代数学 I 第 11 回講義資料

担当：大矢 浩徳 (OYA Hironori)*

10.1 準同型定理

準同型 $\phi\colon G \to G'$ があると，その核 $\operatorname{Ker}\phi$ は G の正規部分群となるのであった (第 10 回講義資料命題 9.3(2))．これより，剰余群 $G/\operatorname{Ker}\phi$ を考えることができる．準同型に関する基本的な重要定理である以下の準同型定理は，この剰余群が実は ϕ の像 $\operatorname{Im}\phi$ と群として同等なものになることを主張する：

定理 10.1 (準同型定理 (第 1 同型定理))

$\phi\colon G \to G'$ が準同型であるとき，写像

$$\overline{\phi}\colon G/\operatorname{Ker}\phi \to \operatorname{Im}\phi,\ g\operatorname{Ker}\phi \mapsto \phi(g)$$

は well-defined であり，群同型になる．特に，$G/\operatorname{Ker}\phi \simeq \operatorname{Im}\phi$ である．

証明. まず，写像 $\overline{\phi}$ の well-defined 性をチェックする．このためには，

$$g_1\operatorname{Ker}\phi = g_2\operatorname{Ker}\phi \text{であるとき}, \phi(g_1) = \phi(g_2)$$

となることを示せばよい．$g_1\operatorname{Ker}\phi = g_2\operatorname{Ker}\phi$ のとき，$g_1 \overset{\operatorname{Ker}\phi}{\sim}_L g_2$ なので (この記号については第 7 回講義資料定義 6.4 を参照)，ある $k \in \operatorname{Ker}\phi$ が存在して，$g_1 = g_2k$．これより，

$$\phi(g_1) = \phi(g_2k) = \phi(g_2)\phi(k) = \phi(g_2)$$

となる (最後の等式は $k \in \operatorname{Ker}\phi$ より $\phi(k)$ が G' の単位元となることからわかる)．よって，$\overline{\phi}$ の well-defined 性は示された．

次に，$\overline{\phi}$ が準同型となることを示す．任意の $g_1\operatorname{Ker}\phi, g_2\operatorname{Ker}\phi \in G/\operatorname{Ker}\phi$ に対し，

$$\overline{\phi}(g_1\operatorname{Ker}\phi \cdot g_2\operatorname{Ker}\phi) = \overline{\phi}(g_1g_2\operatorname{Ker}\phi) = \phi(g_1g_2) = \phi(g_1)\phi(g_2) = \overline{\phi}(g_1\operatorname{Ker}\phi)\overline{\phi}(g_2\operatorname{Ker}\phi)$$

となるので，$\overline{\phi}$ は確かに準同型である．

後は $\overline{\phi}$ が全単射写像であることを見ればよい．まず，任意の $\phi(g) \in \operatorname{Im}\phi$ に対し，$\overline{\phi}(g\operatorname{Ker}\phi) = \phi(g)$ であるから，$\overline{\phi}$ は全射である．単射性を示す．G の単位元を e，G' の単位元 (=$\operatorname{Im}\phi$ の単位元) を e' と書く．$\overline{\phi}(g\operatorname{Ker}\phi) = e'$ となるとき，$\overline{\phi}$ の定義より，$\phi(g) = e'$．よって，$g \in \operatorname{Ker}\phi$．これは，$g \overset{\operatorname{Ker}\phi}{\sim}_L e$ に他ならないので，$g\operatorname{Ker}\phi = e\operatorname{Ker}\phi$ である．これより，

$$\operatorname{Ker}\overline{\phi} \coloneqq \{g\operatorname{Ker}\phi \in G/\operatorname{Ker}\phi \mid \overline{\phi}(g\operatorname{Ker}\phi) = e'\} = \{e\operatorname{Ker}\phi\}$$

がわかるが，剰余群の定義から $e\operatorname{Ker}\phi$ は $G/\operatorname{Ker}\phi$ の単位元なので第 10 回講義資料命題 9.4 (2) より，$\overline{\phi}$ が単射であることがわかる． □

例 1. 乗法群 $\mathbb{C}^\times$ から $\mathbb{R}^\times$ への絶対値を取る写像

$$|\cdot|\colon \mathbb{C}^\times \to \mathbb{R}^\times,\ z = x + iy \mapsto |z| \coloneqq \sqrt{x^2 + y^2}\ (x, y \in \mathbb{R})$$

