{Z}(G) := \mathrm{Z}_G(G)$ を G の**中心** (center) と呼ぶ．

定義 3.17: 共役類

群 G の元 x, y に対して

$$\exists g \in G,\ y = gxg^{-1}$$

が成り立つとき，x と y は**共役**であると言う[a]．x と共役である元全体の集合を $C(x)$ と書き，**共役類** (conjugacy class) と呼ぶ．

[a] 共役は明らかに同値関係である．

3.3 環

公理 3.1: 環の公理

- R を集合とする．**環** (ring) とは，R と写像

$$+: R \times R \to R,\ (a, b) \mapsto a + b$$
$$\cdot: R \times R \to R,\ (a, b) \mapsto a \cdot b$$

  の組 $(R, +, \cdot)$ であって，$\forall a, b, c \in R$ に対して以下を充たすもののことを言う：
  (R1) $(R, +, 0)$ は可換群である
  (R2) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
  (R3) $a \cdot (b + c) = a \cdot b + a \cdot c, \quad (a + b) \cdot c = a \cdot c + b \cdot c$
  (R4) $\exists 1 \in R,\ a \cdot 1 = 1 \cdot a = a$
  (R2)-(R4) は，R が乗法 $\cdot$ に関してモノイドであることを意味する．
- 環 $(R, +, \cdot)$ が以下の条件を充たすとき，R を**可換環** (commutative ring) という：
  (R5) $a \cdot b = b \cdot a$
- 可換環 $(R, +, \cdot)$ において，$\forall a \in R \setminus \{0\}$ が乗法 $\cdot$ に関して逆元を持つとき，R は**体** (field) と呼ばれる．

定義 3.18: 単元

環 $(R, +, \cdot)$ を与える．

- $a \in R$ が乗法 $\cdot$ に関して逆元を持つとき，a は**可逆元**または**単元**と呼ばれる．
- R の単元全体の集合を $\boldsymbol{R^\times}$ と書く．組 $(R^\times, \cdot, 1_R)$ を R の**乗法群**という．

! **(R4)** を除いたものを環と呼ぶ流儀もある．このときは，**(R1)-(R4)** を充たすものを**単位元を持つ環** (unital ring, ring with unity) と呼ぶ．
さらに珍しい（古い？）が，**(R1)**, **(R3)** のみを環の公理とする場合もある．これが Lie「環」と呼ばれる所以である．

定義 3.19: 環の準同型・同型

$(R_1, +, \cdot\,)$, $(R_2, +, *\,)$ を環とする．

- 写像 $\phi\colon R_1 \to R_2$ が以下の条件を充たすとき，ϕ は環の**準同型写像** (homomorphism) と呼ばれる：
  (1) $\phi(x+y) = \phi(x) + \phi(y)$
  (2) $\phi(x \cdot y) = \phi(x) * \phi(y)$
  (3) $\phi(1_{R_1}) = 1_{R_2}$
- $\phi\colon R_1 \to R_2$ が環の準同型写像で逆写像 ϕ^{-1} を持ち，ϕ^{-1} もまた環の準同型写像であるとき，ϕ は**同型写像** (isomorphism) であると言う．このことを記号として $\boldsymbol{R_1 \cong R_2}$ と書く．

いちいち $(R, +, \cdot\,)$ と書くのは面倒なので，以下では環 R と略記する．

定義 3.20: 整域・零因子

R を零環でない**可換環**とする．

(1) R が**整域** (domain) であるとは，次が成立することを言う：

$$\forall a, b \in R \setminus \{0\},\ ab \neq 0$$

(2) $a \in R$ が以下の条件を充たすとき，a は**零因子** (zero-divisor) であると言う：

$$\exists b \in R \setminus \{0\},\ ab = 0$$

i.e. R が整域であるとは，零因子が 0 のみであること．

3.3.1 部分環

定義 3.21: 部分環

R を環とする．R の部分集合 S が R の加法と乗法により環になり，かつ $1_R \in S$ ならば，S を R の**部分環** (subring)，R を S の**拡大環**と呼ぶ．

命題 3.14: 部分環の判定

R を環，$S \subset R$ を部分集合とする．S が部分環であるための必要十分条件は，次の条件が成り立つことである：

(SR1) S は加法に関して部分群である
(SR2) $a, b \in S \implies ab \in S$
(SR3) $1_R \in S$

命題 3.15: 整域の部分環は整域

R が整域，S が R の部分環ならば，S も整域である．

証明 $a, b \in S \setminus \{0\}$ ならば a, b は R の元としても 0 でない．故に R は整域だから R の元として $ab \neq 0$ である．部分環 S は R と加法逆元 0 および乗法を共有するから，S の元としても $ab \neq 0$ である．i.e. S は整域である． ■

定義 3.22: 核・像

$\phi\colon R_1 \to R_2$ を環の準同型写像とする．

(1) ϕ の**核** (kernel) を次のように定義する：

$$\operatorname{Ker}\phi := \left\{\, x \in R_1 \;\middle|\; \phi(x) = 0_{R_2} \,\right\} \subset R_1$$

$\operatorname{Ker}\phi$ は R_1 のイデアルであり，かつ $\operatorname{Ker}\phi \neq A$ である．

(2) ϕ の**像** (image) を次のように定義する：

$$\operatorname{Im}\phi := \left\{\, \phi(x) \;\middle|\; x \in R_1 \,\right\} \subset R_2$$

$\operatorname{Im}\phi$ は R_2 の部分環である．

証明 (1) ϕ は加法準同型なので，命題 3.4 から $\operatorname{Ker}\phi$ は R_1 の加法部分群である．
ここで $a \in R, x \in \operatorname{Ker}\phi$ を任意にとると

$$\phi(ax) = \phi(a)\phi(x) = \phi(a)0_{R_2} = 0_{R_2}$$

なので $ax \in \operatorname{Ker}\phi$ である．以上より $\operatorname{Ker}\phi$ は R_1 のイデアルである．
また，$\phi(1_{R_1}) = 1_{R_2} \neq 0_{R_2}$ なので $1_{R_1} \notin \operatorname{Ker}\phi$ である．よって $\operatorname{Ker}\phi \neq A$.

(2) 命題 3.14 の 3 条件を確認する．

(SR1) ϕ は加法準同型なので，命題 3.4 から $\operatorname{Im}\phi$ は加法部分群.

(SR2)

$$a, b \in \operatorname{Im}\phi \implies \exists x, y \in R_1,\ a = \phi(x), b = \phi(y) \implies ab = \phi(x)\phi(y) = \phi(xy) \in \operatorname{Im}\phi$$

(SR3) ϕ の定義から明らか.

■

命題 3.16: 環準同型の単射性判定

環準同型写像 $\phi\colon R_1 \to R_2$ に対して以下が成立する：

$$\phi \text{ が単射} \iff \operatorname{Ker}\phi = \{0_{R_1}\}$$

証明 ($\Longrightarrow$) ϕ が単射であるとする．命題 3.3-(1) より $0_{R_1} \in \operatorname{Ker}\phi$ だから，仮定より

$$x \in \operatorname{Ker}\phi \implies \phi(x) = \phi(0_{R_1}) = 0_{R_2} \implies x = 0_{R_1}$$

$(\Longleftarrow)$ $\operatorname{Ker}\phi = \{0_{R_1}\}$ とする．このとき命題 3.3-(2) より，$\forall x, y \in R_1$ に対して

$$\begin{aligned}\phi(x) = \phi(y) &\implies \phi(x) - \phi(y) = \phi(x) + \phi(-y) = \phi(x-y) = 0_{R_2} \\ &\implies x - y \in \operatorname{Ker}\phi \implies x = y\end{aligned}$$

i.e. ϕ は単射. ■

3.3.2 イデアル

環において正規部分群に対応するものがイデアルである．

定義 3.23: イデアル

R を環，I を R の部分集合とする．

(1) I が以下を充たすとき，I は**左イデアル** (left ideal) と呼ばれる：
 (a) I は R の加法部分群
 (b) $\forall a \in R, \forall x \in I,\ ax \in I$

(2) I が以下を充たすとき，I は**右イデアル** (right ideal) と呼ばれる：
 (a) I は R の加法部分群
 (b) $\forall a \in R, \forall x \in I,\ xa \in I$

I が左イデアルかつ右イデアルのとき，**両側イデアル** (two-sided ideal) と言う．R が可換環のときは左右の区別はなく，単に**イデアル** (ideal) と言う．

$\{0\}$, R は明らかに両側イデアルである．これらを**自明なイデアル**と呼ぶ．

定義 3.24: イデアルの生成

R を環とする．

- 任意の添字集合 Λ を与える．部分集合 $S := \{s_\lambda\}_{\lambda\in\Lambda} \subset R$ を含む最小の左イデアル

$$\left\{ \sum_{\lambda\in\Lambda} a_\lambda s_\lambda \;\middle|\; a_\lambda \in R,\ \substack{\text{有限個の添字 } i_1, \dots, i_n \text{ を除いた} \\ \text{全ての添字 } \lambda\in\Lambda \text{ について } a_\lambda = 0} \right\}$$

 は $\boldsymbol{S}$ **で生成された** $\boldsymbol{R}$ **の左イデアル**と呼ばれ，記号として $\sum_{\lambda\in\Lambda} Rs_\lambda$ と書かれる．

- S を含む最小の右イデアル

$$\left\{ \sum_{\lambda\in\Lambda} s_\lambda a_\lambda \;\middle|\; a_\lambda \in R,\ \substack{\text{有限個の添字 } i_1, \dots, i_n \text{ を除いた} \\ \text{全ての添字 } \lambda\in\Lambda \text{ について } a_\lambda = 0} \right\}$$

 は $\boldsymbol{S}$ **で生成された** $\boldsymbol{R}$ **の右イデアル**と呼ばれ，記号として $\sum_{\lambda\in\Lambda} s_\lambda R$ と書かれる．

- S を含む最小の両側イデアル

$$\left\{ \sum_{\lambda\in\Lambda} a_\lambda s_\lambda b_\lambda \;\middle|\; a_\lambda,\, b_\lambda \in R,\ \substack{\text{有限個の添字 } i_1,\dots,i_n \text{ を除いた} \\ \text{全ての添字 } \lambda\in\Lambda \text{ について } a_\lambda=0} \right\}$$

は S **で生成された** R **の両側イデアル**と呼ばれ，記号として $\sum_{\lambda\in\Lambda} Rs_\lambda R$ と書かれる．

