「代数と数論の基礎」(中島匠一)　第 1 章の章末問題の解答例

問題 1.1　答えは、$n = 1, 2$ と 8 以上のすべての自然数 n である。

7 以下の n で不等式をみたすものが $n = 1, 2$ だけであることは、簡単な計算で確かめられる。つぎに、$n \geq 8$ ならば $2^{n+1} \geq n^3$ であることを数学的帰納法により証明する。まず、$n = 8$ のときは、両辺とも 2^9 に等しいので、不等号が（等号として）成り立っている。つぎに、$2^{n+1} \geq n^3$ が成り立つと仮定する。このとき、

$$\begin{aligned}
2^{n+2} - (n+1)^3 &= 2 \times 2^{n+1} - (n+1)^3 \\
&\geq 2n^3 - (n+1)^3 \quad (\text{数学的帰納法の仮定による}) \\
&= n^3 - 3n^2 - 3n - 1 \\
&= n^3 \left(1 - \frac{3}{n} - \frac{3}{n^2} - \frac{1}{n^3}\right) \\
&\geq n^3 \left(1 - \frac{3}{8} - \frac{3}{8^2} - \frac{1}{8^3}\right) \quad (n \geq 8 \text{ による}) \\
&> n^3 \left(1 - \frac{3}{8} - \frac{3}{8} - \frac{1}{8}\right) \\
&= \frac{n^3}{8} > 0
\end{aligned}$$

であるので、$2^{(n+1)+1} \geq (n+1)^3$ が成り立つことがわかる。以上で、数学的帰納法により、$2^{n+1} \geq n^3$ $(n \geq 8)$ が証明された。

補足： 上の議論で、$n \geq 9$ ならば $2^{n+1} > n^3$ が成り立つことも示せている。

問題 1.2　両者とも同じ方針で証明できるが、参考のために、それぞれに異なった「風味」の証明を与えておく。

(1) 白玉と黒玉がそれぞれ n 個ずつあるとし、合計 $2n$ 個の玉から（色は問題にせずに）n 個の球を取り出す取り出し方を 2 通りの方法で計算する。まず、$2n$ 個のものから n 個を取り出すのであるから、その総数は $\binom{2n}{n}$ である。つぎに、$0 \leq k \leq n$ をみたす k に対して、n 個の玉の中の白玉の個数が k である場合（したがって、黒玉の個数は $n-k$）の取り出し方を考える。すると、白玉の選び方は $\binom{n}{k}$ 通りあり、それぞれに対して黒玉の選び方が $\binom{n}{n-k}$ 通りあるので、両者を掛け合わせて、選び方が $\binom{n}{k}\binom{n}{n-k}$ 通りであることがわかる。したがって、n 個の玉の取り出し方の数は $\displaystyle\sum_{k=0}^{n} \binom{n}{k}\binom{n}{n-k}$ となる。

2 通りに数えた取り出し方の数は等しいので、等式

$$\sum_{k=0}^{n} \binom{n}{k}\binom{n}{n-k} = \binom{2n}{n}$$

が成り立つ。2 項係数の一般的性質 $\binom{n}{n-k} = \binom{n}{k}$（命題 1.1(2) 参照）を適用すれば、この等式から問題の等式が得られる。

(2) x を変数として、多項式 $(1+x)^{2n}$ の x^{n-1} の係数を N とする。まず、$(1+x)^{2n}$ に 2 項定理（命題 1.2）を適用して、$N = \binom{2n}{n-1}$ がわかる。つぎに、$(1+x)^{2n} = (1+x)^n \times (1+x)^n$ と因数分解する。ここで、2 つの $(1+x)^n$ のそれぞれを 2 項定理で展開すると、左側の $(1+x)^n$ の x^k の係数は $\binom{n}{k}$ で、右

側の $(1+x)^n$ の x^{n-1-k} の係数は $\binom{n}{n-1-k}$ である（$0 \leq k \leq n-1$）。x^k と x^{n-1-k} を掛け合わせて x^{n-1} が得られるので、$N = \sum_{k=0}^{n-1} \binom{n}{k}\binom{n}{n-1-k}$ が成り立つ。

最後に、N の 2 つの表示式を較べて、$\binom{n}{n-1-k} = \binom{n}{n-(n-1-k)} = \binom{n}{k+1}$ を使えば、問題の等式が得られる。

問題 1.3　(1) $n > ab$ だとする。定理 1.7 により $ax + by = 1$ をみたす整数 x, y がとれて、この等式の両辺を n 倍して、$a(nx) + b(ny) = n$ が成り立つ。ここで、

$$nx = qb + u \quad (q, u \text{ は整数で } 1 \leq u \leq b)$$

をみたす q, u をとる（注：$u = (nx \text{ を } b \text{ で割った余り}) + 1$）。そして、この q を使って $v = ny + qa$ とおくと、v は整数であり

$$au + bv = a(nx - qb) + b(ny + qa) = a(nx) + b(ny) = n$$

が成り立つ。さらに、この等式と $u \leq b, n > ab, a > 0, b > 0$ により

$$v = \frac{n - au}{b} \geq \frac{n - ab}{b} > 0$$

が成り立つので、v は自然数である。これで (1) が示された。

(2) 求める個数は $\dfrac{(a+1)(b+1)}{2} - 1$ である。

以下、理由を説明する。

まず、$au + bv = ab$ をみたす自然数 u, v は存在しないことを確認する。（理由：$au + bv = ab$ なら $au = b(a - v)$ なので、a, b が互いに素であることから、$a - v$ は a の倍数でなくてはならない。しかし、u, v が自然数であることから $0 < a - v < a$ であるので、それは不可能である。）このことと (1) により、「$n < ab$ である自然数 n で、$au + bv = n$ をみたす自然数 u, v が存在しないものの個数」を N とすれば、問題の答えは $N + 1$ である（注：$N + 1$ の 1 は $n = ab$ の分）。まず、自然数 u, v が $au + bv < ab$ をみたすなら $1 \leq u \leq b-1, 1 \leq v \leq a-1$ であることがすぐにわかる。また、$1 \leq u, u' \leq b-1, 1 \leq v, v' \leq a-1$ について $au + bv = au' + bv'$ が成り立つなら、$u = u', v = v'$ でなくてはならない。（理由：$au + bv = au' + bv'$ なら $a(u - u') = b(v' - v)$ となるが、a, b は互いに素であるから、$u - u'$ は b の倍数で $v' - v$ は a の倍数でなくてはならない；しかし、$-b < u - u' < b, -a < v' - v < a$ であるから、そうなるのは $u = u', v = v'$ のときだけ。）以上により、条件

$$1 \leq u \leq b-1, \quad 1 \leq v \leq a-1, \quad au + bv < ab$$

をみたす自然数 u, v の組の個数を L とすれば、$N = ab - 1 - L$ である（注：$ab - 1$ は $n < ab$ をみたす自然数 n の個数）。

以下では、u, v は $1 \leq u \leq b-1, 1 \leq v \leq a-1$ をみたす自然数を表すとする。ここで、条件 $au + bv > ab$ をみたす u, v の組の個数を M とおくと、$L + M$ は u, v の組の総数に等しいので、$L + M = (a-1)(b-1)$ が成り立つ。

u, v に対して $\hat{u} = b - u, \hat{v} = a - v$ とおけば $1 \leq \hat{u} \leq b-1, 1 \leq \hat{v} \leq a-1$ であり、

$$(au + bv) + (a\hat{u} + b\hat{v}) = 2ab$$

が成り立つ。この対応 $u, v \leftrightarrow \hat{u}, \hat{v}$ によって $au + bv < ab$ をみたす u, v と $a\hat{u} + b\hat{v} > ab$ をみたす $\hat{u}, \hat{v}$ が一対一に対応する。よって、$L = M$ である。これと $L + M = (a-1)(b-1)$ により、$2L = (a-1)(b-1)$ が得られる。

以上により、$L=\dfrac{(a-1)(b-1)}{2}$ であることがわかったので、

$$N=ab-1-\frac{(a-1)(b-1)}{2}=\frac{(a+1)(b+1)}{2}-2$$

である。したがって、問題の答えは $\dfrac{(a+1)(b+1)}{2}-1$ となる。

問題 1.4　$\alpha=\sqrt{2}+\sqrt{3}$ とおく。このとき $\alpha^2=5+2\sqrt{6}$ であるから、もし α が有理数なら $\sqrt{6}=\dfrac{\alpha^2-5}{2}$ も有理数でなくてはならない。しかし、$\sqrt{6}$ は無理数であることがわかっている（p.23 と同じ議論で証明できる)。したがって、α は有理数ではあり得ない。

（コメント）$\sqrt{6}$ が無理数であることは、多くの教科書で証明されている（たとえば、ウォルタース（中島 訳)「算数から始めよう! 数論」(岩波書店）命題 2.22)。また、同書の問題 2.32 の解答に、別の式変形を使った問題 1.4 の証明が書いてある。

問題 1.5　(1) 命題 1.15 から、

$$\mathrm{ord}_p(n!)=\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right]$$

がわかる。すると、実数 x について $[x]\le x$ がなりたつことと、$p^k>n$ なら $0=\left[\dfrac{n}{p^k}\right]<\dfrac{n}{p^k}$ であることから

$$\mathrm{ord}_p(n!)<\sum_{k=1}^{\infty}\frac{n}{p^k}=\frac{n/p}{1-1/p}=\frac{n}{p-1}$$

が得られる。

(2) 等比級数の和の公式により

$$\sum_{k=1}^{\infty}p^{-k}=\frac{1}{p-1}$$

が成り立つ。したがって、$c<\dfrac{1}{p-1}$ であれば、

$$c<\sum_{k=1}^{N}p^{-k}$$

をみたす自然数 N が存在する。この N に対して $n=p^N$ とおく。すると、命題 1.15 を利用すれば、

$$\begin{aligned}
\mathrm{ord}_p(n!) &= \sum_{k=1}^{\infty}\left[\frac{p^N}{p^k}\right] \\
&= \sum_{k=1}^{N}\left[\frac{p^N}{p^k}\right] \quad \left(k>N \text{ ならば } p^k>p^N \text{ なので } \left[\frac{p^N}{p^k}\right]=0\right) \\
&= \sum_{k=1}^{N}p^{N-k} \\
&= p^N\sum_{k=1}^{N}p^{-k} \\
&> nc
\end{aligned}$$

が成り立つことがわかる。

問題 1.6　n^5 と n の偶奇が一致することはすぐわかるので、$n^5 \equiv n \pmod 2$ が成り立つ。また、フェルマーの小定理（＝定理 1.29）、または直接の計算によって、

$$n^3 \equiv n \pmod 3, \quad n^5 \equiv n \pmod 5$$

が成り立つ。この最初の式から、

$$n^5 = n^3 \times n^2 \equiv n \times n^2 \equiv n^3 \equiv n \pmod 3$$

が得られる。以上で $n^5 - n$ が $2, 3, 5$ のすべてで割り切れることがわかったので、$n^5 - n$ は $\mathrm{lcm}(2, 3, 5) = 30$ で割り切れる。

問題 1.7　(1) 2 項係数の性質により、$2 \le k \le p^n$ に対して

$$\binom{p^n - 1}{k - 2} + \binom{p^n - 1}{k - 1} = \binom{p^n}{k - 1}, \quad (k - 1)\binom{p^n}{k - 1} = p^n \binom{p^n - 1}{k - 2} \tag{$*$}$$

が成り立っている（命題 1.1(2)(4) 参照）。$1 \le k - 1 < p^n$ より $k - 1$ は p^n では割り切れないので、$(*)$ の 2 番目の等式と p が素数であることから、$\binom{p^n}{k - 1} \equiv 0 \pmod p$ が導かれる（$2 \le k \le p^n$）。すると、$(*)$ の最初の等式から、

$$\binom{p^n - 1}{k - 1} \equiv -\binom{p^n - 1}{k - 2} \pmod p$$

が導かれる（$2 \le k \le p^n$）。この合同式を（k の値を変えながら）繰り返し使って、$\binom{p^n}{0} = 1$ に注意すれば、$\binom{p^n - 1}{k - 1} \equiv (-1)^{k-1} \pmod p$ が得られる。

(2) 2 項係数の性質（命題 1.1(4) 参照）により、

$$k\binom{p^n}{k} = p^n \binom{p^n - 1}{k - 1}$$

が成り立つ（$1 \le k \le p^n$）。この問題の (1) により $\mathrm{ord}_p\left(\binom{p^n - 1}{k - 1}\right) = 0$ であるので、この等式から

$$\mathrm{ord}_p\left(\binom{p^n}{k}\right) = n + \mathrm{ord}_p\left(\binom{p^n - 1}{k - 1}\right) - \mathrm{ord}_p(k) = n - \mathrm{ord}_p(k)$$

が得られる（$\mathrm{ord}_p(p^n) = n$ に注意）。

問題 1.8　x を変数とするとき、2 項定理（＝命題 1.2）によって $(1 + x)^n$ の x^k の係数が $\binom{n}{k}$ であることに注意する。また、命題 1.12 を繰り返し使えば、任意の自然数 a について合同式

$$(1 + x)^{p^a} \equiv 1 + x^{p^a} \pmod p \tag{$*$}$$

が成り立つことがわかる（$a = 1$ のときは命題 1.2 そのもので、あとは命題 1.2 を繰り返し使えば、a に関する数学的帰納法によって $(*)$ が証明される；詳細は省略）。

合同式 $(*)$ から、問題の $\Longrightarrow$ は直ちに示される。つまり、$n = p^a$ であれば、$k = 1, 2, \cdots, p^a - 1$ について $(*)$ の右辺の x^k の係数が 0 であることから、$\binom{n}{k} \equiv 0 \pmod p$ が導かれる。