* *e-mail* : hoya@shibaura-it.ac.jp

は準同型であり，

$$\operatorname{Ker}|\cdot| \coloneqq \{z \in \mathbb{C}^\times \mid |z| = 1\} = \{e^{i\theta} \mid \theta \in \mathbb{R}\} (=: \mathbb{T})$$
$$\operatorname{Im}|\cdot| \coloneqq \{r \in \mathbb{R}^\times \mid \text{ある } z \in \mathbb{C}^\times \text{が存在して，} r = |z|\} = \mathbb{R}_{>0}$$

となるのであった (第 10 回講義資料例 2)．よって，準同型定理より，

$$\mathbb{C}^\times/\mathbb{T} \xrightarrow{\sim} \mathbb{R}_{>0},\ z\mathbb{T} \mapsto |z|$$

は同型である．これは “複素数平面において偏角の違い ($\mathbb{T}$ の元倍の差) を同一視すると結局原点からの距離 ($\mathbb{R}_{>0}$) だけを見ていることになる” という事実に対応している．

ちなみに，

$$\phi\colon \mathbb{C}^\times \to \mathbb{T},\ z \mapsto \frac{z}{|z|}$$

という写像を考えるとこれも準同型となっており (チェックせよ．また，任意の $z \in \mathbb{C}^\times$ に対し，$\frac{z}{|z|} \in \mathbb{T}$ であることもあわせて確認せよ．)，

$$\operatorname{Ker}\phi \coloneqq \{z \in \mathbb{C}^\times \mid \frac{z}{|z|} = 1\} = \{z \in \mathbb{C}^\times \mid z = |z|\} = \mathbb{R}_{>0}$$
$$\operatorname{Im}\phi \coloneqq \{t \in \mathbb{T} \mid \text{ある } z \in \mathbb{C}^\times \text{が存在して，} t = \frac{z}{|z|}\} = \mathbb{T}$$

である．なお，最後の等式については任意の $\theta \in \mathbb{R}$ に対し，$\frac{e^{i\theta}}{|e^{i\theta}|} = e^{i\theta}$ であることよりわかる．こちらに対して準同型定理を用いると，

$$\mathbb{C}^\times/\mathbb{R}_{>0} \xrightarrow{\sim} \mathbb{T},\ z\mathbb{R}_{>0} \mapsto \frac{z}{|z|}$$

が同型であることがわかる．こちらは “複素数平面において原点からの距離のみが違う元 ($\mathbb{R}_{>0}$ の元倍の差) を同一視すると結局偏角 ($\mathbb{T}$) だけを見ていることになる” という事実に対応している．

例 2. 加法群 $\mathbb{R}$ から乗法群 $\mathbb{C}^\times$ への写像

$$\phi\colon \mathbb{R} \to \mathbb{C}^\times,\ \theta \mapsto e^{2\pi i\theta}$$

は準同型である．実際，任意の $\theta_1, \theta_2 \in \mathbb{R}$ に対し，

$$\phi(\theta_1 + \theta_2) = e^{2\pi i(\theta_1+\theta_2)} = e^{2\pi i\theta_1}e^{2\pi i\theta_2} = \phi(\theta_1)\phi(\theta_2)$$

が成立する．このとき，

$$\operatorname{Ker}\phi \coloneqq \{\theta \in \mathbb{R} \mid e^{2\pi i\theta} = 1\} = \mathbb{Z},$$
$$\operatorname{Im}\phi \coloneqq \{z \in \mathbb{C}^\times \mid \text{ある}\theta \in \mathbb{R} \text{ が存在して，} z = e^{2\pi i\theta}\} = \mathbb{T}.$$

よって，準同型定理より，

$$\mathbb{R}/\mathbb{Z} \xrightarrow{\sim} \mathbb{T},\ \theta + \mathbb{Z} \mapsto e^{2\pi i\theta}$$

は同型である．

例 3. n を正の整数とし，$\mathbb{K}$ を $\mathbb{Q}, \mathbb{R}$ または $\mathbb{C}$ とする．n 次一般線型群 $GL_n(\mathbb{K})$ の各元に対し，その行列式を与える写像

$$\det\colon GL_n(\mathbb{K}) \to \mathbb{K}^\times,\ A \mapsto \det(A)$$

は全射準同型であり，

$$\operatorname{Ker}\det \coloneqq \{A \in GL_n(\mathbb{K}) \mid \det(A) = 1\} = SL_n(\mathbb{K})$$

となるのであった (第 10 回講義資料例 5)．よって，準同型定理より，

$$GL_n(\mathbb{K})/SL_n(\mathbb{K}) \xrightarrow{\sim} \mathbb{K}^\times,\ A \cdot SL_n(\mathbb{K}) \mapsto \det(A)$$