- $\Lambda = \{1, \dots, n\}$ のとき，S の生成する最小の左（resp. 右，両側）イデアルは $\boldsymbol{Rs_1 + \cdots + Rs_n}$ (resp. $\boldsymbol{s_1R + \cdots + s_nR}$, $\boldsymbol{(s_1, \dots, s_n)}$) と書かれる．特に R が可換環の場合，これは[a]**有限生成なイデアル** (finitly generated ideal) と呼ばれる．
- 1 つの元 $s \in R$ で生成される可換環 R のイデアルを**単項イデアル** (principal ideal) と言い，$\boldsymbol{(s)}$ と書く．

[a] もちろん，R が可換環ならば左・右・両側イデアルの定義は互いに同値である．この場合，有限生成なイデアルの記号として $(s_1, \dots, s_n)$ を使うことが多いように思う．

定義 3.25: イデアルの和・積

R を環，$I, J \subset R$ を左（右）イデアルとする．

(1) I, J の**和**を次のように定義する：

$$I + J := \left\{ x + y \;\middle|\; x \in I,\, y \in J \right\}$$

$I + J$ は左（右）イデアルである．

(2) I, J の**積**を次のように定義する：

$$IJ := \left\{ x_1y_1 + \cdots + x_ny_n \;\middle|\; n \in \mathbb{N},\ x_i \in I,\, y_i \in J \right\}$$

IJ は左（右）イデアルである．

定理 3.7: 剰余環

環 R とその自明でない両側イデアル I を与える．このとき，加法に関する剰余類[a]全体の集合 R/I の上の 2 つの二項演算 $+, \cdot\colon R/I \times R/I \to R/I$ を

$$(x + I) + (y + I) := (x + y) + I$$
$$(x + I) \cdot (y + I) := (xy) + I$$

と定義するとこれらは well-defined であり，かつ $\boldsymbol{(R/I, +, \cdot)}$ **は環を成す．**この環を R の I による**剰余環** (quotient ring) と言う．

[a] $+$ に関して可換群なので，左・右剰余類の区別はない．

! R が可換環ならば，その剰余環も可換環になる．

証明 加法に関する well-definedness および可換群であることは，定理 3.2 より即座に従う．

well-definedness　乗法に関して示す．

剰余類剰余類 $x+I$, $y+I$ の勝手な元は $x' = x + a$, , $y' = y + b$ $(a, b \in I)$ とかける．故に

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

であるが，*I が R の両側イデアルであることにより* xb, ay, $ab \in I$ が言える．従って $x'y' \in (xy) + I$ であり，乗法の定義は剰余類の代表元の取り方に依らない．

環であること　環の公理を充していることを確認すれば良い．

- **(R1)**　定理 3.2 より従う．零元 $0_{R/I} = I$ である．
- **(R2)**　R の結合律より従う．
- **(R3)**　R の分配律より従う．
- **(R4)**　乗法単位元は $1_{R/I} = 1 + I$ である．

■

系 3.8: 剰余環への自然な全射準同型

環 R とその両側イデアル I を与える．このとき標準射影（定義??）$\pi\colon R \to R/I$, $x \mapsto x + I$ は $\boldsymbol{R/I}$ **を剰余環と見做すと全射準同型写像になる**．また，$\operatorname{Ker}\pi = I$ である．π のことを**自然な全射準同型**と呼ぶ．

証明　加法 $+$ に関しては剰余群の全射準同型の場合と同様．後は定義 3.19-(2), (3) の成立を確かめれば良い．

剰余環の乗法の定義より，$\forall x, y \in R$ に対して

$$\pi(xy) = (xy) + I = (x+I)\cdot(y+I) = \pi(x)\cdot\pi(y)$$

だから乗法を保存する．乗法単位元に関しては

$$\pi(1_R) = 1_R + I = 1_{R/I}.$$

従って π は環の準同型である．■

定義 3.26: 単項イデアル整域

任意のイデアルが単項イデアルである整域を**単項イデアル整域** (principal ideal domain; PID) と呼ぶ．

3.3.3　準同型定理

定理 3.9: 環の準同型定理 (第一同型定理)

環の準同型写像 $\phi\colon R \to S$ を与える．$\pi\colon R \to R/\operatorname{Ker}\phi$ を自然な準同型とする．このとき，図 3.1 が可換図式となるような準同型 $\psi\colon R/\operatorname{Ker}\phi \to S$ がただ一つ存在し，$\psi\colon R/\operatorname{Ker}\phi \to \operatorname{Im}\phi$ は同型写像になる．

$$\begin{tikzcd} R \arrow[r, "\phi"] \arrow[d, "\pi"] & S \\ R/\operatorname{Ker}\phi \arrow[ur, dashed, "\exists!\psi"'] & \end{tikzcd}$$

図 3.2: 環の準同型定理

証明 群の準同型定理により，ψ が加法群の準同型として一意的に存在し，$\operatorname{Im}\phi$ への加法群の同型となる．よって環の準同型の定義から，後は ψ が積を保つことを示せば良い．

$I \coloneqq \operatorname{Ker}\phi$ とおく．R/I の勝手な 2 つの元は $x+I,\, y+I$ $(x,\, y \in R)$ と書ける．$\phi = \psi \circ \pi$ は環の準同型なので，

$$\psi(x+I)\psi(y+I) = \big(\psi \circ \pi(x)\big)\big(\psi \circ \pi(y)\big) = \phi(x)\phi(y) = \phi(xy) = \psi(xy+I).$$

従って，ψ は環の準同型． ■

定理 3.10: 環の準同型定理 (第三同型定理)

R を環，$I \subset J$ を自明でない両側イデアルとするとき，次が成り立つ：

(1) 環の準同型 $\phi\colon R/I \to R/J$ であって，$\phi(x+I) = x+J$ となるものが存在する．

(2) $\boldsymbol{(R/I)/(J/I) \cong R/J}$

3.3.4 環の直積

定義 3.27: 環の直積

$R_1,\, \dots,\, R_n$ を環とする．直積集合 $R \coloneqq R_1 \times \cdots \times R_n$ の上に加法 $+\colon R \times R \to R$ と乗法 $\cdot\colon R \times R \to R$ を次のように定めると，組 $(R,\, +,\, \cdot\,)$ は環になる．この環を $R_1,\, \dots,\, R_n$ の**直積**と呼ぶ：

$$\begin{aligned}(a_1,\, \dots,\, a_n) + (b_1,\, \dots,\, b_n) &\coloneqq (a_1+b_1,\, \dots,\, a_n+b_n), \\ (a_1,\, \dots,\, a_n) \cdot (b_1,\, \dots,\, b_n) &\coloneqq (a_1b_1,\, \dots,\, a_nb_n)\end{aligned}$$

3.3.5 中国式剰余定理

定理 3.11: 中国式剰余定理

$m,\, n \neq 0$ が互いに素な整数ならば以下が成り立つ：

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

証明 写像 $\phi\colon \mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ を

$$\phi(x+mn\mathbb{Z}) \coloneqq (x+m\mathbb{Z},\, x+n\mathbb{Z})$$

と定義する．明らかに ϕ は環の準同型写像である．

well-definedness

$\forall y \in x + mn\mathbb{Z}$ は $a \in \mathbb{Z}$ を使って $y = x + mna$ と書ける．従って $y \in x + m\mathbb{Z}$ かつ $y \in x + n\mathbb{Z}$ であり，ϕ の定義は剰余類 $x + mn\mathbb{Z}$ の代表元の取り方によらない．

ϕ は全単射

$|\mathbb{Z}/mn\mathbb{Z}| = |\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}| = mn < \infty$ だから，補題??より ϕ が全射であることを示せば十分．$\forall (x + m\mathbb{Z},\, y + n\mathbb{Z}) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ をとる．仮定より m, n が互いに素なので，$\mathbb{Z}$ が単項イデアル整域であることから $ma + nb = 1$ を充たす $a, b \in \mathbb{Z}$ が存在する．従って $z := may + nbx$ とおくと，

$$z = may + (1 - ma)x = x + ma(y - x) = (1 - nb)y + nbx = y + nb(x - y)$$

が成立する．i.e. $z \in x + m\mathbb{Z}$ かつ $z \in y + n\mathbb{Z}$ であり，

$$(x + m\mathbb{Z},\, y + n\mathbb{Z}) = \phi(z + mn\mathbb{Z}) \in \operatorname{Im}\phi$$

が言えた．

■

系 3.12: 古典的な中国式剰余定理

$m, n \neq 0$ を互いに素な整数とする．$ma + nb = 1$ を充たす整数 $a, b \in \mathbb{Z}$ をとる．このとき $\forall x, y \in \mathbb{Z}$ に対して $\boldsymbol{z := may + nbx}$ とおけば，

$$\begin{aligned} z &\equiv x \mod m, \\ z &\equiv y \mod n \end{aligned}$$

が成り立つ．

証明 定理 3.11 の証明から即座に従う． ■

より一般化すると次のようになる：

定理 3.13: 可換環における中国式剰余定理

R を可換環，$I_1, \dots, I_n \subsetneq R$ を両側イデアルとする．イデアルの和に関して

$$i \neq j \quad \Longrightarrow \quad I_i + I_j = R$$

が充たされている[a]とき，以下が成立する：

(1) $1 \leq \forall i \leq n,\ I_i + \prod_{j \neq i} I_j = R$

(2) $I_1 \cap \cdots \cap I_n = \prod_{i=1}^{n} I_j$

(3) $\boldsymbol{R/(I_1 \cap \cdots \cap I_n) \cong R/I_1 \times \cdots \times R/I_n}$

[a] このことを，イデアル $I_1, \dots, I_n$ は互いに素であると言う．

証明　(1) $i=1$ とする．$I_1+(I_2I_3\cdots I_n)$ は R のイデアルだから，$I_1+(I_2I_3\cdots I_n)\supset R$ を示せばよい．仮定より $2\leq\forall i\leq n$ に対して

$$\exists x_i\in I_1,\,\exists y_i\in I_i,\ x_i+y_i=1$$

である．このとき

$$(x_2+y_2)(x_3+y_3)\cdots(x_n+y_n)=1$$

であるが，左辺を展開すると $y_2y_3\cdots y_n\in I_2I_3\cdots I_n$ かつそれ以外の項は I_1 の元である．よって $1\in I_1+(I_2I_3\cdots I_n)$ であるが，イデアルの定義から $a\in R \implies a=a1\in I_1+(I_2I_3\cdots I_n)$ がわかる．