つぎに、問題の $\Longleftarrow$ の対偶が成り立つことを証明するために、n が p のベキではないと仮定する。つまり、n を $n = p^a m$ (m は p と互いに素な自然数) と表すとき $m \ge 2$ であるとする。ここで $(*)$ の両辺を m 乗して、右辺に現れる式 $(1 + x^{p^a})^m$ に 2 項定理を適用すると

$$(1 + x)^n \equiv (1 + x^{p^a})^m \equiv 1 + mx^{p^a} + \cdots + x^n \pmod p$$

となる。この両辺の x^{p^a} の係数を較べて $\binom{n}{p^a} \equiv m \pmod{p}$ が導かれるが、m に関する仮定によって $\binom{n}{p^a} \not\equiv 0 \pmod{p}$ である。これは、$k = p^a$ について $\binom{n}{k} \equiv 0 \pmod{p}$ が成り立たないことを示している（$m \geq 2$ であるから $p^a < n$ であることに注意）。これで $\Longleftarrow$ の対偶が成り立つことがわかったので、$\Longleftarrow$ が証明された。

（コメント）この問題は例題 1.6 を利用して解答することもできる。ここでは、多項式の合同式を利用する方法を紹介した。

問題 1.9　自然数 n が 10 進法で $n = a_k a_{k-1} \cdots a_1 a_0$ と表されているとする。このとき、n が 11 で割り切れるための条件は、

$$a_0 - a_1 + a_2 - \cdots + (-1)^k a_k \text{ が } 11 \text{ で割り切れること}$$

である。

問題 1.10　(1) 10 以下のすべての自然数、および、$12, 14, 15, 16, 18, 20, 24, 30$。

（注：計算法は、まず、(2) の解答の方法を $N = 9$ に適用して m の候補を得て、つぎに、候補の m の中から $\varphi(m) < 10$ をみたすものをすべて挙げればよい。）

(2) 自然数 N が（任意に）与えられたとして、$\varphi(m) \leq N$ をみたす自然数 m が有限個しかないことを示せばよい。そのために、自然数 m が $\varphi(m) \leq N$ をみたすと仮定し、m が (1.15) のように、

$$m = \prod_{j=1}^{t} p_j^{e_j} \tag{$*$}$$

と素因数分解されたとする。このとき、命題 1.24 により

$$\varphi(m) = \prod_{j=1}^{t} p_j^{e_j - 1}(p_j - 1)$$

であるので、任意の j $(1 \leq j \leq t)$ について

$$p_j - 1 \leq \varphi(m), \quad p_j^{e_j - 1} \leq \varphi(m)$$

が成り立つ。よって、$\varphi(m) \leq N$ により $p_j - 1 \leq N$（つまり、$p_j \leq N + 1$）が成り立つので、素数 p_j の可能性は有限個である（$N + 1$ 以下の素数は有限個しかない）。また、同様に $p_j^{e_j - 1} \leq N$ が成り立つが、$p_j \geq 2$ であるから、$2^{e_j - 1} \leq N$ である。これは、おのおのの j について、e_j の可能性が有限個しかないことを示している。以上のことから、$(*)$ の右辺の表示の可能性が有限個しかないことがわかったので、$\varphi(m) \leq N$ をみたす m は有限個である。N は任意の自然数であったから、これで $\lim_{m \to \infty} \varphi(m) = \infty$ が証明された。

(3) 考察の一例として、$\{a_m\}$ の上極限が 1 であることがわかる。また、本書では扱っていない定理を使えば、$\{a_m\}$ の下極限が 0 であることもわかる。

以下、$\{a_m\}$ の上極限を u とし $\{a_m\}$ の下極限を l として、$u = 1$ であることを証明し、$l = 0$ であることを説明する。

m を上の $(*)$ のように素因数分解しておくと、(1.33) から

$$a_m = \frac{\varphi(m)}{m} = \prod_{j=1}^{t} \left(1 - \frac{1}{p_j}\right)$$

が得られる。よって、すべての m について $a_m \leq 1$ である。これから、$u \leq 1$ が得られる。以下、n 番目の素数を p_n と表すことにする（$n \geq 1$）。まず、n を（任意に）1 つ固定する。自然数 k に対して $m = p_n^k$ の

場合を考えれば、上の公式により、$a_{p_n^k} = 1 - \frac{1}{p_n}$ である。よって、k が無限個の値を取りえることから、$u \geq 1 - \frac{1}{p_n}$ が成り立つ。ここで、n を動かせば、$p_n \to \infty$ $(n \to \infty)$ であることから、$u \geq 1$ が得られる。$u \leq 1$ と $u \geq 1$ の両方が成り立つので、$u = 1$ である。

つぎに、自然数 n をとって、$m = p_1 p_2 \cdots p_n$ を考えると、上の公式から、

$$a_{p_1 p_2 \cdots p_n} = \prod_{j=1}^{n} \left(1 - \frac{1}{p_j}\right)$$

である。ここで、解析的整数論の成果として、

$$\lim_{n \to \infty} \left(\prod_{j=1}^{n} \left(1 - \frac{1}{p_j}\right) \right) = 0$$

という等式（注：この式は $\sum_{n=1}^{\infty} \frac{1}{p_n} = \infty$ と同値）が得られていることを使えば、$l = 0$ が導かれる。

問題 1.11　求める個数は 2^u である。ただし、$p_1, p_2, \cdots, p_t$ の中に 2 が含まれるときは $u = t - 1$ とおき、そうでないとき（つまり、$p_1, p_2, \cdots, p_t$ がすべて奇素数であるとき）には、$u = t$ とおく。

問題 1.12　(1) ウィルソンの定理（＝命題 1.28）により $(p-1)! \equiv -1 \pmod{p}$ である。$(p-1)!$ を「1 から $\frac{p-1}{2}$ までの積」（前半）と「$\frac{p+1}{2}$ から $p-1$ までの積」（後半）に分けると、前半の積は a に等しい。また、p を法とする合同式

$$\frac{p+1}{2} \equiv -\frac{p-1}{2}, \quad \frac{p+3}{2} \equiv -\frac{p-3}{2}, \quad \cdots, \quad p-1 \equiv -1$$

の両辺をそれぞれ掛け合わせれば、後半の積が p を法として $(-1)^{n-1}a$ に合同であることがわかる（$n - 1 = \frac{p-1}{2}$ に注意）。したがって、ウィルソンの定理は $a \times (-1)^{n-1}a \equiv -1 \pmod{p}$ と書き表せる。この合同式の両辺に $(-1)^{n-1}$ を掛ければ、$a^2 \equiv (-1)^n \pmod{p}$ が得られる。

(2) $p \equiv 1 \pmod{4}$ のときは、上の n は奇数なので $(-1)^n = -1$ である。よって (1) の結果は $a^2 \equiv -1 \pmod{p}$ となる。a は整数であるから、ルジャンドル記号の定義（定義 1.38 参照）により $\left(\frac{-1}{p}\right) = 1$ である。

問題 1.13　**（訂正）**問題文の最初に「2 以上の」を付け足してください。つまり、問題文は「2 以上の自然数 n に対して、つぎの 4 つの条件は同値であることを証明せよ。」となります。

（訂正の理由）：$n = 1$ のとき条件 (3)(4) は成り立ってしまいますが、1 は素数ではありません（定義 1.10 参照）。

（解答）(2)(3)(4) のそれぞれが (1) と同値であることを示す。

(1) $\Longrightarrow$ (2)：n は素数だとする。$n \geq 2$ なので、最大公約数の定義により、$\gcd(n, a) = 1 \Longrightarrow n \nmid a$ が成り立つ。また、命題 1.11(1) から $n \nmid a \Longrightarrow \gcd(n, a) = 1$ が導かれる。

(2) $\Longrightarrow$ (1)：対偶を証明するために、(1) が正しくないと仮定する。つまり、n が合成数だと仮定する。すると、n の約数 d で $1 < d < n$ をみたすものが存在する。このとき、$n \nmid d$ だが $\gcd(n, d) = d \neq 1$ であるので、$a = d$ に対して条件 $n \nmid a \Longrightarrow \gcd(n, a) = 1$ が成立していない（つまり、条件 (2) が成立していない）。これで、(2) $\Longrightarrow$ (1)（の対偶）が証明された。

(1) $\Longrightarrow$ (3)：これはウィルソンの定理（＝命題 1.28）の主張である。

(3) $\Longrightarrow$ (1)：対偶を証明するために n が合成数だと仮定する。$n \geq 2$ であるから n を割り切る素数が（少なくとも 1 つ）存在するので、その 1 つを p とする。n は素数でないと仮定していたので、$p \neq n$ であ

り、したがって、$2 \le p \le n-1$ である。よって、p は $(n-1)!$ を割り切る。合同式 $(n-1)! \equiv -1 \pmod{n}$ が成り立つなら、ある整数 k について $(n-1)!+1 = nk$ が成り立つことになるが、p は $(n-1)!$ と n の約数だが 1 の約数ではないので、それは不可能である。つまり、(3) の合同式は成り立たない。これで、(3) $\Longrightarrow$ (1)（の対偶）が証明された。

(1) $\Longrightarrow$ (4)：これは命題 1.12 の主張である。

(4) $\Longrightarrow$ (1)：背理法で証明するために、(4) が成り立つのに n が合成数であると仮定する。$n \ge 2$ であるから n を割り切る素数が（少なくとも 1 つ）存在するので、その 1 つを p とする。n は素数でないと仮定していたので、$p \ne n$ であり、したがって、$2 \le p \le n-1$ である。すると、$k = p$ に対して (4) の合同式が成り立つので、$\binom{n}{p}$ は n で割り切れる。つまり

$$\frac{1}{n}\binom{n}{p} = \frac{1}{n} \times \frac{n(n-1)(n-2)\cdots(n-p+1)}{p!} = \frac{(n-1)(n-2)\cdots(n-p+1)}{p!} \qquad (*)$$

は整数である。しかし、n が p の倍数であるから、$(*)$ の最後の式の分子に現れる $n-1, n-2, \cdots, n-p+1$ はどれも p の倍数ではない。一方、分母の $p!$ は p の倍数であるので、$(*)$ の分子が分母で割り切れることはあり得ない。$(*)$ は整数のはずだったから、これは矛盾である。したがって、n は素数でなくてはならない。

問題 1.14　(1) 不等式 $p_n \le N!+1$ をみたす最大の自然数を n とする。すると、$N!+2, N!+3, \cdots, N!+N$ は合成数である（$N!+k$ $(2 \le k \le N)$ は k で割り切れる）から、p_n のつぎの素数 p_{n+1} は $p_{n+1} \ge N!+N+1$ をみたす。したがって、

$$p_{n+1} - p_n \ge (N!+N+1) - (N!+1) = N$$

が成り立つ。

(2) 数学的帰納法により証明する。まず $n = 1$ のときは $p_1 = 2, 2^{2^{n-1}} = 2$ なので、不等式が（等式として）成立している。つぎに、 $k = 1, 2, \cdots, n$ について $p_k \le 2^{2^{k-1}}$ が成り立つと仮定する。このとき、$N = p_1 p_2 \cdots p_n + 1$ とおけば、上の仮定により、

$$N \le 2 \times 2^2 \times 2^{2^2} \times \cdots \times 2^{2^{n-1}} + 1 = 2^{2^n - 1} + 1 \le 2^{2^n}$$

が成り立つ（$1 + 2 + 2^2 + \cdots + 2^{n-1} = \dfrac{2^n - 1}{2-1} = 2^n - 1$ に注意）。一方、$N > 1$ であるから、N を割り切る素数 p がある。$p = p_m$ とする（p_m は m 番目の素数）。すると、素数 $p_1, p_2, \cdots p_n$ はどれも N を割り切らないから、$m \ge n+1$ であるので、$p_m \ge p_{n+1}$ である。また、p_m が N の約数であることから、$p_m \le N$ が成り立つ。これで

$$p_{n+1} \le p_m \le N \le 2^{2^n}$$

が得られるので、$n+1$ についても問題の不等式が成立する。

これで、数学的帰納法によって、すべての n について $p_n \le 2^{2^{n-1}}$ が成り立つことが示された。

問題 1.15　（解答 1）$m > n$ であるとして証明をおこなう。（$m < n$ のときは、m と n の役割を入れ替えて同じ議論をおこなえばよい。）F_m の定義から

$$F_m - 2 = 2^{2^m} - 1 = \left(2^{2^{m-1}}\right)^2 - 1 = \left(2^{2^{m-1}} + 1\right)\left(2^{2^{m-1}} - 1\right) = F_{m-1}(F_{m-1} - 2)$$

が成り立つ。ここで、$F_{m-1} - 2$ に対して同じ議論をおこなえば

$$F_m - 2 = F_{m-1}(F_{m-1} - 2) = F_{m-1}F_{m-2}(F_{m-2} - 2)$$

が得られる。同じことを繰り返して、最後の段階で $F_0 = 3$（したがって、$F_0 - 2 = 1$）であることを使えば、

$$F_m - 2 = F_{m-1}F_{m-2}\cdots F_1 F_0$$

が得られる。$m > n$ としていたから、この等式の右辺の項には F_n が現れている。したがって、$\gcd(F_m, F_n)$ は等式の右辺と F_m の両方を割り切るので、2 を割り切らなくてはならない。よって $\gcd(F_m, F_n)$ は 1 か 2 に等しい。しかし、F_m（と、F_n）は奇数だから、$\gcd(F_m, F_n)$ は 2 ではあり得ないので、$\gcd(F_m, F_n) = 1$ である。

（コメント） 上の解答例は整数の素朴な計算だけを利用している。しかし、整数の合同式と「合同類の位数」を知っていれば、別の証明（＝下の解答 2）を与えることができる。定義 1.30 で、p を素数として「p を法とする位数」を導入したが、「位数」は法が素数でない場合も定義できる（例 3.5 の群 $(\mathbf{Z}/m\mathbf{Z})^\times$ の元に対して、定義 3.9 を適用すればよい）。また、法が素数でない場合でも、位数は命題 1.31 と類似の性質をもつことが確かめられる。

