(2013/10/14)

問 1.1 これらは通常は「単射なら像の元の数は元と同じで全射になり，単射でなければ減り全射にならないので明らか」と答えればよい．ちゃんと証明すると次のようになる．

(i) A が有限集合なので，ある負でない整数 n について A から $\{1,\dots,n\}$ に全単射が存在する．A から A への写像には，この全単射により対応する $\{1,\dots,n\}$ からそれ自身へのが考えられるので，$A=\{1,\dots,n\}$ の場合に証明すればよい．$f:A\to A$ を単射とする．f が全射であることを n についての数学的帰納法で証明する．$n=0$ であれば $A=\emptyset$ であるから f は全射である．$n>0$ とする．$f(n)=n$ の場合，すべての $i=1,\dots,n-1$ について $g(i)=f(i)$ とおけば，g は $\{1,\dots,n-1\}$ からそれ自身への単射であり，帰納法の仮定から全射である．よって，f の像は g の像である $\{1,\dots,n-1\}$ を含み，$f(n)=n$ と合わせて f の全射性がわかる．$f(n)<n$ の場合は，$g:\{1,\dots,n-1\}\to\{1,\dots,n-1\}$ を $f(i)\neq n$ なら $g(i)=f(i)$ とし，$f(i)=n$ なら $g(i)=f(n)$ と定義する．ここで，$f(i)=n$ となる i が存在しなければ g は f の制限で $\{1,\dots,n-1\}$ から $\{1,\dots,n-1\}$ への単射である．数学的帰納法の仮定により g は全射で，$g(i)=f(n)<n$ となる $1\leqq i\leqq n-1$ が存在するが，$f(i)=f(n)$ となり，f の単射性に矛盾する．したがって，必ずある i について $f(i)=n$ となる．g の単射性は $g(i)=f(n)$ となる i が 1 つかだけが問題であるが，f の単射性から $f(i)=f(n)$ となる i は n 以外になく，また $f(i)=n$ となる i は 1 つだけであるから g は $\{1,\dots,n-1\}$ からそれ自身への単射である．したがって，この g も数学的帰納法により全射である．$j\in\{1,\dots,n-1\}\setminus\{f(n)\}$ については $g(i)=j$ となる i をとれば $f(i)=j$ であり，f の像が $f(n)$ と n を含むことはわかっているので f は全射である．

(ii) $f:A\to A$ を全射とする．各 $i\in A$ について $f(j)=i$ となる j が全射性から存在するので，これを 1 つ選んで $g(i)=j$ と定義する．これにより写像 $g:A\to A$ が得られ，$(f\cdot g)(i)=f(g(i))=i$ より，$f\cdot g=1_A$ となる．恒等写像 1_A は単射であるから g も単射で，(i) により g は全単射である．f が単射でないとすると，ある i について $f(j')=i$ となる $g(i)$ 以外の j' が存在するが，この j' は g の像に含まれないので g の全射性に矛盾する．したがって f は単射である．

問 1.3 $a \equiv b \pmod{n}$ は $a-b$ が n の倍数であることとして定義される．

(i) $a-a=0$ で 0 は n の 0 倍である．よって $a \equiv a \pmod{n}$ となる．

(ii) ある整数 l について $a-b=ln$ であるから，$b-a$ は n の $-l$ 倍である．よって $b \equiv a \pmod{n}$ である．

(iii) ある整数 l,m について $a-b=ln$, $b-c=mn$ であるから，$a-c=(a-b)+(b-c)$ は n の $l+m$ 倍である．よって $a \equiv c \pmod{n}$ である．

問 3.1 次の 5 通りがある．

(1) $((a_1a_2)a_3)a_4 = a_1a_2a_3a_4$

(2) $(a_1(a_2a_3))a_4 = ((a_1a_2)a_3)a_4 = a_1a_2a_3a_4$

(3) $(a_1a_2)(a_3a_4) = ((a_1a_2)a_3)a_4 = a_1a_2a_3a_4$

(4) $a_1((a_2a_3)a_4) = (a_1(a_2a_3))a_4 = ((a_1a_2)a_3)a_4 = a_1a_2a_3a_4$

(5) $a_1(a_2(a_3a_4)) = a_1((a_2a_3)a_4) = (a_1(a_2a_3))a_4 = ((a_1a_2)a_3)a_4 = a_1a_2a_3a_4$