(2)　$n\geq 2$ に関する数学的帰納法により示す．

$n=2$ のとき，$I_1I_2\subset I_1\cap I_2$ は明らか．仮定より $x+y=1$ を充たす $x\in I_1,\,y\in I_2$ が存在する．従って

$$a\in I_1\cap I_2 \implies a=ax+ay$$

だが，$a\in I_2$ かつ ***R* が可換環である**ことから $ax\in I_1I_2$ であり，$a\in I_1$ であることから $ay\in I_1I_2$ である．よって $a\in I_1I_2$ が言えた．

$n-1$ まで成り立っているとすると，帰納法の仮定は

$$I_1\cap\cdots\cap I_{n-1}=I_1I_2\cdots I_{n-1}.$$

(1) より $(I_1\cdots I_{n-1})+I_n=R$ なので，$n=2$ の場合の証明から

$$I_1\cap\cdots\cap I_{n-1}\cap I_n=(I_1\cdots I_{n-1})\cap I_n=I_1\cdots I_{n-1}I_n.$$

(3)　$n\geq 2$ に関する数学的帰納法により示す．

$n=2$ のとき，準同型写像 $\phi\colon R\to R/I_1\times R/I_2$ を

$$\phi(a)\coloneqq\big((a+I_1),\,(a+I_2)\big)$$

で定義する．

$$a\in\operatorname{Ker}\phi \iff \phi(a)=(I_1,\,I_2) \iff a\in I_1\ \text{かつ}\ a\in I_2$$

なので $\operatorname{Ker}\phi=I_1\cap I_2$ である．

$\forall c\in R/I_1\times R/I_2$ は $a,b\in R$ を使って $c=(a+I_1,\,b+I_2)$ と書ける．ここで仮定より，ある $x\in I_1,\,y\in I_2$ が存在して $x+y=1$ を充たすから，$z\coloneqq ay+bx$ とおくと

$$z=a+(b-a)x\in a+I_1,\quad z=b+(a-b)y\in b+I_2$$

である．i.e. $c=\phi(z)$ であり，$\operatorname{Im}\phi=R/I_1\times R/I_2$ がわかった．従って，環準同型定理より

$$R/(I_1\cap I_2)\cong R/I_1\times R/I_2$$

が示された．

$n-1$ まで成り立っているとすると，帰納法の仮定は

$$R/I_1 \cap \cdots \cap I_{n-1} \cong R/I_1 \times \cdots \times R/I_{n-1}.$$

$J := I_1 I_2 \cdots I_{n-1}$ とおく．(2) より $J = I_1 \cap \cdots \cap I_{n-1}$ である．よって **(1) からある $\boldsymbol{x \in J,\ y \in I_n}$ が存在して $\boldsymbol{x + y = 1}$ を充たす**ので，$n = 2$ の場合の証明をそのまま適用することができて，

$$\begin{aligned} R/(I_1 \cap \cdots \cap I_n) &= R/(J \cap I_n) \cong R/J \times R/I_n \\ &= R/(I_1 \cap \cdots \cap {}_{n-1}) \times R/I_n \\ &\cong R/I_1 \times \cdots \times R/I_n. \end{aligned}$$

■

系 3.14:

定理 3.13 の条件が成立しているとき，任意の整数 $a_1, \ldots, a_n$ に対して

$$R/(I_1^{a_1} \cap \cdots \cap I_n^{a_n}) \cong R/I_1^{a_1} \times \cdots \times R/I_n^{a_n}$$

証明 イデアル I, J が互いに素であるとき，$x \in I,\ y \in J$ であって $x + y = 1$ を充たすものを取ることができる．このとき，$\forall a, b \in \mathbb{Z}$ に対して

$$(x+y)^{a+b} = 1$$

であるが，左辺を展開して出現する項は全て I^a に属するか J^b に属するかのどちらかである．i.e. $1 \in I^a + J^b$ であるから，$I^a + J^b = R$ である． ■

3.4 加群

公理 3.2: 加群の公理

- R を環とする．**左 $\boldsymbol{R}$ 加群** (left R-module) とは，可換群 $(M, +, 0)$ と写像[a]

  $$\cdot : R \times M \to M,\ (a, x) \mapsto a \cdot x$$

  の組 $(M, +, \cdot\,)$ であって，$\forall x, x_1, x_2 \in M$，$\forall a, b \in R$ に対して以下を充たすもののことを言う：

  (LM1) $a \cdot (b \cdot x) = (ab) \cdot x$

  (LM2) $(a+b) \cdot x = a \cdot x + b \cdot x$

  (LM3) $a \cdot (x_1 + x_2) = a \cdot x_1 + a \cdot x_2$

  (LM4) $1 \cdot x = x$

  ただし，$1 \in R$ は環 R の乗法単位元である．
- R を環とする．**右 $\boldsymbol{R}$ 加群** (left R-module) とは，可換群 $(M, +, 0)$ と写像

  $$\cdot : M \times R \to M,\ (x, a) \mapsto x \cdot a$$

  の組 $(M, +, \cdot\,)$ であって，$\forall x, x_1, x_2 \in M$，$\forall a, b \in R$ に対して以下を充たすもののことを言う：

(RM1) $(x \cdot b) \cdot a = x \cdot (ba)$
(RM2) $x \cdot (a + b) = x \cdot a + x \cdot b$
(RM3) $(x_1 + x_2) \cdot a = x_1 \cdot a + x_2 \cdot a$
(RM4) $x \cdot 1 = x$

- $R,\ S$ を環とする．**$(R,\ S)$ 両側加群** ($(R,\ S)$-bimodule) とは，可換群 $(M,\ +,\ 0)$ と写像

$$\cdot_{\mathrm{L}} : R \times M \to M,\ (a,\ x) \mapsto a \cdot_{\mathrm{L}} x$$
$$\cdot_{\mathrm{R}} : M \times R \to M,\ (x,\ a) \mapsto x \cdot_{\mathrm{R}} a$$

の組 $(M,\ +,\ \cdot_{\mathrm{L}},\ \cdot_{\mathrm{R}})$ であって，$\forall x \in M,\ \forall a \in R,\ \forall b \in S$ に対して以下を充たすもののことを言う：

(BM1) 左スカラー乗法 $\cdot_{\mathrm{L}}$ に関して M は左 R 加群になる
(BM2) 右スカラー乗法 $\cdot_{\mathrm{R}}$ に関して M は右 S 加群になる
(BM3) $(a \cdot_{\mathrm{L}} x) \cdot_{\mathrm{R}} b = a \cdot_{\mathrm{L}} (x \cdot_{\mathrm{R}} b)$

[a] この写像 $\cdot$ は**スカラー乗法** (scalar multiplication) と呼ばれる．

R が**可換環**の場合，**(LM1)** と **(RM1)** が同値になるので，左 R 加群と右 R 加群の概念は同値になる．これを単に **R 加群** (R-module) と呼ぶ．

R が**体**の場合，R 加群のことを **R-ベクトル空間**と呼ぶ．

以下では，なんの断りもなければ R 加群と言って左 R 加群を意味する．

定義 3.28: 部分加群

R を環，M を R 加群とする．部分集合 $N \subset M$ が M の演算によって R 加群になるとき，N を M の**部分加群** (submodule) と呼ぶ．

命題 3.17: 部分加群の判定法

N が部分加群であることと次の条件が成り立つことは同値である：

(SM1) N は $+$ に関して M の部分群
(SM2) $a \in R,\ n \in N \implies an \in N$

定義 3.29: 部分加群の共通部分・和

M を R 加群，$N_1,\ N_2$ をその部分加群とする．このとき，以下の二つの集合は部分加群になる：

(1) $\boldsymbol{N_1 \cap N_2}$
(2) $\boldsymbol{N_1 + N_2} := \{\, x + y \mid x \in N_1,\ y \in N_2 \,\}$

3.4.1 加群の生成

定義 3.30: 線形独立

M を R 加群，$S = \{x_1, \ldots, x_n\}$ を M の有限部分集合とする．

(1) S が**線形従属**であるとは，

$$\exists a_1, \ldots, a_n \in R^n \quad \text{s.t.} \quad \exists i \in \{1, \ldots, n\},\ a_i \neq 0,\ a_1x_1 + \cdots a_nx_n = 0$$

が成り立つことを言う．

(2) S が線形従属でないとき，S は**線形独立** (linearly independent) であると言う．$\emptyset$ は線形独立であると見做す．

(3) 与えられた S に対して

$$a_1x_1 + \cdots a_nx_n, \quad a_i \in R$$

の形をした R の元を S の**線型結合** (linear combination) と呼ぶ．0 は空集合の線形結合と見做す．

定義 3.31: 加群の生成

M を左 R 加群，Λ を任意の添字集合とする．任意の部分集合 $S := \{x_\lambda\}_{\lambda\in\Lambda} \subset R$ を与える．

- S の任意の有限部分集合が定義 3.30 の意味で一次独立であるとき，S は一次独立であると言う．
- $$M = \left\{ \sum_{\lambda\in\Lambda} a_\lambda x_\lambda \;\middle|\; a_\lambda \in R,\ \substack{\text{有限個の添字 } i_1, \ldots, i_n \text{ を除いた} \\ \text{全ての添字 } \lambda\in\Lambda \text{ について } a_\lambda = 0} \right\}$$
  が成り立つとき，S は M を**張る**，または**生成する** (generate) と言い，S のことを M の**生成系** (generator) と呼ぶ．
  特に $\Lambda = \{1, \ldots, n\}$ のとき，M は ***R* 上有限生成な加群** (finitely generated) と呼ばれる．
- S が一次独立で，かつ M を生成するとき，S を M の**基底** (basis) と言う．

命題 3.18: 部分加群の生成

M を左 R 加群，Λ を任意の添字集合とする．部分集合 $S := \{x_\lambda\}_{\lambda\in\Lambda} \subset R$ を与える．このとき，集合

$$\langle S \rangle := \left\{ \sum_{\lambda\in\Lambda} a_\lambda x_\lambda \;\middle|\; a_\lambda \in R,\ \substack{\text{有限個の添字 } i_1, \ldots, i_n \text{ を除いた} \\ \text{全ての添字 } \lambda\in\Lambda \text{ について } a_\lambda = 0} \right\} \subset M$$

は M の部分加群になる．

証明 命題 3.17 の 2 条件を充していることを確認する．

(SM1)　加法単位元　0 は空集合の線型結合と見做すので $0 \in \langle S \rangle$ である．

和，逆元について閉じていること　$\langle S \rangle$ の勝手な 2 つの元 u, v は $a_i, b_i \in R,\ x_i, y_i \in S$ によって

$$u = a_1x_1 + \cdots + a_nx_n, \quad v = b_1y_1 + \cdots + b_ny_n \quad (m, n < \infty)$$