（解答 2）$g = \gcd(F_m, F_n)$ とおき、$g \neq 1$ であると仮定する。F_m, F_n は奇数なので g も奇数であるから、$g \neq 1$ より、$g \geq 3$ である（よって、特に $-1 \not\equiv 1 \pmod{g}$ であることに注意）。また、g が奇数であるから、2 は $(\mathbf{Z}/g\mathbf{Z})^\times$ の元である（例 2.22 参照）。そこで、2 の g を法とする位数（＝群 $(\mathbf{Z}/g\mathbf{Z})^\times$ での 2 の位数）を d とする。さて、g が F_m の約数であることから、$2^{2^m} \equiv -1 \pmod{g}$ である（よって、特に $2^{2^m} \not\equiv 1 \pmod{g}$ が導かれる）。これより、$2^{2^{m+1}} \equiv (-1)^2 \equiv 1 \pmod{g}$ が得られる。以上により、$2^{2^{m+1}} \equiv 1 \pmod{g}$ かつ $2^{2^m} \not\equiv 1 \pmod{g}$ であるから、$d = 2^{2^{m+1}}$ が成り立つ。（理由：$2^{2^{m+1}} \equiv 1 \pmod{g}$ より d は $2^{2^{m+1}}$ の約数である（命題 1.31(1) の証明と同様の議論による）。よって、$d \neq 2^{2^{m+1}}$ だとすれば d は 2^{2^m} の約数だが、$2^{2^m} \not\equiv 1 \pmod{g}$ だから、それは不可能である。）一方、g は F_n の約数でもあるので、上と同じ議論で $d = 2^{2^{n+1}}$ が導かれる。すると、$2^{2^{m+1}} = d = 2^{2^{n+1}}$ であるから $m = n$ である。以上で、$g \neq 1$ ならば $m = n$ であることが証明されたので、対偶をとって、$m \neq n$ なら $\gcd(F_m, F_n) = 1$ であることが示された。

問題 1.16　（訂正；最新の版では訂正済み）問題の最初の文を「$f(T)$ は定数でない整数係数多項式で最高次の係数が正だとする。」で置き換えてください。

（訂正の理由）：$f(T)$ の最高次の係数が負だと、n が十分大きいときに $f(n)$ が負の整数になってしまうため。

（解答）「最高次の係数が正」という仮定により $\lim_{n\to\infty} f(n) = +\infty$ が成り立つ。したがって、$f(n_0) \geq 2$ となる自然数 n_0 が存在する。このような n_0 を 1 つ取り、$m_0 = f(n_0)$ とおけば、因数定理（下のコメント参照）により

$$f(x) - m_0 = (x - n_0)g(x)$$

をみたす最高次の係数が正の整数係数多項式 $g(x)$ が存在する。t を自然数として、この等式に $x = m_0 t + n_0$ を代入すれば

$$f(m_0 t + n_0) = m_0 + m_0 t g(m_0 t + n_0) = m_0(1 + t g(m_0 t + n_0))$$

が得られる。$m_0 \geq 2$ であるから $1 + t g(m_0 t + n_0) \geq 2$ であれば $f(m_0 t + n_0)$ が合成数である。実際、$g(x)$ の最高次の係数が正であることから、t を動かせば $1 + t g(m_0 t + n_0)$ はいくらでも大きな値を取り得る。これで、$f(m_0 t + n_0)$ が合成数となる t が無限個存在することが示された。

（コメント）「因数定理」とは、多項式 $f(x)$ に関する「$f(\alpha) = 0$ が成り立つことと $f(x)$ が $x - \alpha$ で割り切れることは同値である」という主張のことです。本書でも、例 2.57 などで”暗黙のうちに”因数定理が利用されています。本来は因数定理の主張を明確に述べておくべきだった、と反省しています。因数定理の正式な定式化と証明は、代数学の教科書を参照してください（たとえば、中島匠一「代数方程式とガロア理論」（共立出版）命題 1.1）。

「代数と数論の基礎」(中島匠一)　第 2 章の章末問題の解答例

問題 2.1　X は

$$-E_2,\ 3E_2,\ \begin{pmatrix} -1+\sqrt{4-bc} & b \\ c & -1-\sqrt{4-bc} \end{pmatrix},\ \begin{pmatrix} -1-\sqrt{4-bc} & b \\ c & -1+\sqrt{4-bc} \end{pmatrix}$$

のどれかである。ただし、b, c は $bc \leq 4$ をみたす任意の実数を表す。

(コメント) $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ とおいて、X のみたすべき条件を a, b, c, d の条件で表せば、解答が得られる。他の解法としては、行列 X の対角化を利用する方法が考えられる。ただし、この問題の場合は、あまりわかりやすい形の表示にならない。(主観の問題かもしれないが。)

問題 2.2　(1) 有理数に関する等式

$$\frac{m}{2^l} + \frac{n}{2^k} = \frac{m2^k + n2^l}{2^{l+k}}, \quad \frac{m}{2^l} \times \frac{n}{2^k} = \frac{mn}{2^{l+k}}$$

を使えば、定義 2.8 の条件がすべて成り立つことが確かめられる (詳細は省略)。

(2) 素数からなる集合 S に対して、

$$R(S) = \{r \in \mathbf{Q} \mid r \text{ を既約分数で表したとき、分母を割り切る素数はすべて } S \text{ に属する}\}$$

とおく。$R(S)$ は $\mathbf{Q}$ の部分環であり、逆に、R が $\mathbf{Q}$ の部分環なら、素数全体からなる集合の部分集合 S があって $R = R(S)$ が成り立つ。

注： (2) の記号では、(1) の環は $R(\{2\})$ と表される。また、$\mathbf{Q}$ 自身は $R(P)$ に等しい。ただし、P は素数全体のなす集合である。

問題 2.3　(1) $X, X' \in R$ について、

$$(X + X')A = XA + X'A = AX + AX' = A(X + X')$$

および

$$(XX')A = X(X'A) = X(AX') = (XA)X' = (AX)X' = A(XX')$$

が成り立つ。このことから、定義 2.8 の条件がすべて成立することが確かめられる。

(2) $X = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in M_2(\mathbf{R})$ とするとき、条件 $AX = XA$ は「$b\alpha = b\delta$ かつ $c\alpha = c\delta$ かつ $b\gamma = c\beta$」と同値である。仮定より $bc \neq 0$ なので、この条件は $\alpha = \delta, b\gamma = c\beta$ と同値になる。これは X が実数 u, v によって $\begin{pmatrix} u & bv \\ cv & u \end{pmatrix}$ と表されることと同じである ($u = \alpha = \delta, v = \dfrac{\beta}{b} = \dfrac{\gamma}{c}$)。したがって、

$$R = \left\{ \begin{pmatrix} u & bv \\ cv & u \end{pmatrix} \,\middle|\, u, v \in \mathbf{R} \right\}$$

となる。この R が可換環であることは、行列の計算によって容易に確かめられる。

(3) 答えは $bc < 0$ である。

理由の概略はつぎの通り。(2) と同じ考察により、$bc = 0$ のときは R が可換環でないことがわかる。したがって、R が整域であるためには、$bc \neq 0$ が成り立つことが必要である。$bc \neq 0$ のとき、(2) での考察に

より、R の元は uE_2+vB $(u,v\in\mathbf{R})$ と表される。ただし、E_2 は 2 次の単位行列で、$B=\begin{pmatrix}0&b\\c&0\end{pmatrix}$ である。行列の簡単な計算により $B^2=bcE_2$ となることがわかるので、$u,u',v,v'\in\mathbf{R}$ に対して

$$(uE_2+vB)(u'E_2+v'B)=(uu'+bcvv')E_2+(uv'+vu')B \qquad (*)$$

が成り立つ。ここで、$bc>0$ ならば $u=u'=\sqrt{bc}, v=1, v'=-1$ のときに $(*)$ の右辺が 0 になる。したがって、$bc>0$ なら R は 0 以外の零因子をもつので、R は整域ではない。

つぎに、$bc<0$ であるとする。このとき $(*)$ の右辺が 0 等しいなら,$uu'+bcvv'=uv'+vu'=0$ が成り立つ。すると

$$(u^2-bcv^2)(u'^2-bcv'^2)=(uu'+bcvv')^2-bc(uv'+vu')^2=0$$

となるので、$u^2-bcv^2=0$ または $u'^2-bcv'^2=0$ である。$bc<0$ なので、$u^2-bcv^2=0$ ならば $u=v=0$ で $uE_2+vB=0$ となり、$u'^2-bcv'^2=0$ ならば $u'=v'=0$ で $u'E_2+v'B=0$ となる。これで R の零因子が 0 だけであることが示せたので、R は整域である（定義 2.16 参照)。

問題 2.4　x はベキ零元であるから、$x^n=0$ をみたす自然数 n がとれる。このとき、$y=1_R+x+x^2+\cdots+x^{n-1}$ とおく（y は R の元である)。すると、

$$(1_R-x)y=(1_R-x)(1_R+x+x^2+\cdots+x^{n-1})=1_R-x^n=1_R$$

が成り立つ。また、同様にして $y(1_R-x)=1_R$ も確かめられる。これは y が 1_R-x の逆元であることを示している（定義 2.10(1) 参照）ので、1_R-x は可逆元である。

問題 2.5　(1) $f\in R$ が可逆元であるための条件は「すべての $x\in I$ について $f(x)\neq 0$ が成り立つ」ことである。

(2) $f\in R$ がベキ零元だとすると、ある自然数 n があって、$f^n=0$ が成り立つ。これは、すべての $x\in I$ について $f(x)^n=0$ が成り立つことである。すると、$f(x)$ は実数なので、すべての $x\in I$ について $f(x)=0$ でなくてはならない。つまり、$f=0$ でなくてはならない。以上で、R のベキ零元は 0 だけであることがわかった。

(3) $f(c)=0$ であるから、(1) により、f は R の可逆元ではない。

つぎに、$g\in R$ が $fg=0$ をみたすとする。つまり、すべての $x\in I$ について $f(x)g(x)=0$ が成り立つ。すると、$x\neq c \implies f(x)\neq 0$ であるから、$x\neq c$ をみたすすべての $x\in I$ について $g(x)=0$ でなくてはならない。しかし、g は（R の定義により）連続関数であるから、$g(c)=0$ も成り立つことになる。（理由：すべての n について $x_n\neq c$ で $\lim_{n\to\infty}x_n=c$ をみたす（I の中の）数列 $\{x_n\}$ をとれば、$g(x_n)=0$ なので、$g(c)=\lim_{n\to\infty}g(x_n)=0$ となる。）よって、$g=0$ でなくてはならない。これで $fg=0$ から $g=0$ が導かれたので、f は零因子ではない。

問題 2.6　$A\in M_n(\mathbf{Z})^\times$ とすれば、$AB=E_n$ をみたす $B\in M_n(\mathbf{Z})$ が存在する（定義 2.10 参照；E_n は n 次単位行列)。すると、行列式の性質より

$$\det(A)\det(B)=\det(AB)=\det(E_n)=1$$

となる。一方、A,B の成分は整数であるから、$\det(A)$ と $\det(B)$ も整数である。整数 $\det(A)$ に整数 $\det(B)$ を掛けて 1 になるのであるから、$\det(A)=\pm1$ でなくてはならない。

逆に $\det(A)=\pm1$ であれば、余因子行列式による逆行列の表示式（線型代数の教科書参照）により、A の逆行列が整数係数であることがわかり、$A\in M_n(\mathbf{Z})^\times$ が示せる。

問題 2.7　四元数環の演算の定義に従って計算すれば、すべて確かめられる（詳細は省略）。ただし、(3)(a) については、a, b, c, d が実数であることから、$a^2+b^2+c^2+d^2=0 \iff a=b=c=d=0$ が成り立つことに注意。

問題 2.8　(1) $w=bi+cj+dk$ $(b,c,d \in \mathbf{R}, b^2+c^2+d^2=1)$ と表されるすべての w。

(2) $\mathbf{H}$ の零因子は 0 だけであるが、$M_2(\mathbf{R})$ は 0 でない零因子をもつので、両者は（環として）同型ではない。

(3) $a+bi+cj+dk$ を $\begin{pmatrix} a+bi & c+di \\ -c-di & a+bi \end{pmatrix}$ に写すことで得られる写像は $\mathbf{H}$ から $M_2(\mathbf{C})$ への環準同型である。（この写像が環の準同型であることは、簡単な計算で確かめられる。）

問題 2.9　最初に記号を導入する。一般に、$E(i,j)$ を (i,j) 成分が 1 でその他の成分がすべて 0 である $M_n(\mathbf{R})$ の元とする（$1 \leq i,j \leq n$）。（注：$E(i,j)$ は行列単位と呼ばれることがある。）すると、$M_n(\mathbf{R})$ の任意の元は $E(i,j)$ $(1 \leq i,j \leq n)$ の（$\mathbf{R}$ 係数の）1 次結合で表される（つまり、$\{E(i,j) \mid 1 \leq i,j \leq n\}$ は $M_n(\mathbf{R})$ の $\mathbf{R}$ 上の基底である）。

さて、J は $M_n(\mathbf{R})$ の両側イデアルで $J \neq \{0\}$ だとする。すると、$J \neq \{0\}$ であるから、$A_0 \neq 0$ である $A_0 \in J$ が存在する。$A_0 \neq 0$ であるから、「A_0 の (i_0, j_0) 成分 $\neq 0$」となる i_0, j_0 が存在する（$1 \leq i_0, j_0 \leq n$）。ここで、A_0 の (i_0, j_0) 成分を a_0 とすれば、行列の積の簡単な計算で

$$E(i,j) = a_0^{-1} E(i,i_0) A_0 E(j_0,j) \qquad (*)$$

が成り立つことが確かめられる（$1 \leq i,j \leq n$）。$A_0 \in J$ で J が両側イデアルであることから、$(*)$ の右辺は J に属する。したがって、$(*)$ により、$E(i,j)$ も J に属する。すると、J が両側イデアルであることから、$E(i,j)$ $(1 \leq i,j \leq n)$ の任意の 1 次結合も J に属する。よって、$M_n(\mathbf{R})$ の任意の元が J に属するので、$J = M_n(\mathbf{R})$ が成り立つ。これで、「$\{0\}$ 以外の両側イデアルは $M_n(\mathbf{R})$ しかない」ことが示された。これは、問題の主張に他ならない。