が同型であることがわかる．

例 4. n を 2 以上の整数とする．n 次対称群 $\mathfrak{S}_n$ の各元に対し，その符号を与える写像

$$\operatorname{sgn}\colon \mathfrak{S}_n \to \{1,-1\}, \sigma \mapsto \operatorname{sgn}\sigma$$

は全射準同型であり，

$$\operatorname{Ker}\operatorname{sgn} \coloneqq \{\sigma \in \mathfrak{S}_n \mid \operatorname{sgn}\sigma = 1\} =: \mathfrak{A}_n \ (n \text{ 次交代群})$$

となるのであった (第 10 回講義資料例 6)．よって，準同型定理より，

$$\mathfrak{S}_n/\mathfrak{A}_n \xrightarrow{\sim} \{1,-1\},\ \sigma\mathfrak{A}_n \mapsto \operatorname{sgn}\sigma$$

が同型であることがわかる．

例 5. 任意の有限巡回群 $G = \langle g\rangle = \{g^m \mid m \in \mathbb{Z}\},\ \operatorname{ord} g < \infty$ に対し，

$$p\colon \mathbb{Z} \to G,\ m \mapsto g^m$$

は全射準同型であり，

$$\operatorname{Ker} p = \langle \operatorname{ord} g\rangle = \{k \operatorname{ord} g \mid k \in \mathbb{Z}\} = (\operatorname{ord} g)\mathbb{Z}.$$

となるのであった (第 10 回講義資料例 8)．よって，準同型定理より，

$$\mathbb{Z}/(\operatorname{ord} g)\mathbb{Z} \xrightarrow{\sim} G,\ [m]_{\operatorname{ord} g} \mapsto g^m$$

が同型であることがわかる．よって，第 10 回講義資料例 8 の $\operatorname{ord} g = \infty$ の場合の考察と合わせて以下の命題が言える：

命題 10.2

n を正の整数とすると，位数が n の巡回群は必ず $\mathbb{Z}/n\mathbb{Z}$ と同型である．また，位数が無限の巡回群は必ず $\mathbb{Z}$ と同型となる．

さらに，第 8 回講義資料系 7.6 と合わせると次が言える．

命題 10.3

位数が素数 p の群は必ず $\mathbb{Z}/p\mathbb{Z}$ と同型である．

※以下のこの章の内容はおそらく講義内では時間的に扱えないものである．難しさを感じる方はここから 10.2 節に飛んでもらって構わない．一方で以下は興味のある方には是非勉強してほしい事項である．もしもこの範囲について質問がある場合には，講義前後の時間に是非質問をしてもらいたい．

コラム：有限群の分類

命題 10.3 では群の位数を素数とすると，そのような群は同型なものを同一視すると 1 通りしかないということを見た．群の定義は非常に抽象的なものであったのに，位数によってはこれほどまでに構造がきっちりと決まってしまうというのは大変面白い話である．このように，「正の整数 n を与えたときに，同型なものを同一視したうえで位数 n の群は何通りあるか?」という問題を**位数 n の群の分類問題**という．その中でも特に大事なのは，以下で定義される単純群の分類である．

定義 10.4

群 G が自明な正規部分群 $G, \{e\}$ 以外に正規部分群を持たないとき，G を**単純群 (simple group)** という．

もし群 G が単純群でない場合，G は非自明な正規部分群 N を含む．このとき，G の構造は，正規部分群 N とそれによる剰余群 G/N という G よりも小さな群を調べることから調べ始めることができる (もちろん N と G/N の構造が分かれば G の構造が全てわかるわけではないのだが，大きな助けにはなる)．この意味で，これ以上分割できない “群論の世界の原子” に当たるものが単純群なのである．これは自然数の世界で素数が重要

であったこととも似ていると考えればその重要性がわかるであろう．そして，なんと驚くべきことに有限単純群の分類はわかっているのである！分類は以下の通りである．

(1) 巡回群 $\mathbb{Z}/p\mathbb{Z}$，p は素数.
(2) 交代群 $\mathfrak{A}_n$，$n \geq 5$. (第 10 回講義資料例 6 参照)
(3) Lie 型の単純群 (Tits 群を含む).
(4) 26 個の散在型単純群.