と書ける．よって $u \pm v \in \langle S \rangle$ である．

(SM2)　$c \in R$ ならば，$\forall v = a_1x_1 + \cdots + a_nx_n \in \langle S \rangle$ に対して

$$cv = (ca_1)x_1 + \cdots + (ca_n)x_n \in \langle S \rangle .$$

■

定義 3.32:

$\langle S \rangle$ のことを ***S* によって生成された部分加群**と呼ぶ．$\langle S \rangle$ のことを $\displaystyle\sum_{x \in S} Ax$ とも書く．$\Lambda = \{1, \ldots, n\}$ のときは $\langle x_1, \ldots, x_n \rangle$，あるいは $Ax_1 + \cdots + Ax_n$ とも書く．

R のイデアルがイデアルとして有限生成であることは，R 加群として有限生成であることと同値である．

3.4.2　加群の準同型

定義 3.33: 加群の準同型

M_1, M_2 を環 R 上の加群とする．

- 写像 $f\colon M_1 \to M_2$ が $\forall a \in R \forall x \in M_1$ に対して以下の条件を充たすとき，f は ***R* 加群の準同型**であると言われる．
  (1) f は加法 $+$ に関して可換群の準同型である
  (2) $f(ax) = af(x)$
  R 加群の準同型全体の集合を $\mathbf{Hom}_{\boldsymbol{R}}(\boldsymbol{M_1}, \boldsymbol{M_2})$ と書く．
- 写像 $f\colon M_1 \to M_2$ が R 加群の準同型であり，逆写像が存在してそれも R 加群の準同型であるとき，f を ***R* 加群の同型**と呼び，$M \cong N$ と書く．

R が体または斜体のとき，R 加群の準同型のことを**線型写像**と呼ぶ．

命題 3.19: Hom_R **加群**

R を可換群とする．このとき，$\mathbf{Hom}_{\boldsymbol{R}}(\boldsymbol{M_1}, \boldsymbol{M_2})$ の上の加法 $+$，スカラー乗法 $\cdot$ を次のように定めると，組 $\left(\mathrm{Hom}_R(M_1, M_2), +, \cdot\right)$ は左 R 加群になる：

(1) $\forall x \in M_1,\ (f+g)(x) := f(x) + g(x)$
(2) $\forall a \in R, \forall x \in M_1,\ (af)(x) := af(x)$

証明　命題 3.17 の 2 条件を充たしていることを確かめる．

(SM1) $+$ に関して命題 3.3 の 3 条件を確認する．

(SG1) 零写像を 0 とすると，明らかに $0 \in \mathrm{Hom}_R\,(M_1,\, M_2)$ である．

(SG2)

$$\begin{aligned} & f,\, g \in \mathrm{Hom}_R\,(M_1,\, M_2) \\ \Longrightarrow\ & \forall a \in R,\, \forall x,\, y \in M_1, \\ & \quad (f+g)(x+y) = f(x)+g(x)+f(y)+g(y) = (f+g)(x)+(f+g)(y), \\ & \quad (f+g)(ax) = f(ax)+g(ax) = \big(a(f+g)\big)(x) \\ \Longrightarrow\ & f+g \in \mathrm{Hom}_R\,(M_1,\, M_2) \end{aligned}$$

ただし，赤文字の部分で R が $+$ について可換群であることを使った．

(SG3)

$$\begin{aligned} & f \in \mathrm{Hom}_R\,(M_1,\, M_2) \\ \Longrightarrow\ & \forall a \in R,\, \forall x,\, y \in M_1, \\ & \quad (-f)(x+y) = -f(x+y) = (-f)(x)+(-f)(y), \\ & \quad (-f)(ax) = -f(ax) = \big(a(-f)\big)(x) \\ \Longrightarrow\ & -f \in \mathrm{Hom}_R\,(M_1,\, M_2) \end{aligned}$$

(SM2) R が可換環なので

$$\begin{aligned} & r \in R,\, f \in \mathrm{Hom}_R\,(M_1,\, M_2) \\ \Longrightarrow\ & \forall a \in R,\, \forall x,\, y \in M_1, \\ & \quad (rf)(x+y) = rf(x+y) = (rf)(x)+(rf)(y), \\ & \quad (rf)(ax) = raf(x) = arf(x) = \big(a(rf)\big)(x) \\ \Longrightarrow\ & af \in \mathrm{Hom}_R\,(M_1,\, M_2) \end{aligned}$$

である．

■

3.4.3　剰余加群

M を R 加群，$N \subset M$ を部分加群とする．M は $+$ に関して可換群なので N は $+$ に関して正規部分群であり，剰余群 M/N が定義できる．さらにスカラー乗法 $\cdot : R \times M/N \to M/N$ を上手く定義すれば M/N が左 R 加群になる：

定理 3.15: 剰余加群

左 R 加群 M とその部分加群 N を与える．このとき，加法に関する剰余類[a]全体の集合 M/N の上の 2 つの二項演算 $+\colon M/N \times M/N \to M/N,\ \cdot : R \times M/N \to M/N$ を

$$(x+N)+(y+N) \coloneqq (x+y)+N$$
$$a\cdot(x+N) \coloneqq (ax)+N$$

と定義するとこれらは well-defined であり，かつ $(M/N, +, \cdot)$ **は** R **加群をなす．**この環を M の N による**剰余加群** (quotient module) と言う．

[a] $+$ に関して可換群なので，左・右剰余類の区別はない．

<u>証明</u> 加法に関する well-definedness および可換群であることは，定理 3.2 より即座に従う．

well-definedness　加法に関する well-definedness は定理 3.2 より従う．スカラー乗法に関して示す．

剰余類剰余類 $x+N$ の勝手な元は $x' = x+n\ (n \in N)$ とかける．故に $\forall a \in R$ に対して

$$ax' = a(x+n) = ax+an$$

であるが，N が M の部分加群であることにより $an \in N$ が言える．従って $ax' \in (ax)+N$ であり，乗法の定義は剰余類の代表元の取り方に依らない．

R 加群であること　左 R 加群の公理を充していることを確認すれば良い．

(LM1) $a\cdot\big(b\cdot(x+N)\big) = a\cdot\big((bx)+N\big) = (abx)+N = (ab)\cdot(x+N)$

(LM2) $(a+b)\cdot(x+N) = \big(ax+bx\big)+N = a\cdot(x+N)+b\cdot(x+N)$

(LM3) $a\cdot\big((x+N)+(y+N)\big) = \big(a(x+y)\big)+N = (ax+ay)+N = a\cdot(x+N)+a\cdot(y+N)$

(LM4) $1_R\cdot(x+N) = (1_R x)+N = x+N$

■

系 3.16: 剰余加群への自然な全射準同型

R 加群 M とその部分加群 N を与える．このとき標準射影（定義??）$\pi\colon M \to N/I,\ x \mapsto x+N$ は $\boldsymbol{M/N}$ **を剰余加群と見做すと全射準同型写像になる．**また，$\mathrm{Ker}\,\pi = N$ である．π のことを**自然な全射準同型**と呼ぶ．

<u>証明</u> 加法 $+$ に関しては剰余群の全射準同型の場合と同様．後は定義 3.33-(2) の成立を確かめれば良い．

実際，剰余加群のスカラー乗法の定義より $\forall a \in R, \forall x \in M$ に対して

$$\pi(ax) = (ax)+I = a\cdot(x+N) = a\cdot\pi(x)$$

だから良い．■

定義 3.34: 核・像・余核

$f\colon M \to N$ を R 加群の準同型とする．

(1) $\operatorname{Ker} f \coloneqq \left\{ x \in M \;\middle|\; f(x) = 0 \right\}$ を f の**核** (kernel),
(2) $\operatorname{Im} f \coloneqq \left\{ f(x) \;\middle|\; x \in M \right\}$ を f の**像** (image),
(3) $\operatorname{Coker} f \coloneqq N/\operatorname{Im} f$ を**余核** (cokernel) と呼ぶ.

命題 3.20:

加群の準同型写像 $f\colon M \to N$ を与える．$\operatorname{Ker} f, \operatorname{Im} f$ はそれぞれ M, N の部分 R 加群であり，$\operatorname{Coker} f$ は R 加群である．

証明 **$\operatorname{Ker} f \subset M$ は部分 R 加群**

命題 3.17 の 2 条件を充たしていることを確かめる．加法に関する群準同型の性質から $f(0_M) = 0_N$ が従う．加群の準同型の定義から

$$\begin{aligned} x, y \in \operatorname{Ker} f \quad &\Longrightarrow \quad f(x+y) = f(x) + f(y) = 0,\ f(-x) = -f(x) = 0 \\ &\Longrightarrow \quad x+y, -x \in \operatorname{Ker} f \end{aligned}$$

より $+$ に関して部分群であるとわかった（条件 **(SM1)**），

$$\forall a \in R, \forall x \in \operatorname{Ker} f,\ f(ax) = af(x) = a0 = 0 \quad \Longrightarrow \quad ax \in \operatorname{Ker} f$$

より条件 **(SM2)** も充たす．

$\operatorname{Im} f \subset N$ は部分 R 加群

命題 3.17 の 2 条件を充たしていることを確かめる．まず，$0_N = f(0_M)$ である．

$$\begin{aligned} f(x), f(y) \in \operatorname{Im} f \quad &\Longrightarrow \quad f(x) + f(y) = f(x+y),\ -f(x) = f(-x) \\ &\Longrightarrow \quad 0,\ f(x) + f(y),\ -f(x) \in \operatorname{Im} f \end{aligned}$$

より $+$ に関して部分群であるとわかる（条件 **(SM1)**），

$$\forall a \in R, \forall f(x) \in \operatorname{Im} f,\ af(x) = f(ax) \in \operatorname{Im} f$$

より条件 **(SM2)** も充たす．

$\operatorname{Coker} f$ は R 加群

$\operatorname{Im} f$ が部分加群とわかったので，定理 3.15 から $\operatorname{Coker} f$ も R 加群である．

■

3.4.4 準同型定理

群，環の準同型定理（定理 3.17，定理 3.9）と同様に加群の準同型定理も成り立つ．証明はほとんど同じなので省略する．

定理 3.17: 加群の準同型定理 (第一同型定理)