問題 2.10　(1) 正しくない：$\mathbf{Q}$ は体であるが、$\mathbf{Q}$ の部分環 $\mathbf{Z}$ は体ではない。

(2) 正しくない：$\mathbf{Z}$ は整域であるが、$\mathbf{Z}$ の剰余環 $\mathbf{Z}/4\mathbf{Z}$ は整域ではない。

(3) 正しくない：$\mathbf{Z}$ は整域であるが、$\mathbf{Z}$ の剰余環 $\mathbf{Z}/4\mathbf{Z}$ は体ではない。

(4) 正しくない：多項式環 $\mathbf{Q}[T]$ は整域だが体ではない。しかし、$\mathbf{Q}[T]$ は体 $\mathbf{Q}$ を部分環として含んでいる。

(5) 正しくない：多項式環の剰余環 $\mathbf{Q}[T]/(T^2-1)$ は可換環であり、整域 $\mathbf{Q}$ を部分環として含んでいる。しかし、$T-1$ の定める $\mathbf{Q}[T]/(T^2-1)$ の元（これは 0 ではない）は零因子なので、$\mathbf{Q}[T]/(T^2-1)$ は整域ではない。

注意： 上に挙げた反例は一例（いちれい）に過ぎず、反例は他にもたくさんある。

問題 2.11　(1) I_S の定義から、定義 2.26 の条件が成立することが容易に確かめられる（詳細は省略）。

(2) 定義からただちに導かれる。（$S \subset S'$ ならば、「すべての $s \in S'$ について $f(s)=0$」から「すべての $s \in S$ について $f(s)=0$」が導かれるのは、明らか。）

(3) まず、$[0,1]$ の有限部分集合 S に対して、

$$S = \{x \in [0,1] \mid \text{すべての } f \in I_S \text{ について } f(x)=0\} \qquad (*)$$

であることを示す。$(*)$ の右辺の集合を T とおくと、I_S の定義により、$S \subset T$ は明らかである。つぎに、$x_0 \in [0,1]$ が $x_0 \notin S$ をみたすとする。すると、S が有限集合であるから、$d_0 = \min\{|x_0 - s| \mid s \in S\}$ が存

在し、$x_0 \notin S$ により $d_0 > 0$ である。このとき、$f : [0,1] \to \mathbf{R}$ を

$$f(x) = \begin{cases} \frac{d_0}{2} - |x - x_0| & (|x - x_0| \leq \frac{d_0}{2} \text{ のとき}), \\ 0 & (|x - x_0| \geq \frac{d_0}{2} \text{ のとき}) \end{cases}$$

と定める（$x \in [0,1]$）。f の定義により f が連続であることは容易に確かめられるので、$f \in R$ である。そして、これも定義により、$f(x_0) = \frac{d_0}{2} > 0$ であるから、$x_0 \notin T$ である。x_0 は $x_0 \notin S$ をみたす任意の元であったから、これで $T \subset S$ も示された。以上により、$(*)$ が成り立つことが証明された。

有限集合 S と S' に $(*)$ を適用して、$I_S = I_{S'} \implies S = S'$ が示される。$S = S' \implies I_S = I_{S'}$ は明らかであるから、これで証明が完成した。

(4) $S = \left\{ \frac{1}{n} \mid n \in \mathbf{N} \right\}$, $S' = S \cup \{0\}$ が求める例を与えている。

問題 2.12　$\Longleftarrow$ が成り立つことは簡単に確かめられる。（理由：「$I_1 \subset I_2 \implies I_1 \cup I_2 = I_2$」であるし、「$I_2 \subset I_1 \implies I_1 \cup I_2 = I_1$」である。）$\implies$ の対偶を示すために、「$I_1 \subset I_2$ または $I_2 \subset I_1$」ではないと仮定する。つまり、「$I_1 \not\subset I_2$ かつ $I_2 \not\subset I_1$」であると仮定する。このとき、$a_1 \notin I_2$ をみたす $a_1 \in I_1$ と $a_2 \notin I_1$ をみたす $a_2 \in I_2$ が存在する。すると、$a_1, a_2 \in I_1 \cup I_2$ なので、もし $I_1 \cup I_2$ が左イデアルなら、$a_1 + a_2 \in I_1 \cup I_2$ が成り立つ。しかし、これは矛盾である。なぜなら、$a_1 + a_2 \in I_1$ であれば $a_1 \in I_1$ であることから $a_2 = (a_1 + a_2) - a_1 \in I_1$ となるが、これは $a_2 \notin I_1$ に矛盾しており、$a_1 + a_2 \in I_2$ なら同じ議論で $a_1 = (a_1 + a_2) - a_2 \in I_2$ となり $a_1 \notin I_2$ に矛盾するからである。これで、背理法により、$I_1 \cup I_2$ は左イデアルでないことが証明された。以上で $\implies$ の対偶が示されて、証明が完成した。

問題 2.13　この解答の中では、$\overline{R} = R/\mathrm{Nil}(R)$ とし、$a \in R$ の定める $\overline{R}$ の元を $\overline{a}$ と書くことにする（$\overline{a} = a + \mathrm{Nil}(R)$）。定義により、$\overline{R}$ の任意の元は $\overline{a}$ $(a \in R)$ と表される（定義 2.36 参照）。また、R のゼロ元との区別のために、$\overline{R}$ のゼロ元を $\overline{0}$ と書き表す。この記号を使えば、問題で要求されているのは $\mathrm{Nil}(\overline{R}) = \{\overline{0}\}$ が成り立つことの証明である。

$a \in R$ が $\overline{a} \in \mathrm{Nil}(\overline{R})$ をみたすとすれば、$\overline{a}^m = \overline{0}$ となる自然数 m がある。$\overline{a}^m = \overline{a^m}$ であるので、$\overline{a^m} = \overline{0}$ が成り立つが、これは（剰余環 $\overline{R}$ の定義により）$a^m \in \mathrm{Nil}(R)$ であることを示している。よって、$\mathrm{Nil}(R)$ の定義により、$(a^m)^n = 0$ をみたす自然数 n が存在する。すると、$(a^m)^n = a^{mn}$ であるから、$a^{mn} = 0$ が成り立つことになる。これは、$a \in \mathrm{Nil}(R)$ を意味しているので、剰余環 $\overline{R}$ の定義により、$\overline{a} = \overline{0}$ が成り立つ。$\overline{a}$ は $\mathrm{Nil}(\overline{R})$ の任意の元であったから、これで $\mathrm{Nil}(\overline{R}) = \{\overline{0}\}$ が示された。

問題 2.14　J_1, J_2 がイデアルであることから、$\Longleftarrow$ が成り立つことは簡単に確かめられる（詳細は省略）。$\implies$ の対偶を示すために、「$J_1 \subset I$ または $J_2 \subset I$」ではないと仮定する。つまり、「$J_1 \not\subset I$ かつ $J_2 \not\subset I$」であると仮定する。このとき、$a_1 \notin I$ をみたす $a_1 \in J_1$ と $a_2 \notin I$ をみたす $a_2 \in J_2$ が存在する。すると、まず $a_1 \in J_1, a_2 \in J_2$ であることから $a_1 a_2 \in J_1 J_2$ が成り立つ。また、$a_1 \notin I$ かつ $a_2 \notin I$ であることと I が素イデアルであることから、$a_1 a_2 \notin I$ が成り立つ。したがって、$J_1 J_2 \subset I$ ではあり得ない（$a_1 a_2$ は $J_1 J_2 - I$ の元になっているので、$J_1 J_2 - I \neq \emptyset$ である）。以上で $\implies$ の対偶が示されて、証明が完成した。

問題 2.15　(1): 剰余環 $\mathbf{Z}[i]/(7)$ が可換環であることは直ちにわかるので、$\mathbf{Z}[i]/(7)$ の零元以外の元が可逆であることを示せば良い。以下、$a + bi \in \mathbf{Z}[i]$ の定める $\mathbf{Z}[i]/(7)$ の元を $\overline{a + bi}$ と表すことにする（このとき、$\mathbf{Z}[i]/(7)$ の零元は $\overline{0}$ で、単位元は $\overline{1}$ である）。$\overline{a + bi} \neq \overline{0}$ とすれば「$a \not\equiv 0 \pmod 7$ または $b \not\equiv 0 \pmod 7$」であるので、$a^2 + b^2 \not\equiv 0 \pmod 7$ が成り立つ（理由：$a^2 + b^2 \equiv 0 \pmod 7$ で $a \not\equiv 0 \pmod 7$ とすれば、$ax \equiv 1 \pmod 7$ となる $x \in \mathbf{Z}$ をとるとき $(bx)^2 \equiv -1 \pmod 7$ となるが、$y^2 \equiv -1 \pmod 7$ をみたす整数 y は存在しないので、これは矛盾；$b \not\equiv 0 \pmod 7$ のときも同じ議論ができるので、$\overline{a + bi} \neq \overline{0}$ のときは $a^2 + b^2 \equiv 0 \pmod 7$ は成立しない。）したがって、命題 1.27(1) により、$(a^2 + b^2)z \equiv 1 \pmod 7$

をみたす $z \in \mathbf{Z}$ がとれる。すると

$$\overline{(a+bi)}\ \overline{(za-zbi)} = \overline{(a^2+b^2)z} = \overline{1}$$

が成り立つ。これは、$\overline{za-zbi}$ が $\overline{a+bi}$ の逆元であることを意味しているので、$\overline{a+bi}$ は可逆元である。以上で、$\mathbf{Z}[i]/(7)$ の $\overline{0}$ 以外の元が可逆であることがわかったので、$\mathbf{Z}[i]/(7)$ は体である。

(2): 解答のためには

(i) $\mathbf{Z}[i]/(5)$ は直積 $(\mathbf{Z}[i]/(2+i)) \times (\mathbf{Z}[i]/(2-i))$ に（環として）同型であること

(ii) $\mathbf{Z}[i]/(2+i)$ と $\mathbf{Z}[i]/(2-i)$ はどちらも（環として）$\mathbf{Z}/5\mathbf{Z}$ に同型であること

の 2 つを示せばよい。

(i) の証明：写像 $\varphi : \mathbf{Z}[i] \to (\mathbf{Z}[i]/(2+i)) \times (\mathbf{Z}[i]/(2-i))$ を、$a+bi \in \mathbf{Z}[i]$ に対して

$$\varphi(a+bi) = (a+bi \pmod{(2+i)}, a+bi \pmod{(2-i)}) \in (\mathbf{Z}[i]/(2+i)) \times (\mathbf{Z}[i]/(2-i))$$

とおいて定める（注：$a+bi$ の定める $\mathbf{Z}[i]/(2+i)$ の元を $a+bi \pmod{(2+i)}$ と書き表す；$\mathbf{Z}[i]/(2-i)$ についても同様)。このとき、φ が環準同型であることは容易に確かめられる。また、φ が全射であることもわかる（理由：$(c+di \pmod{(2+i)}, e+fi \pmod{(2-i)}) \in (\mathbf{Z}[i]/(2+i)) \times (\mathbf{Z}[i]/(2-i))$ が与えられたとき

$$a = -2c-d-2e+f, \quad b = c-2d-e-2f$$

とおけば、簡単な計算で

$$a+bi \equiv c+di \pmod{(2+i)}, \quad a+bi \equiv e+fi \pmod{(2-i)}$$

が成り立つことが確かめられる)。さらに、$2+i$ と $2-i$ が互いに素であることと $(2+i)(2-i)=5$ であることから、φ の核はイデアル (5) であることがわかる。(理由：$(2+i)(2-i)=5$ よりイデアル (5) が φ の核に含まれるのは明らかである。逆に $\varphi(a+bi)=0$ とすれば、$a+bi$ は $2+i$ と $2-i$ の両方で割り切れるので、等式 $-(2+i)+(2-i)(1+i)=1$ の両辺に $a+bi$ を掛ければ、$a+bi$ が $5=(2+i)(2-i)$ で割り切れることが示せる。）以上のことと環の準同型定理（＝定理 2.50）により、(i) が証明される。

（コメント）a, b の定め方が「不審」に思われるかもしれない。実際は、

$$-2+i \equiv 1 \pmod{(2+i)}, \quad -2+i \equiv 0 \pmod{(2-i)},$$
$$-2-i \equiv 0 \pmod{(2+i)}, \quad -2-i \equiv 1 \pmod{(2-i)}$$

であることを利用して、

$$a+bi = (-2+i)(c+di) + (-2-i)(e+fi)$$

と定めている。これは、整数環 $\mathbf{Z}$ の場合の中国剰余定理の証明の手法（定理 1.26 参照）をガウス整数環 $\mathbf{Z}[i]$ に適用している、ということである。

(ii) の証明:$\mathbf{Z}[i]/(2+i)$ が（環として）$\mathbf{Z}/5\mathbf{Z}$ に同型であることを示す。そのために、写像 $\psi : \mathbf{Z} \to \mathbf{Z}[i]/(2+i)$ を

$$\psi(a) = a \pmod{(2+i)} \quad (a \in \mathbf{Z})$$

によって定める。この ψ が環準同型であることは容易に確かめられる。また、$c+di \in \mathbf{Z}[i]$ に対して $a = c-2d \in \mathbf{Z}$ とおけば、$a \equiv c+di \pmod{(2+i)}$ が成り立つ（理由：$c-2d-(c+di) = -d(2+i) \in (2+i)$ である）ので、ψ は全射である。また、ψ の核は $\mathbf{Z}$ のイデアル $5\mathbf{Z}$ に等しい。（理由；$5=(2+i)(2-i)$ より、$5\mathbf{Z}$ は ψ の核に含まれる。逆に $a \in \mathbf{Z}$ が ψ の核に含まれるとすれば a は $2+i$ で割り切れるが、a は整数（特に、実数）であるから、a は $2-i$ でも割り切れる。よって、a は $(2+i)(2-i)=5$ で割り切れる。）