(1)–(3) の型については，それぞれ無限個存在しており，それ以外だと (4) の 26 個だけになるという状況である．(4) の 26 個の例外の中で最も大きい群の位数は

$$808017424794512875886459904961710757005754368000000000$$

であり，**モンスター群**と呼ばれる．この分類定理は (主に)20 世紀の多くの数学者による膨大な研究の賜物であり，証明を説明することは到底できないが，結果としては知っていても良いであろう．歴史的な部分やより詳細について知りたい方は，『鈴木 通夫, “有限単純群の分類”, 数学, 1982 年 34 巻 3 号, 193–210 https://doi.org/10.11429/sugaku1947.34.193』などが参考になる．他にも「有限単純群の分類」で検索すると様々な面白い記事に当たることができる．

例 6 (やや発展)**.** G を群とする．G から自己同型群 $\mathrm{Aut}(G) \coloneqq \{\phi\colon G \to G \mid \phi\text{は同型}\}$ への写像

$$\alpha\colon G \to \mathrm{Aut}(G),\ a \mapsto \alpha_a$$

(ただし，α_a は $\alpha_a\colon G \to G,\ g \mapsto aga^{-1}$ で定まる写像．) は準同型であり，

$$\begin{aligned}\mathrm{Ker}\,\alpha &= Z(G)\ (G\text{ の中心})\\ \mathrm{Im}\,\alpha &\coloneqq \{\alpha_a \mid a \in G\}(=: \mathrm{Inn}(G))\end{aligned}$$

となるのであった (第 10 回講義資料例 11)．よって，準同型定理より，

$$G/Z(G) \xrightarrow{\sim} \mathrm{Inn}(G),\ gZ(G) \mapsto \alpha_g$$

が同型であることがわかる．一見とらえどころのない内部自己同型群 $\mathrm{Inn}(G)$ は $G/Z(G)$ に同型だったのである．例えば，n を正の整数とし，$\mathbb{K}$ を $\mathbb{Q}, \mathbb{R}$ または $\mathbb{C}$ とするとき，

$$\mathrm{Inn}(GL_n(\mathbb{K})) \simeq GL_n(\mathbb{K})/Z(GL_n(\mathbb{K})) =: PGL_n(\mathbb{K})\ (\text{射影一般線型群})$$

となる．射影一般線型群は 一般線型群の内部自己同型群に同型な群だったのである．

定理 10.5 (第 2 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．このとき，

$$HN \coloneqq \{hn \mid h \in H, n \in N\}$$

は G の部分群，$H \cap N$ は H の正規部分群であり，

$$H/(H \cap N) \to HN/N,\ h(H \cap N) \mapsto hN \tag{10.1}$$

は well-defined な群同型になる．特に，$H/(H \cap N) \simeq HN/N$ である．

証明.

HN が G の部分群であること： 任意の $h_1n_1, h_2n_2 \in HN$ $(h_1, h_2 \in H, n_1, n_2 \in N)$ に対し，

$$h_1n_1h_2n_2 = h_1h_2(h_2^{-1}n_1h_2)n_2.$$

いま N は正規部分群なので $h_2^{-1}n_1h_2 \in N$ であるから，$(h_2^{-1}n_1h_2)n_2 \in N$ であるので，上式の右辺は HN の元である．よって，$h_1n_1h_2n_2 \in HN$.

任意の $hn \in HN$ $(h \in H, n \in N)$ に対して，

$$(hn)^{-1} = n^{-1}h^{-1} = h^{-1}(hn^{-1}h^{-1}).$$

いま N は正規部分群なので $hn^{-1}h^{-1} \in N$ であるから，上式の右辺は HN の元である．よって，$(hn)^{-1} \in HN$．以上より，HN は二項演算と逆元を取る操作で閉じているので，G の部分群である．

$H \cap N$ が H の正規部分群であること，(10.1) が well-defined な群同型であること： 写像

$$\phi\colon H \to HN/N,\ h \mapsto hN$$

を考える．任意の $h_1, h_2 \in H$ に対し，$\phi(h_1h_2) = h_1h_2N = h_1N \cdot h_2N = \phi(h_1) \cdot \phi(h_2)$ となるので，ϕ は準同型である．また，任意の $h \in H, n \in N$ に対して，$hnN = hN \in HN/N$ なので，

$$HN/N = \{hnN \mid h \in H, n \in N\} = \{hN \mid h \in H\} = \operatorname{Im}\phi.$$

さらに，

$$\operatorname{Ker}\phi = \{h \in H \mid hN = N\} = \{h \in H \mid h \in N\} = H \cap N.$$