問 3.2 一般結合法則の証明：半群 A の重複を許す n 個の元を $a_1, a_2, \ldots, a_{n-1}, a_n$ と並べて書いた場合，もちろんここでは n がいろいろの値をとり得るので途中が省略されているが，実際に n が定まって n 個の元をすべて書いたとすれば，これらは $n-1$ 個のカンマで区切られていることになる．これら $n-1$ 個のカンマを 1 つずつ取り除き，それとともにカンマの両側の元を掛け合わせて 1 つの元とすると考えれば，一般結合法則は取り除くカンマの順番に依らずに最後の元が決まることを主張している．これを n についての数学的帰納法で示したい．$n=1$ ならカンマはないので正しい．$n-1$ 個以下の元については一般結合法則が成り立つと仮定する．カンマを左から順に取り除いて行って得られる元が $a_1 \cdots a_n$ である．ある順でカンマをすべて取り除いたとして，最後に取り除いたカンマが最初に左から k 番目にあったとする．このとき $k, n-k < n$ であるから，このカンマの左の $a_1, \ldots, a_k$ と右の $a_{k+1}, \ldots, a_n$ については一般結合法則が成り立つ．したがって，この場合の最後の積は $(a_1 \cdots a_k)(a_{k+1} \cdots a_n)$ である．これは $k = n-1$ なら $a_1 \cdots a_n$ である．$k < n-1$ なら結合法則により

$$\begin{aligned}(a_1 \cdots a_k)(a_{k+1} \cdots a_n) &= (a_1 \cdots a_k)((a_{k+1} \cdots a_{n-1})a_n) \\ &= ((a_1 \cdots a_k)(a_{k+1} \cdots a_{n-1}))a_n\end{aligned}$$

となり，また帰納法の仮定より

$$(a_1 \cdots a_k)(a_{k+1} \cdots a_{n-1}) = a_1 \cdots a_k a_{k+1} \cdots a_{n-1}$$

であるから，上の式は

$$(a_1 \cdots a_{n-1})a_n = a_1 \cdots a_n$$

に等しい．よって，n 個の元についても一般結合法則が成り立つ．したがって，数学的帰納法によりすべての n について一般結合法則が成り立つ．

n 個の元の積について，そのカッコの付け方の数を $f(n)$ とすると，$f(n)$ は

(1) $f(1) = 1$

(2) $f(n) = \sum_{i=1}^{n-1} f(i)f(n-i) \quad (n = 2, 3, \ldots)$

で計算される．

$n = 20$ まで $f(n)$ を計算する C プログラムとその出力が次のようになる．$f(20)$ は 17 億を超える．

```
/*
カッコの付け方の数
*/
#include <stdio.h>

#define N 20

int main () {
    long f[256];
    int i, n;
    f[1] = 1;
    printf("%03d   %15d\n", 1, f[1]);
    for (n=2; n<=N; n++) {
        f[n] = 0;
        for (i=1; i<n; i++) {
            f[n] += f[i]*f[n-i];
        }
        printf("%03d   %15d\n", n, f[n]);
    }
    return 0;
```

```
}
```

```
001                1
002                1
003                2
004                5
005               14
006               42
007              132
008              429
009             1430
010             4862
011            16796
012            58786
013           208012
014           742900
015          2674440
016          9694845
017         35357670
018        129644790
019        477638700
020       1767263190
```

問 3.3 まず $a_{i_1}\cdots a_{i_n}$ が，ある $1,2,\ldots,n-1$ の順列 $j_1,\ldots,j_{n-1}$ についての $a_{j_1}\cdots a_{j_{n-1}}a_n$ に等しいことを見る．

$i_n=n$ であれば $j_k=i_k$ $(k=1,\ldots,n-1)$ とすればよい．$i_n\neq n$ であれば積の中で $a_n=a_{i_k}$ は右端にはないので，可換性によりこれを右隣の $a_{i_{k+1}}$ と交換しても積の結果は等しい．これを繰り返せば a_n が右端にくるので，最初に述べた形になる．

数学的帰納法により証明を行う．$n=1$ なら並べ方は 1 つなので正しい．$n\leqq 2$ として $n-1$ まで正しいと仮定する．このとき，最初に書いた $a_{j_1}\cdots a_{j_{n-1}}$ に

数学的帰納法を使えば，$a_1 \cdots a_{n-1}$ に等しいので

$$a_{i_1} \cdots a_{i_n} = (a_{j_1} \cdots a_{j_{n-1}})a_n = a_1 \cdots a_{n-1}a_n$$