以上のことと環の準同型定理（＝定理 2.50）により、$\mathbf{Z}/5\mathbf{Z}$ と $\mathbf{Z}[i]/(2+i)$ が（環として）同型であることが証明される。

同様にして $\mathbf{Z}/5\mathbf{Z}$ と $\mathbf{Z}[i]/(2-i)$ が（環として）同型であることも証明されるので、(ii) が成り立つ。

(3): （略解）2 つの環 $\mathbf{Z}[i]/(p)$ と $\mathbf{F}_p[T]/(T^2+1)$ は両方とも剰余環 $\mathbf{Z}[T]/(p, T^2+1)$ に環同型であることが示される（注：(p, T^2+1) は、2 つの元 p と T^2+1 で生成される $\mathbf{Z}[T]$ のイデアルを表している；式 (2.18) 参照）。したがって、$\mathbf{Z}[i]/(p)$ と $\mathbf{F}_p[T]/(T^2+1)$ は同型である。$\mathbf{Z}[T]/(p, T^2+1)$ と $\mathbf{Z}[i]/(p)$ の間の環同型は T を i に写す写像 $\mathbf{Z}[T] \to \mathbf{Z}[i]$ を通じて定義され、$\mathbf{Z}[T]/(p, T^2+1)$ と $\mathbf{F}_p[T]/(T^2+1)$ の間の環同型は多項式の係数を法 p で還元することで定まる写像 $\mathbf{Z}[T] \to \mathbf{F}_p[T]$ を通じて定義される。

問題 2.16　(1): イデアル $I_1^2, I_2^2, I_3^2, I_4^2, I_1I_4, I_2I_3$ はそれぞれ $2-\sqrt{5}i, 2+\sqrt{5}i, 2-3\sqrt{5}i, 2+3\sqrt{5}i, 1-2\sqrt{5}i, 1+2\sqrt{5}i$ で生成される単項イデアルである。ここでは、I_1^2 についてだけ証明を与える。他の場合も、同様の計算で証明できる。

まず、イデアルの積の定義により

$$I_1^2 = (3^2, 3(4+\sqrt{5}i), (4+\sqrt{5}i)^2) = (9, 12+3\sqrt{5}i, 11+8\sqrt{5}i)$$

であることがわかる。ここで、

$$9 = (2-\sqrt{5}i)(2+\sqrt{5}i), \quad 12+3\sqrt{5}i = (2-\sqrt{5}i)(1+2\sqrt{5}i), \quad 11+8\sqrt{5}i = (2-\sqrt{5}i)(-2+3\sqrt{5}i)$$

であることから、

$$I_1^2 = (2-\sqrt{5}i)(2+\sqrt{5}i, 1+2\sqrt{5}i, -2+3\sqrt{5}i)$$

が成り立つ。さらに、

$$11(2+\sqrt{5}i)(2-\sqrt{5}i) + 2(-2+3\sqrt{5}i)(2+3\sqrt{5}i) = 1 \qquad (*)$$

であることから、イデアル $(2+\sqrt{5}i, 1+2\sqrt{5}i, -2+3\sqrt{5}i)$ は 1 を含むので、$(2+\sqrt{5}i, 1+2\sqrt{5}i, -2+3\sqrt{5}i) = (1)$ である（命題 2.27(4)）。以上で、$I_1^2 = (2-\sqrt{5}i)$ が示された。

（コメント 1）上の計算で、等式 $(*)$ の導き方が「不審」かもしれないので、コメントしておこう。イデアル $(2+\sqrt{5}i, 1+2\sqrt{5}i, -2+3\sqrt{5}i)$ の元 $2+\sqrt{5}i$ と $-2+3\sqrt{5}i$ について、それぞれ自分自身の複素共役と掛け合わせると、$(2+\sqrt{5}i)(2-\sqrt{5}i) = 9$, $(-2+3\sqrt{5}i)(-2-3\sqrt{5}i) = 49$ となる。ここで、9 と 49 は互いに素であることに着目して $1 = 11 \times 9 - 2 \times 49$ を導き（定理 1.7 参照）、9 と 49 に上の等式を代入すれば $(*)$ が得られる。

（コメント 2）代数的整数論（または、特に 2 次体の整数論）の結果により、$\mathbf{Z}[\sqrt{5}i]$ のイデアルについては、「イデアルの商」をとれることが知られている。それを使えば、$I_1^2 = (2-\sqrt{5}i)$ と、$I_1I_2 = (3), I_1I_3 = (4+\sqrt{5}i)$（命題 2.82 参照）から、$I_2I_3 = (1+2\sqrt{5}i)$ であることが簡単に導ける。具体的計算は

$$I_2I_3 = \frac{(I_1I_2)(I_1I_3)}{I_1^2} = \frac{(3)(4+\sqrt{5}i)}{(2-\sqrt{5}i)} = \frac{(3)(4+\sqrt{5}i)(2+\sqrt{5}i)}{(9)} = \frac{(3+6\sqrt{5}i)}{(3)} = (1+2\sqrt{5}i)$$

となる。

(2): 答えは、$p=3$、$p=7$、それ以外（つまり、$p \neq 3, 7$）の場合に、それぞれ、$\mathbf{Z}/3\mathbf{Z}$、$\mathbf{Z}/7\mathbf{Z}$、$\{0\}$ となる（注：$\{0\}$ は零環を表す：例 2.9 参照）。

問題で扱っているイデアルを $J = (p, 4+\sqrt{5}i)$ とおく。イデアル J は、$p=3$ の場合は 2.7 節の I_1 であり、$p=7$ の場合は I_3 である。したがって、$p=3, 7$ のときは、命題 2.80 によって、問題は解決されている。あとは、$p \neq 3, 7$ と仮定して、$J = (1)$ であることを示せばよい。$p \neq 3, 7$ であるから、p は 21 と互いに素なので、$px + 21y = 1$ をみたす整数 x, y が存在する（定理 1.7 参照）。よって、

$$px + (4-\sqrt{5}i)(4+\sqrt{5}i)y = 1$$

が成り立つ（$(4-\sqrt{5}i)(4+\sqrt{5}i)=21$ に注意）。J の定義により、この等式の左辺は J に属するから、$1\in J$ である。よって、$J=(1)$ でなくてはならない（命題 2.27(4)）。したがって、$\mathbf{Z}[\sqrt{5}i]/J=\{0\}$ である（例 2.40）。

「代数と数論の基礎」(中島匠一)　第 3 章の章末問題の解答例

問題 3.1　定義 3.1 の条件 (G1)(G2)(G3) と定義 3.4 の条件 (CG2) が成り立つことを確かめればよい。以下、X, Y, Z は G の元を表すとする。

(G1) $(X * Y) * Z$ と $X * (Y * Z)$ は両方とも $(X - (Y \cup Z)) \cup (Y - (Z \cup X)) \cup (Z - (X \cup Y))$ に等しいので、$(X * Y) * Z = X * (Y * Z)$ である。

(G2) 問 A.1(6) により、$\emptyset \in G$（空集合）が $*$ の単位元である。

(G3) $X \cup X = X \cap X = X$, $X - X = \emptyset$ であるから、$X * X = \emptyset$ が成り立つ。つまり、X 自身が X の逆元であるので、逆元はかならず存在する。

(CG2) 問 A.1(1) により、$X * Y = Y * X$ が成り立つ。

（コメント）この問題での $X * Y$ は「X と Y の対称差」と呼ばれている。(中島匠一「集合・写像・論理」(共立出版) p.71 参照。)

問題 3.2　(1) 群ではない。(理由：単位元が存在しない。)

(2) 群ではない。(理由：単位元が存在しない。)

(3) 定義 3.1 の条件が成り立つことが確かめられる（詳細は省略）ので、群である。(注：単位元は 1 で、a の逆元は $(-1)^{a+1}\left[\frac{a}{2}\right]$ である。)

(4) 群ではない。(理由：単位元が存在しない。)

（コメント）(3) の写像 $f : \mathbf{N} \to \mathbf{Z}$ は $\mathbf{N}$ と $\mathbf{Z}$ の間の全単射を与えている。(3) の演算 $*$ は、$\mathbf{Z}$ の加法演算を f で $\mathbf{N}$ に引き戻したものである。

問題 3.3　(1) θ が π の整数倍のときは $\mathrm{Cent}_G(\sigma) = GL_2(\mathbf{R})$ で、それ以外のときは

$$\mathrm{Cent}_G(\sigma) = \left\{ \begin{pmatrix} r\cos t & -r\sin t \\ r\sin t & r\cos t \end{pmatrix} \mid r, t \in \mathbf{R},\ r > 0,\ 0 \le t < 2\pi \right\}$$

である。

(2) $a = b$ のときは $\mathrm{Cent}_G(\sigma) = GL_2(\mathbf{R})$ で、$a \neq b$ のときは

$$\mathrm{Cent}_G(\sigma) = \left\{ \begin{pmatrix} u & 0 \\ 0 & v \end{pmatrix} \mid u, v \in \mathbf{R}^\times \right\}$$

である。

問題 3.4　(1) $\epsilon \in \mathrm{Cent}(S_n)$ であるので、$\sigma \in S_n,\ \sigma \neq \epsilon$ ならば $\sigma \notin \mathrm{Cent}(S_n)$ であることを示せばよい。$\sigma \neq \epsilon$ であるから、$\sigma(i) \neq i$ となる i が（少なくとも 1 つ）存在する（$1 \le i \le n$)。そのような i を 1 つとり、i の $\sigma(i)$ どちらとも等しくない数 k をとる（$1 \le k \le n$；$n \ge 3$ という仮定により、これは可能)。ここで $\tau = (i\,k) \in S_n$（互換）とおけば、$\sigma\tau$ は i を $\sigma(k)$ に移し $\tau\sigma$ は i を $\sigma(i)$ に移す。$i \neq k$ より $\sigma(i) \neq \sigma(k)$ であるから、$\sigma\tau \neq \tau\sigma$ である。これで σ は $\mathrm{Cent}(S_n)$ の元でないことがわかったので、証明が終わる。

(2) $GL_n(\mathbf{R})$ の中心に属するのはスカラー行列だけである。つまり、

$$\mathrm{Cent}(GL_n(\mathbf{R})) = \{aE_n \mid a \in \mathbf{R}^\times\}$$

が成り立つ（E_n は n 次単位行列を表す)。

問題 3.5　部分群の個数は $p+3$ である。(位数 1 の部分群が 1 つ（単位群)、位数 p^2 の部分群が 1 つ（G 自身)、位数 p の部分群が $p+1$ 個ある。)

問題 3.6　(2) $\Longrightarrow$ (1) が成り立つことは簡単にわかる（命題 3.12 参照）。

(1) $\Longrightarrow$ (2) を示すために、G の部分群は自明なものだけだと仮定する。このとき、G が単位群なら (2) が成り立つ。G が単位群でないときは、単位元でない $\sigma \in G$ を 1 つとり、σ の生成する G の部分群を H とする（$H = \langle \sigma \rangle \subset G$）。$\sigma \neq \epsilon$ より H は単位群ではないので、仮定により、$H = G$ でなくてはならない。つまり、G は σ の生成する巡回群である。また、G の位数（$= \sigma$ の位数）が合成数であれば、G は自明でない部分群をもつ（命題 3.12 参照）。よって、問題の仮定により、G の位数は素数でなくてはならない。これで、G が素数位数の巡回群であることが示されたので、この場合も (2) が成り立つ。以上で (2) が成り立つことがわかったので、証明が終わる。

記号に関する注意：対称群の元である互換は、通常、(12) などと、2 つの数の間にコンマをいれないで書き表している。しかし、問題 3.7 や問題 3.8 など互換の中に記号が登場するときは数の「切れ目」がわかりにくい。そのような場合には、適宜、$(i, i+1)$ などのように、コンマを入れて切れ目を明示することがある。長さ 3 以上の循環置換についても同じである。

問題 3.7　$H = \langle (12), (12\cdots n) \rangle \subset S_n$ とおく。$2 \leq i \leq n$ をみたす i に対して $\sigma_i = (12\cdots n)^{i-1}$ とおけば、$\sigma_i \in H$ であり、$\sigma_i(1) = i, \sigma_i(2) = i+1$ が成り立つ。よって、$\sigma_i(12)\sigma_i^{-1} = (i, i+1)$ であること（命題 3.17(3) 参照）から、$(i, i+1) \in H$ である。さらに、簡単な計算で

$$(1, i+1) = (1, i)(i, i+1)(1, i) \qquad (*)$$

であることがわかる。よって、まず $(12) \in H$ であることと $i = 2$ に対する $(*)$ から $(13) \in H$ がわかる。つぎに、$(13) \in H$ と $i = 3$ に対する上の等式から $(14) \in H$ がわかる。この議論を繰り返せば、$(12), (13), \cdots, (1n) \in H$ が示せる。すると、系 3.16 によって、$H = S_n$ が成り立つ。これが証明すべきことであった。

問題 3.8　(1) 部分群ではない（理由：単位元が X の元ではない；命題 3.7(1) 参照）。

(2) 部分群である（理由：$X = \{\epsilon\}$（単位群）である）。

(3) $n = 2$ のときは部分群である（$X = \{\epsilon\}$ となる）が、$n \geq 3$ のときは部分群ではない。（理由：$n \geq 3$ のとき、$\sigma_1 = (n-2, n), \sigma_2 = (n-2, n-1) \in S_n$（互換）とすれば、$\sigma_1, \sigma_2 \in X$ だが $\sigma_2\sigma_1 = (n-2, n, n-1) \notin X$ である。）

(4) 部分群である（理由：定義 3.6 の条件が成り立つことが確かめられる；詳細は省略）。

(5) 部分群ではない（理由：単位元が X の元ではない；命題 3.7(1) 参照）。

問題 3.9　素数 p に対して、$\mathbf{Q}^\times$ の部分群 $H(p, n)$ を

$$H(p, n) = \left\{ \frac{b}{a} \in \mathbf{Q}^\times \mid a, b \in \mathbf{Z},\ \mathrm{ord}_p(b) - \mathrm{ord}_p(a) \equiv 0 \pmod{n} \right\}$$