R 加群の準同型写像 $\phi\colon M \to N$ を与える．$\pi\colon M \to M/\operatorname{Ker}\phi$ を自然な全射準同型とする．このとき，図 3.3 が可換図式となるような準同型 $\psi\colon M/\operatorname{Ker}\phi \to N$ がただ一つ存在し，$\psi\colon M/\operatorname{Ker}\phi \to \operatorname{Im}\phi$ は同型写像になる．

$$\begin{tikzcd} M \arrow[r, "\phi"] \arrow[d, "\pi"] & N \\ M/\operatorname{Ker}\phi \arrow[ur, dashed, red, "\exists!\psi"'] & \end{tikzcd}$$

図 3.3: 加群の準同型定理

定理 3.18: 環の準同型定理 (第二，第三同型定理)

M を R 加群，N_1, N_2 を部分加群とする．

(1) $\boldsymbol{(N_1 + N_2)/N_2 \cong N_1/N_1 \cap N_2}$

(2) $N_1 \subset N_2$ ならば $\boldsymbol{(M/N_1)/(N_2/N_1) \cong M/N_2}$

3.5　直積・直和・自由加群

R を環，Λ を任意の添字集合とする．$\forall\lambda \in \Lambda$ に対応して R 加群 M_λ が与えられているとする．R 加群の族 $\{(M_\lambda, +, \cdot)\}_{\lambda\in\Lambda}$ の集合としての直積は

$$\prod_{\lambda\in\Lambda} M_\lambda = \left\{ (x_\lambda)_{\lambda\in\Lambda} \;\middle|\; \forall\lambda \in \Lambda,\ x_\lambda \in M_\lambda \right\}$$

と書かれるのだった．

定義 3.35: 加群の直積・直和

Λ, $\{(M_\lambda, +, \cdot)\}_{\lambda\in\Lambda}$ を上述の通りにとる．

(1) 集合 $\prod_{\lambda\in\Lambda} M_\lambda$ の上の加法 $+$ およびスカラー乗法 $\cdot$ を次のように定めると，組 $\left(\prod_{\lambda\in\Lambda} M_\lambda, +, \cdot\right)$ は左 R 加群になる．これを加群の族 $\{(M_\lambda, +, \cdot)\}_{\lambda\in\Lambda}$ の**直積** (direct product) と呼ぶ：

$$+\colon \prod_{\lambda\in\Lambda} M_\lambda \times \prod_{\lambda\in\Lambda} M_\lambda \to \prod_{\lambda\in\Lambda} M_\lambda,\ \left((x_\lambda)_{\lambda\in\Lambda}, (y_\lambda)_{\lambda\in\Lambda}\right) \mapsto (x_\lambda + y_\lambda)_{\lambda\in\Lambda}$$
$$\cdot\colon R \times \prod_{\lambda\in\Lambda} M_\lambda \to \prod_{\lambda\in\Lambda} M_\lambda,\ \left(a, (x_\lambda)_{\lambda\in\Lambda}\right) \mapsto (a \cdot x_\lambda)_{\lambda\in\Lambda}$$

添字集合 Λ が有限集合 $\{1, \dots, n\}$ であるときは

$$M_1 \times M_2 \times \cdots \times M_n$$

とも書く．

(2) 加群の直積 $\left(\prod_{\lambda\in\Lambda} M_\lambda,\, +,\, \cdot\right)$ を与えると，次のように定義される部分集合 $\bigoplus_{\lambda\in\Lambda} M_\lambda$ は部分 R 加群をなす．これを加群の族 $\{(M_\lambda,\, +,\, \cdot\,)\}_{\lambda\in\Lambda}$ の**直和** (direct sum) と呼ぶ：

$$\bigoplus_{\lambda\in\Lambda} M_\lambda := \left\{ (x_\lambda)_{\lambda\in\Lambda} \in \prod_{\lambda\in\Lambda} M_\lambda \;\middle|\; \begin{array}{c}\text{有限個の添字 } i_1, \ldots, i_n \in \Lambda \text{ を除いた} \\ \text{全ての添字 } \lambda\in\Lambda \text{ について } x_\lambda = 0\end{array} \right\}$$

添字集合 Λ が有限集合 $\{1,\, \ldots,\, n\}$ であるときは

$$M_1 \oplus M_2 \oplus \cdots \oplus M_n$$

とも書く．

! 添字集合 Λ が有限のときは R 加群として $\prod_{\lambda\in\Lambda} M_\lambda \cong \bigoplus_{\lambda\in\Lambda} M_\lambda$ である．Λ が無限集合の時は，包含写像 $\bigoplus_{\lambda\in\Lambda} M_\lambda \hookrightarrow \prod_{\lambda\in\Lambda} M_\lambda$ によって準同型であるが，同型とは限らない．

定義 3.36: 標準射影，標準包含

加群の族 $\{(M_\lambda,\, +,\, \cdot\,)\}_{\lambda\in\Lambda}$ を与える．

(1) 各添字 $\mu \in \Lambda$ に対して，次のように定義される写像 $\pi_\mu \colon \prod_{\lambda\in\Lambda} M_\lambda \to M_\mu$ のことを**標準射影** (canonical projection) と呼ぶ：

$$\pi_\mu\big((x_\lambda)_{\lambda\in\Lambda}\big) := x_\mu$$

(2) 各添字 $\mu \in \Lambda$ に対して，次のように定義される写像 $\iota_\mu \colon M_\mu \hookrightarrow \bigoplus_{\lambda\in\Lambda} M_\lambda$ のことを**標準包含** (canonical inclusion) と呼ぶ：

$$\iota_\mu(x) := (y_\lambda)_{\lambda\in\Lambda}, \quad {}^{\text{w/}} \; y_\lambda := \begin{cases} x, & : \lambda = \mu \\ 0. & : \text{otherwise} \end{cases}$$

加群の族をいちいち $\{(M_\lambda,\, +,\, \cdot\,)\}_{\lambda\in\Lambda}$ と書くと煩雑なので，以降では省略して $\{M_\lambda\}_{\lambda\in\Lambda}$ と書くことにする．

3.5.1 普遍性

核，余核，直積，直和の普遍性による特徴付けを行う．これらは全て左 R 加群の圏 R-**Mod** における極限，余極限である．

命題 3.21: 核・余核の普遍性

左 R 加群の準同型写像 $f\colon M \longrightarrow M'$ を与える．また $i\colon \mathrm{Ker}\, f \hookrightarrow M,\ x \mapsto x$ を標準的包含，$p\colon M' \twoheadrightarrow \mathrm{Coker}\, f,\ x \mapsto x + \mathrm{Coker}\, f$ を標準的射影とする．このとき以下が成り立つ：

(核の普遍性) 任意の左 R 加群 N に対して，写像

$$\begin{aligned} i_*\colon \mathrm{Hom}_R(N,\, \mathrm{Ker}\, f) &\longrightarrow \left\{\, g \in \mathrm{Hom}_R(N,\, M) \;\middle|\; f \circ g = 0 \,\right\}, \\ h &\longmapsto i \circ h \end{aligned}$$

は well-defined な全単射である．i.e. $f \circ g = 0$ を充たす任意の $g \in \mathrm{Hom}_R(N,\, M)$ に対して，ある $h \in \mathrm{Hom}_R(N,\, \mathrm{Ker}\, f)$ が一意的に存在して図式 3.4a を可換にする．

(余核の普遍性) 任意の左 R 加群 N に対して，写像

$$p^*\colon \mathrm{Hom}_R(\mathrm{Coker}\, f,\, N) \longrightarrow \left\{\, g \in \mathrm{Hom}_R(M',\, N) \;\middle|\; g \circ f = 0 \,\right\},\ h \longmapsto h \circ p$$

は well-defined な全単射である．i.e. $g \circ f = 0$ を充たす任意の $g \in \mathrm{Hom}_R(M',\, N)$ に対して，ある $h \in \mathrm{Hom}_R(\mathrm{Coker}\, f,\, N)$ が一意的に存在して図式 3.4b を可換にする．

$$\begin{tikzcd} \mathrm{Ker}\, f \arrow[r, "i"] & M \arrow[r, shift left, "f"] \arrow[r, shift right, "0"'] & M' \\ \forall N \arrow[u, dashed, "\exists! h"] \arrow[ur, "g"'] & & \end{tikzcd}$$

(a) 核の普遍性

$$\begin{tikzcd} M \arrow[r, shift left, "f"] \arrow[r, shift right, "0"'] & M' \arrow[r, "p"] \arrow[dr, "g"'] & \mathrm{Coker}\, f \arrow[d, dashed, "\exists! h"] \\ & & \forall N \end{tikzcd}$$

(b) 余核の普遍性

<u>**証明**</u> (1) **well-definedness** 核の定義により $f \circ i = 0$ だから，$\forall h \in \mathrm{Hom}_R(N,\, \mathrm{Ker}\, f)$，$f \circ \bigl(i_*(h)\bigr) = (f \circ i) \circ h = 0$.

全単射であること $\forall g \in \left\{\, g \in \mathrm{Hom}_R(N,\, M) \;\middle|\; f \circ g = 0 \,\right\}$ をとる．このとき $\forall x \in N$ に対して $f\bigl(g(x)\bigr) = 0 \iff g(x) \in \mathrm{Ker}\, f$ なので，写像

$$h\colon N \longrightarrow \mathrm{Ker}\, f,\ x \longmapsto g(x)$$

は well-defined かつ $g = i \circ h \in \mathrm{Im}\, i_*$ が成り立つ．i.e. i_* は全射．

また，$h,\, h' \in \mathrm{Hom}_R(N,\, \mathrm{Ker}\, f)$ に対して

$$i_*(h) = i_*(h') \iff i \circ h = i \circ h' \implies \forall x \in N,\ i\bigl(h(x)\bigr) = i\bigl(h'(x)\bigr)$$

だが，i は単射なので $\forall x \in N,\ h(x) = h'(x) \iff h = h'$ が成り立つ．i.e. i_* は単射．

(2) **well-definedness** 余核の定義により $p \circ f = 0$ だから，$\forall h \in \mathrm{Hom}_R(\mathrm{Coker}\, f,\, N)$，$p^*(h) \circ f = h \circ (p \circ f) = 0$.