これより，第 10 回講義資料命題 9.3 (2) から $H \cap N$ は H の正規部分群であり，準同型定理から，

$$H/(H \cap N) \xrightarrow{\sim} HN/N,\ h(H \cap N) \mapsto hN$$

は well-defined な群同型になる． □

例 7. n を 3 以上の整数とし，$D_n = \{\sigma^k\tau^\ell \mid k = 0, \dots, n-1, \ell = 0, 1\}$ を n 次二面体群とする $(\sigma^n = e, \tau^2 = e, \sigma^k\tau = \tau\sigma^{-k}\ (k \in \mathbb{Z}))$．$H = \langle\tau\rangle = \{e, \tau\}, N = \langle\sigma\rangle = \{e, \sigma, \dots, \sigma^{n-1}\}$ とする．H は D_n の正規でない部分群であり，N は D_n の正規部分群であったことを思い出そう (第 9 回講義資料例 2，命題 8.3 参照)．このとき，

$$HN \coloneqq \{\tau^\ell\sigma^k \mid \ell = 0, 1, k = 0, \dots, n-1\} = D_n \qquad H \cap N = \{e\}$$

であるので，第 2 同型定理より，

$$H/\{e\} = H \xrightarrow{\sim} D_n/N,\ \tau^\ell \mapsto \tau^\ell N\ (\ell = 0, 1)$$

は well-defined な群同型になる．

定理 10.6 (第 3 同型定理)

G を群，M, N を $M \subset N$ を満たす G の正規部分群とする．このとき，剰余群 N/M は剰余群 G/M の正規部分群であり，

$$(G/M)/(N/M) \to G/N,\ (gM) \cdot N/M \mapsto gN$$

は well-defined な群同型になる．特に，$(G/M)/(N/M) \simeq G/N$ である．(M を “約分” できる．)

証明. 写像

$$\phi\colon G/M \to G/N,\ gM \mapsto gN$$

を考える．これが well-defined であることは以下のように確かめられる：

$$g_1M = g_2M \text{ であるとき，} g_1N = g_2N$$

となることを示せばよい．$g_1M = g_2M$ のとき，$g_1 \overset{M}{\sim}_L g_2$ なので，ある $m \in M$ が存在して，$g_1 = g_2m$ となる．いま $M \subset N$ であるので，m は N の元でもあるから，このとき $g_1 \overset{N}{\sim}_L g_2$ でもある．よって，$g_1N = g_2N$.

いま，任意の $g_1, g_2 \in G$ に対し，$\phi(g_1M \cdot g_2M) = \phi(g_1g_2M) = g_1g_2N = g_1N \cdot g_2N = \phi(g_1M) \cdot \phi(g_2M)$ となるので，ϕ は準同型である．また，

$$\begin{aligned}\operatorname{Im}\phi &= \{\phi(gM) \mid g \in G\} = \{gN \mid g \in G\} = G/N,\\ \operatorname{Ker}\phi &= \{gM \in G/M \mid gN = N\} = \{gM \in G/M \mid g \in N\} = N/M.\end{aligned}$$

よって，第 10 回講義資料命題 9.3 (2) から N/M は G/M の正規部分群であり，準同型定理から，

$$(G/M)/(N/M) \xrightarrow{\sim} G/N,\ (gM) \cdot N/M \mapsto gN$$

は well-defined な群同型になる． □

例 8. $\mathbb{R}$ 上の 2 次一般線型群 $GL_2(\mathbb{R})$ からの写像

$$\phi\colon GL_2(\mathbb{R}) \to \{1, -1\},\ A \mapsto \frac{\det(A)}{|\det(A)|}$$

を考えるとこれは全射準同型である (チェックせよ)．このとき，

$$\begin{aligned}\operatorname{Ker}\phi &\coloneqq \{A \in GL_2(\mathbb{R}) \mid \frac{\det(A)}{|\det(A)|} = 1\}\\ &= \{A \in GL_2(\mathbb{R}) \mid \det(A) = |\det(A)|\}\\ &= \{A \in GL_2(\mathbb{R}) \mid \det(A) > 0\} =: GL_2^+(\mathbb{R})\end{aligned}$$

となる (この正規部分群は第 9 回レポート課題で扱った)．よって，準同型定理より，

$$GL_2(\mathbb{R})/GL_2^+(\mathbb{R}) \xrightarrow{\sim} \{1, -1\},\ A \cdot GL_2^+(\mathbb{R}) \mapsto \frac{\det(A)}{|\det(A)|}$$

が同型であることがわかる．ここで，$GL_2(\mathbb{R})$ の中心は

$$Z(GL_2(\mathbb{R})) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \;\middle|\; a \in \mathbb{R}^\times \right\}$$