と定める（記号 ord_p については、p.25 参照）。このとき、$H(p, n)$ は $\mathbf{Q}^\times$ の指数 n の部分群である（$\mathbf{Q}^\times / H(p, n)$ の代表元として、$1, p, p^2, \cdots, p^{n-1}$ がとれる）。さらに、2 つの素数 p, p' について、$p \neq p' \Longrightarrow H(p, n) \neq H(p', n)$ が成り立つ（理由：$n \geq 2$ により、$p \neq p'$ のとき $p' \in H(p, n), p \notin H(p, n)$ である）。素数は無限個存在する（定理 1.41）ことから、$\mathbf{Q}^\times$ の指数 n の部分群が無限個存在することがわかる。

問題 3.10　記号を簡単にするために、$H_0 = K \cap H$ とおく。最初に、$k, k' \in K$ が $kH_0 \cap k'H_0 = \emptyset$ をみたすと仮定して、$kH \cap k'H = \emptyset$ であることを示す。もし $kH \cap k'H \neq \emptyset$ ならば、$l \in kH \cap k'H$ をとることができる。$l \in kH$ より $l = kh$ をみたす $h \in H$ があり、$l \in k'H$ より $l = k'h'$ をみたす $h' \in H$ がある。すると $kh = k'h'$ である（両方とも l に等しい）から、$k'^{-1}k = h'h^{-1}$ が成り立つ。ここで $m = k'^{-1}k = h'h^{-1}$

とおけば、$m = k'^{-1}k$ より $m \in K$ であり、$m = h'h^{-1}$ より $m \in H$ であるので、$m \in H_0 (= K \cap H)$ となる。すると $k = k'm \in k'H_0$ であるから、$k \in kH_0 \cap k'H_0$ となり、$kH_0 \cap k'H_0 = \emptyset$ であるという仮定に矛盾する。よって、背理法によって、$kH \cap k'H = \emptyset$ が成り立つことが示せた。

さて、$k_1, k_2, \cdots, k_n \in K$ が $k_1H_0 \cup k_2H_0 \cup \cdots \cup k_nH_0$（ディスジョイント）をみたすとする。すると、上で証明したことから、$k_1H \cup k_2H \cup \cdots \cup k_nH$（ディスジョイント）が成り立つ。したがって、$(K : H_0)$ が有限のときは $n = (K : H_0)$ とすることで、$(G : H) \geq n = (K : H_0)$ が示される。また、$(K : H_0)$ が無限であれば、いくらでも大きな n に対して $(G : H) \geq n$ であることがわかるので、$(G : H)$ も無限である。いずれにしても $(G : H) \geq (K : H_0)$ が成り立つ。

問題 3.11　群同型 $\varphi : G_1 \to G_2$ が存在すると仮定して、$a = \varphi(2) \in G_2$ とおく。このとき、$2b = a$ をみたす $b \in G_2$ をとる（つまり、$b = \frac{a}{2} \in G_2 = \mathbf{Q}$）。すると、$\varphi$ は群同型であるから、$b = \varphi(x)$ をみたす $x \in G_1$ が存在する。したがって、$\varphi(2) = a = 2b = 2\varphi(x) = \varphi(x^2)$ である。よって、$2 = x^2$ が成立する。（注：φ は全単射であるから、$\varphi(2) = \varphi(x^2)$ から $2 = x^2$ が導かれる。）しかし、$x^2 = 2$ をみたす元 $x \in \mathbf{Q}^\times$ は存在しない（p.23 参照）から、これは矛盾である。よって、G_1 と G_2 は同型ではあり得ない。

問題 3.12　条件をみたす写像の一例として、つぎのものが挙げられる。

(1) $\varphi(z) = \frac{z}{|z|}$　$(z \in \mathbf{C}^\times)$

(2) $\psi(z) = \frac{z^2}{|z|^2}$　$(z \in \mathbf{C}^\times)$

問題 3.13　G の H による左コセット分解が

$$G = \tau_1 H \cup \tau_2 H \cup \cdots \cup \tau_p H \quad (\text{ディスジョイント})$$

で与えられるとする。ただし、$\tau_1 = \epsilon$（単位元）ととることにする（したがって、$\tau_1 H = H$ である）。また、H の左コセット全体の集合 G/H を X と書き、群の演算によって H を X に左から作用させる。（具体的に書けば、$X = \{\tau_1 H, \tau_2 H, \cdots, \tau_p H\}$ であり 、H の作用は $h \in H$ と $i = 1, 2, \cdots, p$ に対して $h \cdot \tau_i H = h\tau_i H$ で与えられる。）これから、この作用の軌道分解を考察する。

まず、$hH = H$ $(h \in H)$ であることから、$H = \tau_1 H \in X$ の軌道は H のみである（注：定義 3.53 の記号では、$\mathrm{Orb}(H) = \{H\}$）。つぎに $2 \leq i \leq p$ をとり、$\tau_i H \in X$ の固定群を H_i とする（記号で書けば、$H_i = \{h \in H \mid h\tau_i H = \tau_i H\}$ である）。H_i は H の部分群であり、$\tau_i H$ の軌道（注：定義 3.53 の記号では、$\mathrm{Orb}(\tau_i H)$）の元の個数は群の指数 $(H : H_i)$ に等しい（命題 3.56(3) 参照）。また、すでに $\mathrm{Orb}(H) = \{H\}$ であることはわかっているので、X の軌道分解を考えれば、$(H : H_i) = |\mathrm{Orb}(\tau_i H)| \leq |X| - |\mathrm{Orb}(H)| = p - 1$ が成り立つ。

ここで、$H_i = H$ であることを（背理法で）示すために、$H_i \neq H$ であると仮定する。すると、$(H : H_i) > 1$ が成り立つ（命題 3.33）。また、指数 $(H : H_i)$ は H の位数 $|H|$ の約数であり（定理 3.34）、$|H|$ は $|G|$ の約数である（系 3.35(1)）ので、$(H : H_i)$ は $|G|$ の約数となる。よって、p が $|G|$ を割り切る最小の素数であることから、$(H : H_i) \geq p$ でなくてはならない。（注：一般的に、p が自然数 n を割り切る最小の素数、d が n の約数で $d > 1$ であるなら、$d \geq p$ でなくてはならない。）しかし、これは前に示した不等式 $(H : H_i) \leq p - 1$ と矛盾している。したがって、$H_i \neq H$ ではあり得ないので、$H_i = H$ でなくてはならない。

以上で、すべての i $(1 \leq i \leq p)$ について $\mathrm{Orb}(\tau_i H) = \{\tau_i H\}$ であることが示せた。これは、作用の定義により、

$$h\tau_i H = \tau_i H \quad (\text{すべての } i = 1, \cdots, p \text{ とすべての } h \in H)$$

が成り立つことに他ならない。この等式の両辺に左から τ_i^{-1} を掛ければ、$\tau_i^{-1} h \tau_i H = H$ となるので、$\tau_i^{-1} h \tau_i \in H$ が成り立つ（$1 \leq i \leq p$）。h は H の任意の元であったから、これで $\tau_i^{-1} H \tau_i \subset H$ が示された。

さらに、この 2 つの集合は元の個数が等しい（両方とも $|H|$ 個の元からなる）ことから、$\tau_i^{-1}H\tau_i = H$ が導かれる（$1 \leq i \leq p$）。

さて、ここで G の任意の元 $\sigma \in G$ をとるとき、$\sigma^{-1} \in \tau_i H$ をみたす i $(1 \leq i \leq p)$ が定まる（左コセット分解の定義による）。つまり、（この i に対して）$\sigma^{-1} = \tau_i h_1$ をみたす $h_1 \in H$ が存在する。このとき、上で示した等式 $\tau_i^{-1}H\tau_i = H$ と $h_1 \in H$ により

$$\sigma H \sigma^{-1} = h_1^{-1}\tau_i^{-1}H\tau_i h_1 = h_1^{-1}Hh_1 = H$$

が成り立つ。σ は G の任意の元であったから、これで H が G の正規部分群であることが示された（定義 3.36）。

（コメント）この問題（＝章末問題 3.13）の主張は、命題 3.38 の拡張である。（章末問題 3.13 で $p = 2$ である場合が、命題 3.38 になっている。）同じことを、命題 3.38 は章末問題 3.13 の主張の特別な場合である、と表現してもよい。ただし、章末問題 3.13 に対する上の解答は、命題 3.38 の証明を拡張したものではないので、注意してほしい。

（命題 3.38 の証明に対するコメント）命題 3.38 に対する証明は、まだるっこしく感じられるかもしれない。右コセット分解を使えば、証明はつぎのように述べられる。「右コセット」を使わないようにしたかったので本文のような述べ方を採用した、という事情である。

まず、本文で述べたように、$\sigma H = G - H$ が成り立つ。また、G の H による右コセット分解は $G = H \cup H\sigma$（ディスジョイント）となるので、$H\sigma = G - H$ が得られる。よって、$\sigma H = G - H = H\sigma$ が成り立つので、両辺に右から σ^{-1} を掛けて、$\sigma H \sigma^{-1} = H$ が得られる。（証明終わり）

問題 3.14　$A = \{(a,b) \in \mathbf{R} \times \mathbf{R} \mid a^2 - 4b \geq 0\}$ とおき、$\mathbf{R}^2$ の元 $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ を (x_1, x_2) と書き表すことにする。この記号のもとで、写像 $\psi : \mathbf{R}^2 \to A$ を

$$\psi((x_1, x_2)) = (x_1 + x_2, x_1 x_2) \quad ((x_1, x_2) \in \mathbf{R}^2)$$

によって定める。（注：$(x_1 + x_2)^2 - 4x_1x_2 = (x_1 - x_2)^2 \geq 0$ なので、$(x_1 + x_2, x_1x_2) \in A$ である。）このとき、$\psi(\gamma_2 \cdot (x_1, x_2)) = \psi((x_2, x_1)) = \psi((x_1, x_2))$ が成り立つので、ψ から写像 $\varphi : \mathbf{R}^2/C_2 \to A$ が定まる（命題 A.7 参照）。この φ が $\mathbf{R}^2/C_2$ と A の間の全単射を与える。その理由は、つぎのことからわかる。$(a,b) \in A$ とするとき、2 次方程式 $x^2 - ax + b = 0$ は（重複度を考慮して）2 つの実数解 x_1, x_2 をもつ（この 2 次方程式の判別式が $a^2 - 4b$ であることに注意）。このとき、$\psi((x_1, x_2)) = (a,b)$ が成り立つ。よって、φ は全射である。また、2 次方程式 $x^2 - ax + b = 0$ の解は、（順序を無視して）1 組しかない。したがって、φ は単射である。

問題 3.15　群 G の位数が p^2 であるとし、G が可換群であることを示す。定理 3.57 により、G の中心 $\mathrm{Cent}(G)$ は単位群ではない。また、p は素数であるから、$\mathrm{Cent}(G)$ の位数は p か p^2 に等しい（系 3.35(1) 参照）。$\mathrm{Cent}(G)$ の位数が p^2 であれば、$G = \mathrm{Cent}(G)$ となるので、G は可換群である。$\mathrm{Cent}(G)$ の位数が p のとき、$\mathrm{Cent}(G)$ の単位元以外の元（の 1 つ）を σ とし、$\mathrm{Cent}(G)$ に属さない G の元（の 1 つ）を τ とする。このとき、$\sigma \in \mathrm{Cent}(G)$ なので、σ と τ は可換である。また、$\mathrm{Cent}(G)$ は σ で生成され（つまり、$\mathrm{Cent}(G) = \langle\sigma\rangle$）、剰余群 $G/\mathrm{Cent}(G)$ は τ の剰余類 $\tau\mathrm{Cent}(G)$ で生成される（理由：$\mathrm{Cent}(G)$ と $G/\mathrm{Cent}(G)$ は位数が素数の巡回群なので、部分群は単位群と自分自身しかない；章末問題 3.6 参照）。このことから、G が σ と τ で生成されることがわかる（$G = \langle\sigma, \tau\rangle$）。上に述べたように σ と τ が可換であるから、G は可換群である。

問題 3.16　最初に

$$G \text{ は位数 } p^{n-1} \text{ の部分群をもつ} \tag{$*$}$$

ことを、n に関する数学的帰納法で証明する。$n=1$ のとき $(*)$ が成立するのは明らかである（単位群が条件をみたす）。つぎに $n \geq 2$ とし、$m < n$ をみたすすべての自然数 m について、性質

$$\text{位数が } p^m \text{ の群は、位数が } p^{m-1} \text{ の部分群をもつ} \tag{$**$}$$

が成り立つと仮定する（数学的帰納法の仮定）。

$(*)$ を証明するために、G を位数が p^n の群とする。

(i) まず、G が可換群である場合を扱う。単位元以外の G の元を 1 つとり、それを σ とする。さらに、σ の生成する G の部分群を N とする（$N = \langle\sigma\rangle$）。G が可換群なので、N は G の正規部分群である（命題 3.37(3)）。N の位数は $|G| = p^n$ の約数（系 3.35(1)）なので、$|N| = p^l$ $(1 \leq l \leq n)$ と表される。$l = n$ のときは σ^p の生成する部分群の位数は p^{n-1} である（命題 3.12(2)）。よって、この場合は $(*)$ が成り立っている。$1 \leq l < n$ のとき、剰余群 G/N の位数を p^m とすれば $m = n - l$ なので、$1 \leq m < n$ が成り立っている。したがって、数学的帰納法の仮定 $(**)$ によって、G/N は位数 p^{m-1} の部分群 H' をもつ。ここで、自然な群準同型 $\varphi : G \to G/N$（例 3.54 参照）による H' の引き戻しを H とする（記号では、$H = \{\tau \in G \mid \varphi(\tau) \in H'\}$ と表される）。すると、H は、N を含む G の部分群であり、剰余群 H/N は H' と同型な群である。よって、

$$|H| = |H'| \times |N| = p^{m-1} \times p^l = p^{m+l-1} = p^{n-1}$$

であるので、$(*)$ が成り立つ。以上で、G が可換群のときは、$(*)$ が証明された。

(ii) つぎに、G が非可換群と仮定して、$(*)$ を証明する。定理 3.57 により、G の中心 $\mathrm{Cent}(G)$ は単位群ではない。また、G は可換群ではないから、$G \neq \mathrm{Cent}(G)$ である。よって、$\mathrm{Cent}(G)$ の位数を p^l とすれば、$1 \leq l < n$ である。さらに、剰余群 $\overline{G} = G/\mathrm{Cent}(G)$ の位数を p^m とすれば、$m = n - l$ であるので、$1 \leq m < n$ が成り立つ。したがって、数学的帰納法の仮定 $(**)$ により、$\overline{G}$ は位数 p^{m-1} の部分群 H' をもつ。ここで、自然な群準同型 $\varphi : G \to \overline{G}$ による H' の引き戻しを H とする（つまり、$H = \{\tau \in G \mid \varphi(\tau) \in H'\}$）。すると、$H$ は G の部分群で、

$$|H| = |H'| \times |\mathrm{Cent}(G)| = p^{m-1} \times p^l = p^{m+l-1} = p^{n-1}$$