全単射であること $\forall g \in \left\{\, g \in \mathrm{Hom}_R(M',\, N) \;\middle|\; g \circ f = 0 \,\right\}$ をとる．このとき $\forall x' \in x + \mathrm{Coker}\, f$ はある $y \in M$ を用いて $x' = x + f(y)$ と書けるから

$$g(x') = g(x) + (g \circ f)(y) = g(x) \in N$$

が成り立つ．したがって写像

$$h\colon \operatorname{Coker} f \longrightarrow N,\ x+\operatorname{Im} f \longmapsto g(x)$$

は well-defined であり，かつ $g = h \circ p \in \operatorname{Im} p^*$ が成り立つ．i.e. p^* は全射．
また，$h,\, h' \in \operatorname{Hom}_R(\operatorname{Coker} f,\, N)$ に対して

$$p^*(h) = p^*(h') \quad\Longrightarrow\quad h \circ p = h' \circ p$$

が成り立つが，p は全射なので $h = h'$ が言える．i.e. p^* は単射．

■

【例 3.5.1】商加群の普遍性

左 R 加群 M と，その任意の部分加群 $N \subset M$ を与える．包含準同型 $i\colon N \longrightarrow M,\, x \longmapsto x$ の余核の普遍性の図式は

$$\begin{tikzcd}
N \arrow[r, shift left, "i"] \arrow[r, shift right, "0"'] & M' \arrow[r, "p"] \arrow[dr, "f"'] & \operatorname{Coker} i = M/N \arrow[d, dashed, "\exists!\overline{f}"] \\
& & \forall N
\end{tikzcd}$$

のようになる．すなわち，任意の左 R 加群 N と，$f \circ i = 0$ を充たす任意の準同型写像 $f\colon M \longrightarrow N$ に対して，ある $\overline{f}\colon M/N \longrightarrow N$ が一意的に存在して可換図式

$$\begin{tikzcd}
M \arrow[r, "f"] \arrow[d, "p"'] & \forall N \\
M/N \arrow[ur, dashed, "\exists!\bar{f}"']
\end{tikzcd}$$

が成り立つということである．$f \circ i = 0$ は $N \subset \operatorname{Ker} f$ と同値なので，次の命題が示されたことになる：

命題 3.22: 商加群の普遍性

$M,\, L$ を左 R 加群，$f\colon M \longrightarrow L$ を準同型とする．部分加群 $N \subset M$ が

$$N \subset \operatorname{Ker} f$$

を充たすならば，準同型 $\bar{f}\colon M/N \longrightarrow L$ であって標準的射影

$$p\colon M \longrightarrow M/N,\ x \longmapsto x+N$$

に対して図式 3.5 を可換にするようなものが一意に存在する．このような準同型 $\bar{f}\colon M/N \to L$ を $f\colon M \to L$ によって M/N 上に**誘導される準同型** (induced homomorphism) と呼ぶ．

$$
\begin{tikzcd}
M \arrow[r, "f"] \arrow[d, "p"'] & L \\
M/N \arrow[ur, dashed, "\exists!\bar{f}"'] &
\end{tikzcd}
$$

図 3.5: 商加群の普遍性

命題 3.23: 直積・直和の普遍性

任意の添字集合 Λ，および加群の族 $\{M_\lambda\}_{\lambda\in\Lambda}$ を与える．添字 $\mu\in\Lambda$ に対する標準射影，標準包含をそれぞれ $\pi_\mu,\ \iota_\mu$ と書く．

(1) 任意の左 R 加群 N に対して，写像

$$
\begin{array}{ccc}
\mathrm{Hom}_R\left(N,\ \prod_{\lambda\in\Lambda} M_\lambda\right) & \longrightarrow & \prod_{\lambda\in\Lambda}\mathrm{Hom}_R(N,\ M_\lambda) \\
\rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\
f & \longmapsto & \{\pi_\lambda\circ f\}_{\lambda\in\Lambda}
\end{array}
$$

は全単射である．i.e. 任意の左 R 加群 N ，および任意の左 R 加群の準同型写像の族 $\{f_\lambda\colon N\to M_\lambda\}_{\lambda\in\Lambda}$ に対して，$\forall\lambda\in\Lambda,\ \pi_\mu\circ f=f_\lambda$ を充たす準同型写像 $f\colon N\to\prod_{\lambda\in\Lambda} M_\lambda$ が一意的に存在する（図式 3.6a）．

(2) 任意の左 R 加群 N に対して，写像

$$
\begin{array}{ccc}
\mathrm{Hom}_R\left(\bigoplus_{\lambda\in\Lambda} M_\lambda,\ N\right) & \longrightarrow & \prod_{\lambda\in\Lambda}\mathrm{Hom}_R(M_\lambda,\ N) \\
\rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\
f & \longmapsto & \{f\circ\iota_\lambda\}_{\lambda\in\Lambda}
\end{array}
$$

は全単射である．i.e. 任意の左 R 加群 N ，および任意の左 R 加群の準同型写像の族 $\{f_\lambda\colon M_\lambda\to N\}_{\lambda\in\Lambda}$ に対して，$\forall\lambda\in\Lambda,\ f\circ\iota_\lambda=f_\lambda$ を充たす準同型写像 $f\colon\bigoplus_{\lambda\in\Lambda} M_\lambda\to N$ が一意的に存在する（図式 3.6b）．

$$
\begin{tikzcd}
N \arrow[r, dashed, "\exists! f"] \arrow[dr, "f_\lambda"'] & \prod_{\lambda\in\Lambda} M_\lambda \arrow[d, "\pi_\lambda"] \\
& M_\lambda
\end{tikzcd}
$$

(a) 直積の普遍性

$$
\begin{tikzcd}
M_\lambda \arrow[r, "\iota_\lambda"] \arrow[dr, "f_\lambda"'] & \bigoplus_{\lambda\in\Lambda} M_\lambda \arrow[d, dashed, "\exists! f"] \\
& N
\end{tikzcd}
$$

(b) 直和の普遍性

証明　(1) **存在**　左 R 加群の準同型写像の族 $\{\, f_\lambda\colon N \to M_\lambda \,\}_{\lambda\in\Lambda}$ が与えられたとき，写像 f を

$$f\colon N \to \prod_{\lambda\in\Lambda} M_\lambda,\ x \mapsto \bigl(f_\lambda(x)\bigr)_{\lambda\in\Lambda}$$

と定義する．このとき $\forall\mu\in\Lambda, \forall x\in N$ に対して

$$(\pi_\mu \circ f)(x) = f_\mu(x)$$

なので図 3.6a は可換図式になる．

一意性　図 3.6a を可換図式にする別の準同型写像 $g\colon N \to \prod_{\lambda\in\Lambda} M_\lambda$ が存在したとする．このとき $\forall x\in N, \forall\lambda\in\Lambda$ に対して

$$\pi_\lambda\bigl(g(x)\bigr) = f_\lambda(x) = \pi_\lambda\bigl(f(x)\bigr)$$

なので $f(x) = g(x)$ となる．i.e. f は一意である．

(2) **存在**　左 R 加群の準同型写像の族 $\{\, f_\lambda\colon M_\lambda \to N \,\}_{\lambda\in\Lambda}$ が与えられたとき，写像 f を

$$f\colon \bigoplus_{\lambda\in\Lambda} M_\lambda \to N,\ (x_\lambda)_{\lambda\in\Lambda} \mapsto \sum_{\lambda\in\Lambda} f_\lambda(x_\lambda)$$

と定義する．右辺は有限和なので意味を持つ．

このとき $\forall\mu\in\Lambda, \forall x\in M_\mu$ に対して

$$f\bigl(\iota_\mu(x)\bigr) = f_\mu(x_\mu) + \sum_{\lambda\neq\mu} f_\lambda(0) = f_\mu(x_\mu)$$

なので図 3.6b は可換図式になる．

一意性　図 3.6b を可換図式にする別の準同型写像 $g\colon \bigoplus_{\lambda\in\Lambda} M_\lambda \to N$ が存在したとする．このとき $\forall(x_\lambda)_{\lambda\in\Lambda} \in \bigoplus_{\lambda\in\Lambda}$ に対して

$$g\bigl((x_\lambda)_{\lambda\in\Lambda}\bigr) = g\left(\sum_{\lambda\in\Lambda} \iota_\lambda(x_\lambda)\right) = \sum_{\lambda\in\Lambda} g\bigl(\iota_\lambda(x_\lambda)\bigr) = \sum_{\lambda\in\Lambda} f_\lambda(x_\lambda) = f\bigl((x_\lambda)_{\lambda\in\Lambda}\bigr)$$

なので $f = g$ となる．i.e. f は一意である．

■

3.5.2　自由加群

Λ を集合，M を左 R 加群とする．左 R 加群の族 $\{M_\lambda\}_{\lambda\in\Lambda}$ に対して，$\forall\lambda\in\Lambda,\ M_\lambda = M$ が成り立つとき

$$M^\Lambda := \prod_{\lambda\in\Lambda} M_\lambda, \quad M^{\oplus\Lambda} := \bigoplus_{\lambda\in\Lambda} M_\lambda$$

と書く．得に $\Lambda = \{1, \ldots, n\}$ のとき $M^n, M^{\oplus n}$ と書くが，$M^n \cong M^{\oplus n}$ である．

定義 3.37: 自由加群

- ある集合 Λ に対して，左 R 加群 M が R 上の**自由加群** (free module) であるとは，以下を充たすことを言う：
$$M \cong R^{\oplus\Lambda} = \bigoplus_{\lambda\in\Lambda} R$$
- $R^{\oplus\Lambda}$ の元を
$$\sum_{\lambda\in\Lambda} a_\lambda \lambda \quad {}^{\mathrm{w}/}\ a_\lambda \in R \text{ は有限個を除いて } 0$$
と書き，Λ の元の，R を係数とする**形式的な線型結合** (formal linear combination) という．
- 自由加群 $R^{\oplus\Lambda}$ の元のうち，第 $\lambda\in\Lambda$ 成分のみが $1\in R$ で他が全て $0\in R$ であるようなものを $\forall\lambda\in\Lambda$ について集めた族
$$\{\,\iota_\lambda(1)\,\}_{\lambda\in\Lambda} \subset R^{\oplus\Lambda}$$
は $R^{\oplus\Lambda}$ の**基底** (basis) である．

命題 3.24: 基底を持つ R 加群は自由加群

R 加群 M が基底 S を持てば
$$M \cong R^{\oplus S}$$
である．

3.6 ベクトル空間

$\mathbb{K}$ を体とする．このとき $\mathbb{K}$ 加群のことを体 $\mathbb{K}$ 上のベクトル空間と呼び，$\mathbb{K}$ 加群の準同型写像のことを**線型写像**と呼ぶのだった．