であり (第 6 回講義資料例 5)，任意の $a \in \mathbb{R}^\times$ に対し，$\det \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = a^2 > 0$ なので，$Z(GL_2(\mathbb{R}))$ は $GL_2^+(\mathbb{R})$ の部分群である．これより，G を $GL_2(\mathbb{R})$，M を $Z(GL_2(\mathbb{R}))$，N を $GL_2^+(\mathbb{R})$ とすると，これは第 3 同型定理が適用できる状況になっている．よって，第 3 同型定理より，

$$\begin{array}{ccc}(GL_2(\mathbb{R})/Z(GL_2(\mathbb{R})))/(GL_2^+(\mathbb{R})/Z(GL_2(\mathbb{R}))) & \xrightarrow{\sim} & GL_2(\mathbb{R})/GL_2^+(\mathbb{R})(\simeq \{1, -1\}),\\ \cup & & \cup \\ (A \cdot Z(GL_2(\mathbb{R}))) \cdot GL_2^+(\mathbb{R})/Z(GL_2(\mathbb{R})) & \mapsto & A \cdot GL_2^+(\mathbb{R})\end{array}$$

は well-defined な群同型になる．ちなみに，$GL_2(\mathbb{R})/Z(GL_2(\mathbb{R}))$ は $PGL_2(\mathbb{R})$ と書かれたことも合わせて思い出しておこう．

10.2 中国式剰余定理

準同型定理の応用として，中国式剰余定理を述べよう．このために 1 つ用語を準備する．

定義 10.7

G_1, G_2 を群とし，それぞれの単位元を e_1, e_2 とする．G_1 と G_2 直積集合

$$G_1 \times G_2 \coloneqq \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}$$

に二項演算 $\cdot\colon (G_1 \times G_2) \times (G_1 \times G_2) \to G_1 \times G_2$ を

$$(g_1, g_2) \cdot (h_1, h_2) \coloneqq (g_1 h_1, g_2 h_2),\ \forall g_1, h_1 \in G,\ g_2, h_2 \in G_2$$

と定義する．この二項演算によって，$G_1 \times G_2$ は再び群となる (チェックは容易なのでここでは省略する．試してみよ．)．ここで，$G_1 \times G_2$ の単位元は (e_1, e_2) であり，(g_1, g_2) の逆元は (g_1^{-1}, g_2^{-1}) である．この群を G_1 と G_2 の**直積 (direct product)** という．

以下は直積の基本性質である．この命題も証明は容易なので省略する．

命題 10.9

G_1, G_2 を群とし，それぞれの単位元を e_1, e_2 とする．このとき，以下が成立する．

(1) $G_1 \times G_2$ の位数は $|G_1| \cdot |G_2|$ である．
(2) $\mathrm{pr}_1\colon G_1 \times G_2 \to G_1,\ (g_1, g_2) \mapsto g_1$，$\mathrm{pr}_2\colon G_1 \times G_2 \to G_2,\ (g_1, g_2) \mapsto g_2$ は全射準同型である．(**自然な射影 (canonical projection)** と呼ばれる．)
(3) $\iota_1\colon G_1 \to G_1 \times G_2,\ g_1 \mapsto (g_1, e_2)$，$\iota_2\colon G_2 \to G_1 \times G_2,\ g_2 \mapsto (e_1, g_2)$ は単射準同型である．(**自然な入射 (canonical injection)** と呼ばれる．)
(4) $\mathrm{Ker}\,\mathrm{pr}_2 = \mathrm{Im}\,\iota_1 = G_1 \times \{e_2\} \simeq G_1, \mathrm{Ker}\,\mathrm{pr}_1 = \mathrm{Im}\,\iota_2 = \{e_1\} \times G_2 \simeq G_2$．とくに，$G_1 \simeq G_1 \times \{e_2\}$，$G_2 \simeq \{e_1\} \times G_2$ は $G_1 \times G_2$ の正規部分群である．

例 9. $\mathbb{Z}/2\mathbb{Z}$ と $\mathbb{Z}/3\mathbb{Z}$ の直積 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ を考えてみよう．まず集合としては，

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = \{([0]_2, [0]_3), ([0]_2, [1]_3), ([0]_2, [2]_3), ([1]_2, [0]_3), ([1]_2, [1]_3), ([1]_2, [2]_3)\}$$

であり，位数は $2 \cdot 3 = 6$ である (命題 10.9 (1))．二項演算は例えば，

$$([1]_2, [1]_3) + ([0]_2, [2]_3) = ([1]_2 + [0]_2, [1]_3 + [2]_3) = ([1]_2, [0]_3)$$