であるので、$(*)$ が成り立つ。以上で、G が非可換群のときにも、$(*)$ が証明された。

上の (i)(ii) によって、$(*)$ が完全に証明された。

最後に、$(*)$ を利用して、n に関する数学的帰納法で問題の主張を証明する。そのために、G を位数が p^n の群として、$1 \leq k \leq n$ とする。まず、$n = 1$ のときに問題の主張が成り立つことは明らかである（k の可能性は $k = 1$ しかなくて、G 自身が位数 p の部分群になっている）。つぎに、位数が p^{n-1} の群については問題の主張が成り立つと仮定して、G が位数 p^k の部分群をもつことを証明する。さて、$k = n$ であれば、G 自身が位数 p^k の部分群なので、問題の主張は成り立つ。つぎに $k \leq n-1$ と仮定する。このとき、G の位数が p^{n-1} の部分群（の 1 つ）を G' とする（$(*)$ によって、G' が存在することが保証されている）。すると、$|G'| = p^{n-1}$ であり $1 \leq k \leq n-1$ であるから、帰納法の仮定により、G' は位数 p^k の部分群 H をもつ。このとき、H は G の部分群でもあるので、G が位数 p^k の部分群をもつことが示された。

以上で数学的帰納法が完成して、問題の主張が証明された。

「代数と数論の基礎」(中島匠一)　「付録」の章末問題の解答例

問題 A.1　(1)　$a \in A, b \in B$ とするとき、

$$\begin{aligned}
(a,b) \in A \times B - A' \times B' &\iff (a,b) \notin A' \times B' \\
&\iff a \notin A' \text{ または } b \notin B' \\
&\iff a \in A - A' \text{ または } b \in B - B' \\
&\iff (a,b) \in (A - A') \times B \text{ または } (a,b) \in A \times (B - B') \\
&\iff (a,b) \in ((A - A') \times B) \cup (A \times (B - B'))
\end{aligned}$$

が成り立っている。したがって、集合の等式

$$A \times B - A' \times B' = ((A - A') \times B) \cup (A \times (B - B'))$$

が成立する。

(2) $a \in A, b \in B$ について、つぎの 4 つの場合分けが生じる。

(i) $a \in A'$ かつ $b \in B'$

(ii) $a \in A'$ かつ $b \notin B'$

(iii) $a \notin A'$ かつ $b \in B'$

(iv) $a \notin A'$ かつ $b \notin B'$

これらは、それぞれ

(i) $(a,b) \in A' \times B'$

(ii) $(a,b) \in A' \times (B - B')$

(iii) $(a,b) \in (A - A') \times B'$

(iv) $(a,b) \in (A - A') \times (B - B')$

に対応しているので、(2) の等式が成立する。また、条件 (i)(ii)(iii)(iv) はどれも互いに両立しないので、(2) の右辺の和集合はディスジョイントである。

問題 A.2　中島匠一「集合・写像・論理」(共立出版) の 3.9 節に解説がある。

問題 A.3　つぎのように式変形をおこなえばよい。ここで、

$$\text{記号} \sum_{1 \le i < j \le n} \quad \text{と} \quad \sum_{\substack{1 \le i,j \le n \\ i<j}} \quad \text{は同じ意味である}$$

ことと、変形の最後のほうで和の条件が $i > j$ から $i < j$ に変わっている部分では「i と j の入れ替え」をおこなっていることに注意。

$$\begin{aligned}
&\left(\sum_{i=1}^{n} x_i^2\right)\left(\sum_{i=1}^{n} y_i^2\right) - \left(\sum_{i=1}^{n} x_i y_i\right)^2 \\
&= \left(\sum_{i=1}^{n} x_i^2\right)\left(\sum_{j=1}^{n} y_j^2\right) - \left(\sum_{i=1}^{n} x_i y_i\right)\left(\sum_{j=1}^{n} x_j y_j\right)
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{i=1}^{n}\sum_{j=1}^{n} x_i^2 y_j^2 - \sum_{i=1}^{n}\sum_{j=1}^{n} x_i x_j y_i y_j \\
&= \sum_{i=1}^{n} x_i^2 y_i^2 + \sum_{\substack{1\le i,j\le n \\ i\neq j}} x_i^2 y_j^2 - \left(\sum_{i=1}^{n} x_i^2 y_i^2 + \sum_{\substack{1\le i,j\le n \\ i\neq j}} x_i x_j y_i y_j \right) \\
&= \sum_{\substack{1\le i,j\le n \\ i\neq j}} x_i^2 y_j^2 - \sum_{\substack{1\le i,j\le n \\ i\neq j}} x_i x_j y_i y_j \\
&= \sum_{\substack{1\le i,j\le n \\ i<j}} x_i^2 y_j^2 + \sum_{\substack{1\le i,j\le n \\ i>j}} x_i^2 y_j^2 - \left(\sum_{\substack{1\le i,j\le n \\ i<j}} x_i x_j y_i y_j + \sum_{\substack{1\le i,j\le n \\ i>j}} x_i x_j y_i y_j \right) \\
&= \sum_{\substack{1\le i,j\le n \\ i<j}} x_i^2 y_j^2 + \sum_{\substack{1\le i,j\le n \\ i<j}} x_j^2 y_i^2 - \left(\sum_{\substack{1\le i,j\le n \\ i<j}} x_i x_j y_i y_j + \sum_{\substack{1\le i,j\le n \\ i<j}} x_j x_i y_j y_i \right) \\
&= \sum_{\substack{1\le i,j\le n \\ i<j}} \left(x_i^2 y_j^2 + x_j^2 y_i^2 - 2 x_i x_j y_i y_j \right) \\
&= \sum_{\substack{1\le i,j\le n \\ i<j}} \left(x_i y_j - x_j y_i \right)^2
\end{aligned}
$$

問題 A.4　(1) 答えは下の表の通り（注：記号 (b,c) は開区間、$[b,c)$ は半開区間を表している）。

a の範囲	$a \le 0$	$0 < a \le 1$	$1 \le a < 2$	$a \ge 2$
$\mathrm{Image}(f)$	$(0, 1-a)$	$\left[-a^2/4, 1-a\right)$	$\left[-a^2/4, 0\right)$	$(1-a, 0)$

(2) f が単射であるための（必要十分）条件は、$0 \le a \le 2$ が成り立つこと。

（コメント）答えの導き方の詳細は省略する。2 次関数のグラフを描いて考えれば、解答するのは難しくない。

問題 A.5　前半は、中島匠一「集合・写像・論理」（共立出版）命題 4.32 参照。後半の答えは、

$$f \text{ が全射} \quad \Longleftrightarrow \quad f \circ g = \mathrm{id}_B \text{ をみたす写像 } g : B \to A \text{ が存在する}$$

となる（ただし、この主張を一般的に証明するには選択公理が必要である；選択公理については、松坂和夫「集合・位相入門」（岩波書店）などの集合論の教科書を参照）。

問題 A.6　中島匠一「集合・写像・論理」（共立出版）命題 7.9 参照。

問題 A.7　有限集合 X について、$|X|$ は X の元の個数を表す。

(1) $|A| \neq |B|$ なら 0 個（つまり、存在しない）で、$|A| = |B|$ のときは $m!$ 個（$m = |A| = |B|$）。

(2) $|A| > |B|$ なら 0 個（つまり、存在しない）で、$|A| \le |B|$ のときは $n(n-1)\cdots(n-m+1)$ 個（$m = |A|, n = |B|$）。

(3) $|A| < |B|$ なら 0 個（つまり、存在しない）で、$|A| \ge |B|$ のときは $\displaystyle\sum_{k=1}^{n} (-1)^{n-k} \binom{n}{k} k^m$ 個（$m = |A|, n = |B|$）。ここで、$\displaystyle\binom{n}{k}$ は 2 項係数を表している。

問題 A.8　ベルンシュタインの定理（中島匠一「集合・写像・論理」（共立出版）定理 7.31 および定理 7.35 参照）を利用すれば、容易に示せる。

(1) A が無限集合であるから、(A の濃度) $\geq$ (**N** の濃度) である。また、単射 $f : A \to \mathbf{N}$ が存在するので、(A の濃度) $\leq$ (**N** の濃度) が成り立つ。すると、ベルンシュタインの定理により、(A の濃度) = (**N** の濃度) である。よって、「濃度が等しい」ことの定義により、全単射 $g : \mathbf{N} \to A$ が存在する。

(2) B が無限集合であるから、(B の濃度) $\geq$ (**N** の濃度) である。また、全射 $h : \mathbf{N} \to B$ が存在するので、(B の濃度) $\leq$ (**N** の濃度) が成り立つ。よって、ベルンシュタインの定理により、(B の濃度) = (**N** の濃度) である。よって、「濃度が等しい」ことの定義により、全単射 $j : \mathbf{N} \to B$ が存在する。

問題 A.9　中島匠一「集合・写像・論理」（共立出版）例 4.42 参照。

問題 A.10　**（訂正 1）** 問題 (2) は正しくない主張でした。（たとえば、$\alpha = \frac{1}{2}$ のときに $\mathrm{Image}(f_\alpha) = \mathbf{N} \cup \{0\} \neq \mathbf{N}$ であることがすぐにわかります。）問題文をつぎのように変更してください。

(2') $\alpha < 1$ なら $\mathrm{Image}(f_\alpha) = \mathbf{N} \cup \{0\}$ であることを示せ。

（訂正 2） (4) で与えた条件は正しくありませんでした。(4) の文章の「 $\cdots$ 必要十分条件は $\cdots$ 」の部分を、「 $\cdots$ 必要十分条件は α, β が無理数で $\frac{1}{\alpha} + \frac{1}{\beta} = 1$ が成り立つことである。」と訂正してください。

（解答）(1) f_α が単射であるための条件は $\alpha \geq 1$ である。理由はつぎの通り。

まず、$\alpha \geq 1$ と仮定して、f_α が単射であることを示す。2 つの自然数 n_1, n_2 が $f_\alpha(n_1) = f_\alpha(n_2)$ をみたすとすれば、定義により、$[n_1\alpha] = [n_2\alpha]$ が成り立つ。これから、$|(n_1 - n_2)\alpha| < 1$ が導かれる（注：一般に 2 つの実数 x_1, x_2 について、$[x_1] = [x_2] \implies |x_1 - x_2| < 1$ が成立している）。すると、$\alpha \geq 1$ より $|n_1 - n_2| < \frac{1}{\alpha} \leq 1$ となるが、n_1, n_2 は自然数であるから、$n_1 = n_2$ でなくてはならない。以上で、f_α が単射であることがわかった。

つぎに、$\alpha < 1$ と仮定して、f_α が単射でないことを示す。（以下の議論では、仮定により $\alpha > 0$ であることに注意。）そのために、$\frac{1}{1-\alpha}$ の整数部分を N とする。すると、$0 < \alpha < 1$ から $\frac{1}{1-\alpha} > 1$ が導かれるので、N は自然数である。ここで、$N \leq \frac{1}{1-\alpha}$ であることから $N - 1 \leq N\alpha$ が導かれ、$\frac{1}{1-\alpha} < N + 1$ であることから $(N+1)\alpha < N$ が導かれる。これらを合わせて

$$N - 1 \leq N\alpha < (N+1)\alpha < N$$

が成り立つので、$[N\alpha] = N - 1, [(N+1)\alpha] = N - 1$ が得られる。これは $f_\alpha(N) = f_\alpha(N+1)$ であることを示しているので、f_α は単射ではない。

(2')（上の**（訂正 1）**参照）$\alpha < 1$ であるとする。$\alpha > 0$ であることから、$\mathrm{Image}(f_\alpha) \subset \mathbf{N} \cup \{0\}$ は明らかである。

これから、逆方向の包含関係を示す。そのために、$m \in \mathbf{N} \cup \{0\}$ を（任意に）とり、$m \in \mathrm{Image}(f_\alpha)$ であることを示す。まず $m = 0$ のときは、$\alpha < 1$ より $f_\alpha(1) = [\alpha] = 0$ となるので、$0 \in \mathrm{Image}(f_\alpha)$ である。つぎに、$m \geq 1$ として、$m \leq n\alpha$ をみたす最小の $n \in \mathbf{N}$ をとる（$\alpha > 0$ より、これは可能）。このとき、n の最小性より、$(n-1)\alpha < m$ が成り立つ。このことと $\alpha < 1$ から、

$$n\alpha = (n-1)\alpha + \alpha < m + \alpha < m + 1$$

が得られる。結局、$m \leq n\alpha < m + 1$ であるので、$f_\alpha(n) = [n\alpha] = m$ となり、$m \in \mathrm{Image}(f_\alpha)$ が成り立つ。m は $\mathbf{N} \cup \{0\}$ の任意の元であったから、これで $\mathbf{N} \cup \{0\} \subset \mathrm{Image}(f_\alpha)$ が示された。