線型写像 $f\colon V \longrightarrow W$ の核，像，余核は左 R 加群の核，像，余核と全く同様に
$$\begin{aligned}\operatorname{Ker} f &:= \{\,\boldsymbol{v}\in V \mid f(\boldsymbol{v}) = 0\,\},\\ \operatorname{Im} f &:= \{\,f(\boldsymbol{v})\in W \mid \boldsymbol{v}\in V\,\},\\ \operatorname{Coker} f &:= W/\operatorname{Im} f\end{aligned}$$
として定義される．$\operatorname{Ker} f, \operatorname{Im} f$ がそれぞれ V, W の部分ベクトル空間であることは，左 R 加群の場合と全く同じ議論によって示される．

3.6.1 階数・退化次数の定理

V, W を**有限次元** $\mathbb{K}$ ベクトル空間とし，線型写像 $T\colon V \longrightarrow W$ を与える．V, W の基底 $\{\mathbf{e}_1, \dots, \mathbf{e}_{\dim V}\}$, $\{\mathbf{f}_1, \dots, \mathbf{f}_{\dim W}\}$ をとり，

$$T(\mathbf{e}_\mu) = T^\nu{}_\mu \mathbf{f}_\nu$$

のように左辺を展開したときに得られる行列

$$\begin{bmatrix} T^1{}_1 & \cdots & T^1{}_{\dim V} \\ \vdots & \ddots & \vdots \\ T^{\dim W}{}_1 & \cdots & T^{\dim W}{}_{\dim V} \end{bmatrix}$$

は基底 $\{\mathbf{e}_1, \dots, \mathbf{e}_{\dim V}\}$, $\{\mathbf{f}_1, \dots, \mathbf{f}_{\dim W}\}$ に関する T の**表現表列**と呼ばれる．$\forall \boldsymbol{v} = v^\nu \mathbf{e}_\nu \in V$ に対して

$$T(\boldsymbol{v}) = T(v^\nu \mathbf{e}_\nu) = v^\nu T(\mathbf{e}_\nu) = v^\nu T^\mu{}_\nu \mathbf{f}_\mu$$

と書けるので，成分表示だけを見ると T はその表現行列を左から掛けることに相当する：

$$\begin{bmatrix} T^1{}_1 & \cdots & T^1{}_{\dim V} \\ \vdots & \ddots & \vdots \\ T^{\dim W}{}_1 & \cdots & T^{\dim W}{}_{\dim V} \end{bmatrix} \begin{bmatrix} v^1 \\ \vdots \\ v^{\dim V} \end{bmatrix}$$

定義 3.38: 線型写像の階数

$\operatorname{Im} T$ の次元のことを T の**階数** (rank) と呼び，$\mathbf{rank}\, \boldsymbol{T}$ と書く．

命題 3.25: 表現行列の標準形

V, W を**有限次元**ベクトル空間とし，任意の線型写像 $T\colon V \longrightarrow W$ を与える．このとき V, W の基底であって，T の表現行列を

$$\begin{bmatrix} I_{\operatorname{rank} T} & 0 \\ 0 & 0 \end{bmatrix}$$

の形にするものが存在する．

証明 $\operatorname{Im} T$ の基底 $\{\mathbf{f}_1, \dots, \mathbf{f}_{\operatorname{rank} T}\}$ および $\operatorname{Ker} T$ の基底 $\{\mathbf{k}_1, \dots \mathbf{k}_{\dim(\operatorname{Ker} T)}\}$ を勝手にとる．像の定義から，$1 \le \forall \mu \le \operatorname{rank} T$ に対して $\mathbf{e}_\mu \in V$ が存在して $\mathbf{f}_\mu = T(\mathbf{e}_\mu)$ を充たす．

まず $\mathbf{e}_1, \dots, \mathbf{e}_{\operatorname{rank} T}, \mathbf{k}_1, \dots, \mathbf{k}_{\dim(\operatorname{Ker} T)}$ が V の基底を成すことを示す．

線型独立性

$$\sum_{\mu=1}^{\operatorname{rank} T} a^\mu \mathbf{e}_\mu + \sum_{\nu=1}^{\dim(\operatorname{Ker} T)} b^\nu \mathbf{k}_\nu = 0$$

を仮定する．左辺に T を作用させることで

$$\sum_{\mu=1}^{\operatorname{rank} T} a^\mu \mathbf{f}_\mu = 0$$

がわかるが，$\mathbf{f}_1, \dots, \mathbf{f}_{\mathrm{rank}\, T}$ は $\mathrm{Im}\, T$ の基底なので線型独立であり，$1 \leq \forall \mu \leq \mathrm{rank}\, T$ に対して $a_\mu = 0$ が言える．故に仮定から

$$\sum_{\nu=1}^{\dim(\mathrm{Ker}\, T)} b^\nu \mathbf{k}_\nu = 0$$

であるが，$\mathbf{k}_1, \dots, \mathbf{k}_{\dim(\mathrm{Ker}\, T)}$ は $\mathrm{Ker}\, T$ の基底なので線型独立であり，$1 \leq \forall \nu \leq \dim(\mathrm{Ker}\, T)$ に対して $b_\nu = 0$ が言える．i.e. $\mathbf{e}_1, \dots, \mathbf{e}_{\mathrm{rank}\, T}, \mathbf{k}_1, \dots, \mathbf{k}_{\dim(\mathrm{Ker}\, T)}$ は線型独立である．

V を生成すること $\forall \boldsymbol{v} \in V$ を 1 つとる．このとき $T(\boldsymbol{v}) \in \mathrm{Im}\, T$ なので

$$T(\boldsymbol{v}) = \sum_{\mu=1}^{\mathrm{rank}\, T} v^\mu \mathbf{f}_\mu$$

と展開できる．ここで $\boldsymbol{w} := \sum_{\mu=1}^{\mathrm{rank}\, T} v^\mu \mathbf{e}_\mu \in V$ とおくと，$T(\boldsymbol{v}) = T(\boldsymbol{w})$ が成り立つが，T が線型写像であることから $T(\boldsymbol{v} - \boldsymbol{w}) = 0 \iff \boldsymbol{v} - \boldsymbol{w} \in \mathrm{Ker}\, T$ が言えて

$$\boldsymbol{v} - \boldsymbol{w} = \sum_{\nu=1}^{\dim(\mathrm{Ker}\, T)} w^\nu \mathbf{k}_\nu$$

と展開できる．従って

$$\boldsymbol{v} = \boldsymbol{w} + (\boldsymbol{v} - \boldsymbol{w}) = \sum_{\mu=1}^{\mathrm{rank}\, T} v^\mu \mathbf{e}_\mu + \sum_{\nu=1}^{\dim(\mathrm{Ker}\, T)} w^\nu \mathbf{k}_\nu$$

であり，$\mathbf{e}_1, \dots, \mathbf{e}_{\mathrm{rank}\, T}, \mathbf{k}_1, \dots, \mathbf{k}_{\dim(\mathrm{Ker}\, T)}$ は V を生成する．

$\mathbf{f}_1, \dots, \mathbf{f}_{\mathrm{rank}\, T}$ と線型独立な $\dim W - \mathrm{rank}\, T$ 個のベクトル $\tilde{\mathbf{f}}_{\mathrm{rank}\, T+1}, \dots, \tilde{\mathbf{f}}_{\dim W}$ をとると，

- V の基底 $\{\mathbf{e}_1, \dots, \mathbf{e}_{\mathrm{rank}\, T}, \mathbf{k}_1, \dots, \mathbf{k}_{\dim(\mathrm{Ker}\, T)}\}$
- W の基底 $\{\mathbf{f}_1, \dots, \mathbf{f}_{\mathrm{rank}\, T}, \tilde{\mathbf{f}}_{\mathrm{rank}\, T+1}, \dots, \tilde{\mathbf{f}}_{\dim W}\}$

に関する T の表現行列は

$$\begin{bmatrix} I_{\mathrm{rank}\, T} & 0 \\ 0 & 0 \end{bmatrix}$$

になる． ■

系 3.19: 階数・退化次数の定理（有限次元）

V, W を**有限次元**ベクトル空間とし，任意の線型写像 $T \colon V \longrightarrow W$ を与える．このとき

$$\dim V = \dim(\mathrm{Im}\, T) + \dim(\mathrm{Ker}\, T)$$

が成り立つ．

証明 命題 3.25 の証明より従う． ■

系 3.19 から便利な補題がいくつか従う：

補題 3.2: 有限次元ベクトル空間に関する小定理集

V, W を**有限次元**ベクトル空間とし，任意の線型写像 $T\colon V \longrightarrow W$ を与える．このとき以下が成り立つ：

(1) $\mathrm{rank}\, T \le \dim V$. 特に $\mathrm{rank}\, T = \dim V \iff T$ は単射
(2) $\mathrm{rank}\, T \le \dim W$. 特に $\mathrm{rank}\, T = \dim W \iff T$ は全射
(3) $\dim V = \dim W$ かつ T が単射 $\implies$ T は同型写像
(4) $\dim V = \dim W$ かつ T が全射 $\implies$ T は同型写像

<u>証明</u>　(1) 系 3.19 より

$$\dim V = \mathrm{rank}\, T + \dim(\mathrm{Ker}\, T) \ge \mathrm{rank}\, T$$

が成り立つ．特に命題 3.9 から T が単射 $\iff$ $\mathrm{Ker}\, T = 0$ $\iff$ $\dim(\mathrm{Ker}\, T) = 0$ $\iff$ $\mathrm{rank}\, T = \dim V$ が従う．

(2) rank の定義より $\mathrm{rank}\, T \le \dim W$ は明らか．特に次元の等しい有限次元ベクトル空間は同型なので，T が全射 $\iff$ $\mathrm{Im}\, T \cong W$ $\iff$ $\dim(\mathrm{Im}\, T) = \mathrm{rank}\, T = \dim W$ が言える．

(3) $\dim V = \dim W$ かつ T が単射とする．T が単射なので (1) より $\mathrm{rank}\, T = \dim V = \dim W$ が従い，(2) より T は全射でもある．

(4) $\dim V = \dim W$ かつ T が全射とする．T が全射なので (2) より $\mathrm{rank}\, T = \dim W = \dim V$ が従い，(1) より T は単射でもある．

■

3.6.2　分裂補題と射影的加群

実は，系 3.19 は有限次元でなくとも成り立つ．それどころか，左 R 加群の場合の分裂補題に一般化される．

補題 3.3: 分裂補題

左 R 加群の短完全列

$$0 \longrightarrow M_1 \xrightarrow{i_1} M \xrightarrow{p_2} M_2 \longrightarrow 0 \tag{3.6.1}$$