というようにそれぞれの成分ごとに計算される (ここでは直積を考えている群が共に加法群なので直積の二項演算も $+$ で書いた)．ちなみに，

$([1]_2, [1]_3) + ([1]_2, [1]_3) = ([0]_2, [2]_3)$　$([0]_2, [2]_3) + ([1]_2, [1]_3) = ([1]_2, [0]_3)$　$([1]_2, [0]_3) + ([1]_2, [1]_3) = ([0]_2, [1]_3)$
$([0]_2, [1]_3) + ([1]_2, [1]_3) = ([1]_2, [2]_3)$　$([1]_2, [2]_3) + ([1]_2, [1]_3) = ([0]_2, [0]_3)$

となるので，$\mathrm{ord}([1]_2, [1]_3) = 6$ であり，$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ は $([1]_2, [1]_3)$ によって生成される巡回群 $\langle([1]_2, [1]_3)\rangle$ であることがわかる．よって，命題 10.2 より，これは $\mathbb{Z}/6\mathbb{Z}$ と同型であり，具体的な同型写像は

$$\mathbb{Z}/6\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z},\ [a]_6 \mapsto ([a]_2, [a]_3)$$

で与えられることがわかる (生成元 $[1]_6$ を生成元 $([1]_2, [1]_3)$ にうつした)．次の中国式剰余定理はこの同型の一般化である．

定理 10.10 (中国式剰余定理)

n_1, n_2 を互いに素な2 以上の自然数とする．このとき，

$$\mathbb{Z}/n_1 n_2\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z},\ [a]_{n_1 n_2} \mapsto ([a]_{n_1}, [a]_{n_2})$$

は well-defined な群同型となる．特に，$\mathbb{Z}/n_1 n_2\mathbb{Z} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ である．

証明. 写像

$$\phi\colon \mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z},\ a \mapsto ([a]_{n_1}, [a]_{n_2})$$

を考える．任意の $a, b \in \mathbb{Z}$ に対し，$\phi(a+b) = ([a+b]_{n_1}, [a+b]_{n_2}) = ([a]_{n_1}, [a]_{n_2}) + ([b]_{n_1}, [b]_{n_2}) = \phi(a) + \phi(b)$ となるので，ϕ は準同型である．また，

$$\begin{aligned}
\operatorname{Ker}\phi &= \{a \in \mathbb{Z} \mid ([a]_{n_1}, [a]_{n_2}) = ([0]_{n_1}, [0]_{n_2})\} \\
&= \{a \in \mathbb{Z} \mid a \text{ は } n_1 \text{と } n_2 \text{で割り切れる}\} \\
&= \{a \in \mathbb{Z} \mid a \text{ は } n_1 n_2 \text{で割り切れる}\} \text{ (ここで，} n_1 \text{と } n_2 \text{が互いに素であることを用いた.)} \\
&= \{n_1 n_2 k \in \mathbb{Z} \mid k \in \mathbb{Z}\} = n_1 n_2 \mathbb{Z}
\end{aligned}$$

これより，準同型定理から，

$$Z/n_1 n_2\mathbb{Z} \xrightarrow{\sim} \operatorname{Im}\phi,\ [a]_{n_1 n_2} \mapsto ([a]_{n_1}, [a]_{n_2})$$

は well-defined な群同型になる．ここで，$\operatorname{Im}\phi$ は $Z/n_1 n_2\mathbb{Z}$ と同型であることから位数 $n_1 n_2$ の群となるが，一方 $\operatorname{Im}\phi$ は位数 $n_1 n_2$ の群である $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ の部分群であったことに注意すると，結局 $\operatorname{Im}\phi = \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ となることがわかる．よって，

$$Z/n_1 n_2\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z},\ [a]_{n_1 n_2} \mapsto ([a]_{n_1}, [a]_{n_2})$$

が同型となることがわかる． □

ちなみに，中国式剰余定理の仮定である「n_1, n_2 は互いに素」は重要であり，実際 n_1, n_2 が互いに素でないとき必ず

$$\mathbb{Z}/n_1 n_2\mathbb{Z} \not\simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$$

となる．例えば，$\mathbb{Z}/60\mathbb{Z} \not\simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ などとなる．今回の本レポート課題となっているので，理由を考えてみて欲しい (ヒント：各元の位数に着目せよ)．