以上で両方向の包含関係が示されたので、$\mathrm{Image}(f_\alpha) = \mathbf{N} \cup \{0\}$ が証明された。

(3) $\Longleftarrow$ が成り立つことは明らかなので、$\Longrightarrow$ を証明すればよい。そのために $\mathrm{Image}(f_\alpha) = \mathbf{N}$ であると仮定する。仮定により、任意の $m \in \mathbf{N}$ について $f_\alpha(n) = m$ をみたす $n \in \mathbf{N}$ が存在する。m に対し、

$f_\alpha(n)=m$ をみたす n を 1 つ選び、それを n_m と書くことにする。すると、f_α が単調非減少であることから、$n_1<n_2<\cdots$ が成り立つ。n_m はすべて自然数であるから、この不等式から、任意の m について $n_m\geq m$ でなくてはならないことがわかる。（理由：まず n_1 は自然数であるから $n_1\geq 1$ である。すると、$n_2>n_1$ より、$n_2\geq n_1+1\geq 2$ が成り立つ。つぎは、$n_3>n_2$ より、$n_3\geq n_2+1\geq 3$ が導かれる、$\cdots$ と、同じ議論を繰り返せば、$n_m\geq m$ が示される。）以上のことから、任意の m について不等式

$$m=f_\alpha(n_m)=[n_m\alpha]>n_m\alpha-1\geq m\alpha-1$$

が導かれる（注：任意の実数 x について $[x]>x-1$ である）。この不等式の両辺を m で割って $m\to\infty$ での極限をとれば、$1\geq\alpha$ が得られる。一方、(2') によって、$\alpha<1$ ではあり得ないことがわかっている。したがって、$\alpha=1$ でなくてはならない。これで、$\Longrightarrow$ も証明された。

(4)（上の**（訂正 2）**参照）最初に、$\mathbf{N}=S_\alpha\cup S_\beta$（ディスジョイント）であると仮定して、

$$\alpha\ \text{と}\ \beta\ \text{は（両方とも）無理数で、}\frac{1}{\alpha}+\frac{1}{\beta}=1\ \text{が成り立つ}\qquad(*)$$

ことを証明する。そのために、（任意の）自然数 m に対して、S_α の元 u で $u<m$ をみたすものの個数を a_m とし、S_β の元 v で $v<m$ をみたすものの個数を b_m とする。m より小さい自然数の個数は $m-1$ であるから、仮定により、$a_m+b_m=m-1$ が成り立っている。一方、(1) の結果により f_α は単射であるから、a_m は $[n\alpha]<m$ をみたす自然数 n の個数に等しい。すると、

$$[n\alpha]<m\iff n\alpha<m\iff n<\frac{m}{\alpha}$$

であるので、a_m は $\left[\frac{m}{\alpha}\right]$ または $\left[\frac{m}{\alpha}\right]-1$ に等しい（注：$\frac{m}{\alpha}$ が整数となる場合に後者がおきる）。同様にして、b_m が $\left[\frac{m}{\beta}\right]$ または $\left[\frac{m}{\beta}\right]-1$ に等しいこともわかる。したがって、

$$0\leq\left[\frac{m}{\alpha}\right]+\left[\frac{m}{\beta}\right]-(a_m+b_m)\leq 2$$

が成り立つ。この不等式を（一斉に）m で割って $a_m+b_m=m-1$ を代入し、$m\to\infty$ での極限をとれば、$\frac{1}{\alpha}+\frac{1}{\beta}=1$ が得られる（注：実数 x について、$x\to\infty$ のとき $\frac{[x]}{x}\to 1$ である）。

つぎに、α と β が（両方とも）無理数であることを、背理法で証明する。そのために、α か β のどちらかが有理数であると仮定する。すると、等式 $\frac{1}{\alpha}+\frac{1}{\beta}=1$ により、もう一方も有理数でなくてはならない。つまり、α と β は両方とも有理数となるので、$\alpha=\frac{b}{a},\beta=\frac{d}{c}$ と表す（a,b,c,d は自然数; α,β は正であることに注意）。このとき、$n=ad, n'=bc$ とすれば、$[n\alpha]=[n'\beta]$ が成り立つ（両方とも bd に等しい）。しかし、$[n\alpha]\in S_\alpha, [n'\beta]\in S_\beta$ であるから、これは最初の仮定である $S_\alpha\cap S_\beta=\emptyset$ に矛盾している。「α か β のどちらかが有理数」と仮定して矛盾が導かれたので、α と β は両方とも無理数でなくてはならない。

以上で、$\mathbf{N}=S_\alpha\cup S_\beta$（ディスジョイント）であれば、$(*)$ が成り立つことが示された。

逆を証明するために、$(*)$ が成り立っていると仮定する。そして、$m\in\mathbf{N}$ を（任意に）とる。このとき、m に対して、$[n\alpha]=m$ をみたす自然数 n か $[n'\beta]=m$ をみたす自然数 n' のどちらか一方だけが存在することを示せばよい。

さて、

$$[n\alpha]=m\iff m\leq n\alpha<m+1\iff\frac{m}{\alpha}\leq n<\frac{m}{\alpha}+\frac{1}{\alpha}<\frac{m}{\alpha}+1$$

である（$\alpha>1$ より $\frac{1}{\alpha}<1$ であることに注意）。したがって、$[n\alpha]=m$ をみたす n があるとすれば、それは $\frac{m}{\alpha}\leq n$ をみたす最小の自然数でなくてはならない。（注意：この主張の逆は成立しない；言い換えれば、「$\frac{m}{\alpha}\leq n$ をみたす最小の自然数」を n とするとき、$[n\alpha]=m$ が成り立つとは限らない。）そこで、m に対して、「$\frac{m}{\alpha}\leq n$ をみたす最小の自然数 n」をとり、$t=n-\frac{m}{\alpha}$ とおく。定義により $0\leq t<1$ であるが、α は無理数、という仮定により t も無理数なので、t は 0 ではあり得ない。したがって、$0<t<1$ である。n と t の定義により $m=n\alpha+t\alpha$ であるので、「$[n\alpha]=m$ が成り立つことは $t\alpha<1$ と同値」である。

α の代わりに β をとっても同じ議論がおこなえる。つまり、「$\frac{m}{\beta} \leq n'$ をみたす最小の自然数 n'」をとり $t' = n' - \frac{m}{\beta}$ とおく。このとき、$0 < t' < 1$ であり、「$[n\beta] = m$ が成り立つことは $t'\beta < 1$ と同値」である。

上の記号を使えば、証明すべき主張は「$t\alpha < 1$ か $t'\beta < 1$ のどちらか一方だけが成り立つ」ことである。

t, t' の定義と $(*)$ の 2 番目の条件より

$$t + t' = n + n' - \left(\frac{m}{\alpha} + \frac{m}{\beta}\right) = n + n' - \left(\frac{1}{\alpha} + \frac{1}{\beta}\right) m = n + n' - m$$

が成り立つので、$t + t'$ は整数である。一方、$0 < t, t' < 1$ より $0 < t + t' < 2$ である。よって、$t + t'$ が整数なので、$t + t' = 1$ でなくてはならない。等式 $t + t' = 1$ を

$$\frac{t\alpha}{\alpha} + \frac{t'\beta}{\beta} = 1 \qquad (**)$$

と書き換えて、$(*)$ の等式と較べる。ここで、$(*)$ の最初の条件から $t\alpha$ と $t'\beta$ は無理数である（$t\alpha = n\alpha - m, t'\beta = n'\beta - m'$ に注意）。よって、$t\alpha, t'\beta$ はどちらも 1 に等しくはない。すると、$(*)$ の等式と $(**)$ が両方成り立つためには、$t\alpha, t'\beta$ のどちらか一方は 1 より小さく、もう一方は 1 より大きくなくてはならないことがわかる（理由：両方とも 1 より小さければ $(**)$ の左辺が 1 より小さくなってしまうし、両方とも 1 より大きければ $(**)$ の左辺が 1 より大きくなってしまう）。これで「$t\alpha < 1$ か $t'\beta < 1$ のどちらか一方だけが成り立つ」ことが示された。つまり、$m = [n\alpha]$ か $m = [n'\beta]$ のどちらか一方だけが成り立つことがわかった。m は $\mathbf{N}$ の任意の元であったので、これで $\mathbf{N} = S_\alpha \cup S_\beta$（ディスジョイント）が証明された。

（コメント）この問題の (4) はヴィノグラドフ「整数論入門」（共立全書；共立出版）の「第 2 章の問題 3 番」から取りました。難しい問題だったので出題の形式を少し変更したのですが、その際に (2)(4) で誤りが混入してしまいました。申し訳ありませんでした。

問題 A.11

（解答例 1）$\lim_{n\to\infty} a_n = a$ であるが $\lim_{n\to\infty} f(a_n) = f(a)$ をみたさない数列 $\{a_n\}$ が存在する。

（解答例 2）$\lim_{n\to\infty} a_n = a$ をみたすある数列 $\{a_n\}$ について、つぎの条件 (i)(ii) のどちらかが成り立つ。

(i) $n \to \infty$ のとき $f(a_n)$ は収束しない。

(ii) $n \to \infty$ のとき $f(a_n)$ は $f(a)$ 以外の値に収束する。

（コメント）「$\lim_{n\to\infty} a_n = a$ かつ $\lim_{n\to\infty} f(a_n) \neq f(a)$ をみたす数列 $\{a_n\}$ が存在する。」という解答は間違っています。このことをよく理解しておいてください。理由は、「記号の意味」に関わっています。具体的に言うと、$\lim_{n\to\infty} f(a_n) \neq f(a)$ という表現は、「極限 $\lim_{n\to\infty} f(a_n)$ は存在するが、その値は $f(a)$ には等しくない」という意味に解釈されて、そして、それは（解答例 2）の条件 (ii) と同じです。しかし、（解答例 2）の条件 (i) をみたす場合も実際にあるわけで、それを無視してはいけないのです。

別の言い方をすると、表現 $\lim_{n\to\infty} f(a_n) \neq f(a)$ は「$\lim_{n\to\infty} f(a_n) = f(a)$ の否定」**ではない**、ということです。

問題 A.12　(1)「甘くない砂糖がある。」

(2)「（A 君が）勉強しているとしたら、それは彼が叱られたからだ。」

（コメント） 中島匠一「集合・写像・論理」（共立出版）の 2.9 節に「カラスは黒い」の否定についての説明があります。(1) の解答の参考にしてください。

(2) は、日本語の言い回しに関するジョークです。「叱られないと勉強しない」を『「叱られない」ならば「勉強しない」』と ” 言い換え ” て、「P ならば Q」の対偶の作り方を ” 形式的に ” 適用すると、『「勉強する」ならば「叱られる」』となってしまいます。これはどう考えてもヘンだろう、というのが「ジョー

ク」という意味です。これは、日常会話での「ならば」の使い方と厳密な論理での「ならば」の使い方のズレが引き起こす問題です。この類いの現象については、中島匠一「集合・写像・論理」（共立出版）の第2章に解説があります。

問題 A.13　**(ER1)** を導こうとした山村君は「$a \sim b$ なら」といって、元 a に対して $a \sim b$ をみたす b が（少なくとも1つ）存在することにして話を進めてしまっている。しかし、2つの条件 **(ER2)** と **(ER3)** だけからは、a に対して「$a \sim b$ をみたす b の存在」を導くことはできない（実際、「$a \sim b$ をみたす a,b が1組も存在しない」という状況だと、**(ER2)** と **(ER3)** は成立するが、**(ER1)** は成立しない）。したがって、残念ながら、山村君の議論は無効である。

（コメント） 山村君の議論を生かすためには、**(ER1)** より弱い条件である

(ER1)' 任意の a に対して、$a \sim a'$ をみたす a' が（少なくとも1つ）存在する

を考えて、同値関係の定義を「3つの条件 **(ER1)'(ER2)(ER3)** をみたすこと」としてもよい。（山村君の議論によって、**(ER2)** と **(ER3)** を使って **(ER1)'** から **(ER1)** を導くことができる。）

条件 **(ER1)'** は、「$a \sim a'$ をみたす a'」が（何でもいいから）とにかく1つ存在すればいい、といっているのに対して、条件 **(ER1)** は、「$a \sim a'$ をみたす a'」として $a' = a$ がとれる、といっている。言い換えれば、条件 **(ER1)'** では a' は存在すれば何でもいいが、条件 **(ER1)** では $a' = a$ として a が「指名」されている。この意味で、「条件 **(ER1)'** は条件 **(ER1)** より弱い（＝条件 **(ER1)** は条件 **(ER1)'** より強い）」と表現される。

問題 A.14　「友達である」という条件について、同値関係の条件を言葉で表現すると

(ER1) 自分は（自分の）友達だ。

(ER2) 俺があいつの友達なら、あいつは俺の友達だ。

(ER3) 友達の友達は友達だ。

となる（ただし、**(ER2)** の表現は、男性バージョン）。これらの条件が成り立つかどうかは、「友達」をどう理解するかに依存している。

問題 A.15

(1) 同値関係である。

(2) 同値関係ではない（**(ER2)** が不成立）。

(3) 同値関係ではない（**(ER1)** と **(ER3)** が不成立）。

(4) 同値関係である。

(5) 同値関係である。

問題 A.16　**（訂正：ミスプリント）** (2) に現れる $A/\sim$ は $\mathcal{P}(A)/\sim$ のミスプリントです。（問題の $\sim$ は $\mathcal{P}(A)$ 上の同値関係です。）

(1) 中島匠一「集合・写像・論理」（共立出版）7.4節参照。（同値関係の条件 **(ER1)**、**(ER2)**、**(ER3)** がそれぞれ例 4.26、命題 4.39、命題 4.43 に対応している。）

(2) 「A の濃度」以下の濃度全体の集合。

(3) 同値類全体の個数は $n+1$ である。また、$0 \leq k \leq n$ をみたす整数 k に対して、A の部分集合 $\{1, 2, \cdots, k\}$ の属する同値類の元の個数は 2 項係数 $\binom{n}{k}$ に等しい。(注：$k = 0$ のときは、集合 $\{1, 2, \cdots, k\}$ は空集合を表す。)