が与えられたとする．このとき，以下の二つは同値である：

(1) 左 R 加群の準同型 $i_2\colon M_2 \longrightarrow M$ であって $p_2 \circ i_2 = 1_{M_2}$ を充たすものが存在する
(2) 左 R 加群の準同型 $p_1\colon M \longrightarrow M_1$ であって $p_1 \circ i_1 = 1_{M_1}$ を充たすものが存在する

<u>証明</u> **(1) $\implies$ (2)**　写像

$$p_1'\colon M \longrightarrow M,\ x \longmapsto x - i_2\bigl(p_2(x)\bigr)$$

を定義すると，

$$p_2\bigl(p_1'(x)\bigr) = p_2(x) - ((p_2 \circ i_2) \circ p_2)(x) = p_2(x) - p_2(x) = 0$$

が成り立つ．従って，(3.6.1) が完全列であることを使うと $p_1'(x) \in \mathrm{Ker}\, p_2 = \mathrm{Im}\, i_1$ である．さらに i_1 が単射であることから

$$\exists! y \in M_1,\ p_1'(x) = i_1(y)$$

が成り立つ．ここで写像

$$p_1 \colon M \longrightarrow M_1,\ x \longmapsto y$$

を定義するとこれは準同型写像であり，$\forall x \in M_1$ に対して

$$p_1'\bigl(i_1(x)\bigr) = i_1(x) - (i_2 \circ (p_2 \circ i_1))(x) = i_1(x)$$

が成り立つ[*1]ことから

$$(p_1 \circ i_1)(x) = x$$

とわかる．i.e. $p_1 \circ i_1 = 1_{M_1}$

(1) $\Longleftarrow$ **(2)** (3.6.1) は完全列であるから $M_2 = \mathrm{Ker}\, 0 = \mathrm{Im}\, p_2$ である．従って $\forall x \in M_2 = \mathrm{Im}\, p_2$ に対して，$x = p_2(y)$ を充たす $y \in M$ が存在する．ここで写像

$$i_2 \colon M_2 \longrightarrow M,\ x \longmapsto y - i_1\bigl(p_1(y)\bigr)$$

は well-defined である．$x = p_2(y')$ を充たす勝手な元 $y' \in M$ をとってきたとき，$p_2(y - y') = 0$ より $y - y' \in \mathrm{Ker}\, p_2 = \mathrm{Im}\, i_1$ だから，i_1 の単射性から

$$\exists! z \in M_1, \quad y - y' = i_1(z)$$

が成り立ち，このとき

$$\Bigl(y - i_1\bigl(p_1(y)\bigr)\Bigr) - \Bigl(y' - i_1\bigl(p_1(y')\bigr)\Bigr) = i_1(z) - (i_1 \circ (p_1 \circ i_1))(z) = i_1(z) - i_1(z) = 0$$

とわかるからである．i_2 は準同型写像であり，$\forall x \in M_2$ に対して

$$(p_2 \circ i_2)(x) = p_2(y) - ((p_2 \circ i_1) \circ p_1)(y) = p_2(y) = x$$

なので $p_2 \circ i_2 = 1_{M_2}$．

■

系 3.20:

左 R 加群の短完全列

$$0 \longrightarrow M_1 \xrightarrow{i_1} M \xrightarrow{p_2} M_2 \longrightarrow 0$$

が補題 3.3 の条件を充たすならば

$$M \cong M_1 \oplus M_2$$

[*1] (3.6.1) が完全列であるため，$p_2 \circ i_1 = 0$

証明 補題 3.3 の条件 (1) が満たされているとする．このとき補題 3.3 証明から $\forall x \in M$ に対して

$$i_1\bigl(p_1(x)\bigr) = p_1'(x) = x - i_2\bigl(p_2(x)\bigr) \iff i_1\bigl(p_1(x)\bigr) + i_2\bigl(p_2(x)\bigr) = x$$

また，完全列の定義から $p_2\bigl(i_1(x)\bigr) = 0$ であるから $\forall x \in M_2$ に対して

$$p_1'\bigl(i_2(x)\bigr) = i_2(x) - ((i_2 \circ p_2) \circ i_2)(x) = 0 = i_1(0)$$

であり，結局 $p_1\bigl(i_2(x)\bigr) = 0$ とわかる．

ここで準同型写像

$$\begin{aligned} &f\colon M_1 \oplus M_2 \longrightarrow M,\ (x,\, y) \longmapsto i_1(x) + i_2(y), \\ &g\colon M \longrightarrow M_1 \oplus M_2,\ x \longmapsto \bigl(p_1(x),\, p_2(x)\bigr) \end{aligned}$$

を定めると

$$\begin{aligned} (g \circ f)(x,\, y) &= \bigl(p_1(i_1(x)) + p_1(i_2(y)),\, p_2(i_1(x)) + p_2(i_2(x))\bigr) = (x,\, y), \\ (f \circ g)(x) &= i_1(p_1(x)) + i_2(p_2(x)) = x \end{aligned}$$

なので $f,\, g$ は同型写像. ■

定義 3.39: 分裂

左 R 加群の短完全列

$$0 \longrightarrow M_1 \xrightarrow{i_1} M \xrightarrow{p_2} M_2 \longrightarrow 0$$

が**分裂** (split) するとは，補題 3.3 の条件を充たすことをいう．

定義 3.40: 射影的加群

左 R 加群 P が**射影的加群** (projective module) であるとは，任意の左 R 加群の**全射準同型** $f\colon M \longrightarrow N$ および任意の準同型写像 $g\colon P \longrightarrow N$ に対し，左 R 加群の準同型写像 $h\colon P \longrightarrow M$ であって $f \circ h = g$ を充たすものが存在することを言う（図式 3.7）.

$$\begin{tikzcd} & P \arrow[d, "g"] \arrow[dl, dashed, "\exists h"'] \\ M \arrow[r, two heads, "f"] & N \end{tikzcd}$$

図 3.7: 射影的加群

命題 3.26:

左 R 加群の完全列

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$$

は，N が射影的加群ならば分裂する．

証明 射影的加群の定義において $P=N$ とすることで，左 R 加群の準同型写像 $s\colon N\longrightarrow M$ であって $g\circ s=1_N$ を充たすものが存在する． ■

命題 3.27: 射影的加群の直和

左 R 加群の族 $\{P_\lambda\}_{\lambda\in\Lambda}$ に対して以下の 2 つは同値：

(1) $\forall\lambda\in\Lambda$ に対して P_λ が射影的加群

(2) $\displaystyle\bigoplus_{\lambda\in\Lambda}P_\lambda$ が射影的加群

証明 標準的包含を $\iota_\lambda\colon P_\lambda\hookrightarrow\bigoplus_{\lambda\in\Lambda}P_\lambda$ と書く．

(1)⟹(2) 仮定より，$\forall\lambda\in\lambda$ に対して，任意の全射準同型写像 $f\colon M\longrightarrow N$ および任意の準同型写像 $g\colon\bigoplus_{\lambda\in\Lambda}P_\lambda\longrightarrow N$ に対して，準同型写像 $h_\lambda\colon P_\lambda\longrightarrow M$ であって $f\circ h_\lambda=g\circ\iota_\lambda$ を充たすものが存在する．従って直和の普遍性より準同型写像

$$h\colon\bigoplus_{\lambda\in\Lambda}P_\lambda\longrightarrow M$$

であって $f\circ h_\lambda=h\circ\iota_\lambda$ を充たすものが一意的に存在する．このとき

$$(f\circ h)\circ\iota_\lambda=f\circ h_\lambda=g\circ\iota_\lambda$$

であるから，h の一意性から $f\circ h=g$.

(1)⟸(2) $\lambda\in\Lambda$ を一つ固定し，任意の全射準同型写像 $f\colon M\longrightarrow N$ および任意の準同型写像 $g\colon P_\lambda\longrightarrow M$ を与える．直和の普遍性より準同型写像

$$h\colon\bigoplus_{\lambda\in\Lambda}P_\lambda\longrightarrow N$$

であって $h\circ\iota_\lambda=g$（$\forall\mu\in\Lambda\setminus\{\lambda\}$, $h\circ\iota_\lambda=0$）を充たすものが一意的に存在する．さらに仮定より，準同型写像

$$\alpha\colon\bigoplus_{\lambda\in\Lambda}\longrightarrow M$$

であって $f\circ\alpha=h$ を充たすものが存在する．このとき

$$f\circ(\alpha\circ\iota_\lambda)=h\circ\iota_\lambda=g$$

なので $\beta:=h\circ\iota_\lambda$ とおけば良い．

■

系 3.21: 自由加群は射影的加群

環 R 上の自由加群は射影的加群である

証明 R が射影的加群であることを示せば命題 3.27 より従う．

左 R 加群の全射準同型写像と準同型写像 $f\colon M \longrightarrow N,\ g\colon R \longrightarrow N$ を任意に与える．このときある $x \in M$ が存在して $f(x) = g(1)$ となる．この x に対して準同型写像 $h\colon R \longrightarrow M,\ a \longmapsto ax$ を定めると，$\forall a \in R$ に対して

$$f\bigl(h(a)\bigr) = f(ax) = af(x) = ag(1) = g(a)$$

が成り立つので $f \circ h = g$ となる． ■

V, W を任意の（有限次元とは限らない）$\mathbb{K}$ ベクトル空間，$T\colon V \longrightarrow W$ を任意の線型写像とする．

$$\begin{aligned} i_1 &\colon \operatorname{Ker} T \longrightarrow V,\ \boldsymbol{v} \longmapsto \boldsymbol{v}, \\ p_2 &\colon V \longrightarrow \operatorname{Im} T,\ \boldsymbol{v} \longmapsto T(\boldsymbol{v}), \end{aligned}$$

と定めると，i_1 は単射，p_2 は全射で，かつ $p_2 \circ i_1 = 0$ が成り立つ．よって $\mathbf{Vec}_{\mathbb{K}}$ の図式

$$0 \longrightarrow \operatorname{Ker} T \xrightarrow{i_1} V \xrightarrow{p_2} \operatorname{Im} T \longrightarrow 0 \tag{3.6.2}$$

は短完全列だが，$\operatorname{Im} T$ はベクトル空間なので自由加群であり，系 3.21 より射影的加群でもある．従って命題 3.26 より短完全列 (3.6.2) は分裂し，系 3.20 から

$$V \cong \operatorname{Im} T \oplus \operatorname{Ker} T$$

が言える．

定理 3.22: 階数・退化次数の定理

V, W をベクトル空間とし，任意の線型写像 $T\colon V \longrightarrow W$ を与える．このとき

$$\dim V = \dim(\operatorname{Im} T) + \dim(\operatorname{Ker} T)$$

が成り立つ．