最後にこの定理の “意味” を考えてみよう．$\mathbb{Z}/n\mathbb{Z}$ において $[a]_n$ は “a を n で割った余りを見る” というように考えられるのであった．このため，n_1 と n_2 が互いに素のとき，

$$\phi_{n_1.n_2}\colon \mathbb{Z}/n_1 n_2\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z},\ [a]_{n_1 n_2} \mapsto ([a]_{n_1}, [a]_{n_2})$$

という同型が存在するという事実は，

> n_1 と n_2 が互いに素のとき，任意の $0 \le r_1 < n_1, 0 \le r_2 < n_2$ に対して，『n_1 で割った余りが r_1，n_2 で割った余りが r_2 となるような整数 a』[*1]が $\bmod n_1 n_2$ でただ一つ存在する．

ということに他ならない．$\phi_{n_1.n_2}$ が全単射なので，任意の $0 \le r_1 < n_1, 0 \le r_2 < n_2$ に対して，$\phi^{-1}_{n_1.n_2}(([r_1]_{n_1}, [r_2]_{n_2})) \in \mathbb{Z}/n_1 n_2\mathbb{Z}$ が定まり，これを $[a]_{n_1 n_2}$ とすると，a は n_1 で割った余りが r_1，n_2 で割った余りが r_2 となるような整数なのである．

具体的には次のように計算すればよい．

[*1] このような数を求める問題が古代中国の文献『孫子算経』に登場しており，そのことが中国式剰余定理という名前の由来となっている．

n_1 と n_2 を互いに素な整数としたとき，n_1 で割った余りが r_1，n_2 で割った余りが r_2 となるような整数 a を求める $(0 \leq r_1 < n_1, 0 \leq r_2 < n_2)$.

(Step 1) 拡張ユークリッド互除法を用いて $n_1x + n_2y = 1$ を満たす整数の組 (x, y) を 1 つ求める (第 1, 2 回講義資料参照)．見つけた解を (x_0, y_0) とする．

(Step 2) いま，

$$\phi_{n_1.n_2}([n_1x_0]_{n_1n_2}) = ([n_1x_0]_{n_1}, [n_1x_0]_{n_2}) = ([n_1x_0]_{n_1}, [n_1x_0 + n_2y_0]_{n_2}) = ([0]_{n_1}, [1]_{n_2})$$
$$\phi_{n_1.n_2}([n_2y_0]_{n_1n_2}) = ([n_2y_0]_{n_1}, [n_2y_0]_{n_2}) = ([n_1x_0 + n_2y_0]_{n_1}, [n_2y_0]_{n_2}) = ([1]_{n_1}, [0]_{n_2})$$

であることに注意すると，

$$\begin{aligned}\phi_{n_1.n_2}([r_2n_1x_0 + r_1n_2y_0]_{n_1n_2}) &= \phi_{n_1.n_2}([r_2n_1x_0]_{n_1n_2}) + \phi_{n_1.n_2}([r_1n_2y_0]_{n_1n_2}) \\ &= ([0]_{n_1}, [r_2]_{n_2}) + ([r_1]_{n_1}, [0]_{n_2}) = ([r_1]_{n_1}, [r_2]_{n_2}).\end{aligned}$$

となることがわかるので，

$$\phi^{-1}_{n_1.n_2}(([r_1]_{n_1}, [r_2]_{n_2})) = [r_2n_1x_0 + r_1n_2y_0]_{n_1n_2}.$$

よって，求める a は $r_2n_1x_0 + r_1n_2y_0 + n_1n_2k$ (k は任意の整数).

この解法を用いて 1 つ問題を解いてみよう．

例題

39 で割ると 2 余り，119 で割ると 3 余る整数を 1 つ求めよ.

解答例.【まず拡張ユークリッド互除法で $39x + 119y = 1$ を満たす整数の組 (x, y) を見つける.】

$$119 = 3 \times 39 + 2 \qquad 39 = 19 \times 2 + 1$$

より，$1 = 39 - 19 \times 2 = 39 - 19 \times (119 - 3 \times 39) = 58 \times 39 + (-19) \times 119.$

【$(x_0, y_0) = (58, -19), r_1 = 2, r_2 = 3$ として，$r_2(39x_0) + r_1(119y_0)$ を計算】

これより求める値の 1 つは，

$$3 \times (39 \times 58) + 2 \times (119 \times (-19)) = 2264.$$

□

※この解法において，r_1 を n_2y_0 の方に掛けて，r_2 を n_1x_0 の方に掛けないといけないという点は間違えがちである.「この方法でなぜ求まるか」という原理も含めて解法を覚えておくことが望ましい．また，この問題は検算ができるので検算を行うこと.