となる．

問 3.5 (i), (ii) は定義から自明といってよい．ベキ乗が $a^0 = 1$ および $a^n = a^{n-1}a$ $(n = 1, 2, \ldots)$ と帰納的に定義されているとすると，これらは次のように数学的帰納法で証明される．

(i) $n = 0$ とすると $a^m a^0 = a^m 1 = a^m = a^{m+0}$ となり正しい．$n \geqq 1$ として $n-1$ まで正しいと仮定する．この仮定を使うと

$$a^m a^n = a^m a^{n-1} a = a^{m+n-1} a = a^{m+n-1+1} = a^{m+n}$$

となり n の場合が証明される．

(ii) $n = 0$ とすると $(a^m)^0 = 1 = a^{m0}$ となり正しい．$n \geqq 1$ として $n-1$ まで正しいと仮定する．この仮定と (i) を使うと

$$(a^m)^n = (a^m)^{n-1} a^m = a^{m(n-1)} a^m = a^{m(n-1)+m} = a^{mn}$$

となり n の場合も正しい．

(iii) まず，任意の $n \geqq 0$ について $b^n a = ab^n$ を数学的帰納法で示す．$n = 0$ なら $1a = a1$ より正しい．$n > 0$ として $b^{n-1}a = ab^{n-1}$ を仮定する．このとき $b^n a = bb^{n-1}a = bab^{n-1} = abb^{n-1} = ab^n$ となり n でも正しいことがわかる．

次に $(ab)^n = a^n b^n$ を数学的帰納法で示す．$n = 0$ なら $(ab)^0 = 1 = 1 \cdot 1 = a^0 b^0$ で正しい．$n > 0$ として $(ab)^{n-1} = a^{n-1}b^{n-1}$ を仮定する．このとき $(ab)^n = (ab)^{n-1}ab = a^{n-1}b^{n-1}ab = a^{n-1}ab^{n-1}b = a^n b^n$ となり n でも正しい．

問 3.8 $u = u_1 \cdots u_n$ および $u' = u_n^{-1} \cdots u_1^{-1}$ と置けば，

$$uu' = u_1 \cdots u_n u_n^{-1} \cdots u_1^{-1} = u_1 \cdots u_{n-1} u_{n-1}^{-1} \cdots u_1^{-1} = \cdots = u_1 u_1^{-1} = 1$$

となる．$u'u$ も同様に 1 となる．したがって u は正則で u' がその逆元となる．

問 3.9 X^X の積の定義から $\sigma\tau$ は合成写像 $\tau \cdot \sigma$ に等しい．σ が全単射であれば逆写像 σ^{-1} が存在する．$\sigma\sigma^{-1} = \sigma^{-1} \cdot \sigma = \mathrm{id}_X$ および $\sigma^{-1}\sigma = \sigma \cdot \sigma^{-1} = \mathrm{id}_X$ か

ら σ^{-1} が σ の逆元となる．また σ が逆元 σ' をもてば，$\sigma\cdot\sigma' = \sigma'\sigma = \mathrm{id}_X$ と $\sigma'\cdot\sigma = \sigma\sigma' = \mathrm{id}_X$ から σ' が σ の逆写像となり，σ が全単射であることがわかる．

問 4.1 (i) それぞれ，両辺の左から a^{-1} を掛けて

$$ax = ay \Rightarrow x = a^{-1}ax = a^{-1}ay = y\ ,$$

両辺の右から a^{-1} を掛けて

$$xa = ya \Rightarrow x = xaa^{-1} = yaa^{-1} = y$$

が得られる．

(ii) $ax = b$ の両辺に左から a^{-1} を掛けて $x = a^{-1}b$ となり一意性がわかる．また $ax = b$ の x に $a^{-1}b$ を代入すれば $a(a^{-1}b) = aa^{-1}b = b$ となり方程式の解となっている．

$ya = b$ の両辺に右から a^{-1} を掛けて $y = ba^{-1}$ となり一意性がわかる．また $ya = b$ の y に ba^{-1} を代入すれば $(ba^{-1})a = ba^{-1}a = b$ となり方程式の解となっている．

(iii) 合成写像 $f\cdot f$ により任意の $x \in G$ は $x \mapsto x^{-1} \mapsto x$ となるので，$f\cdot f$ は恒等写像である．したがって f は逆写像 f をもち全単射である．

(iv) それぞれ，$g_{a^{-1}}$ が g_a の，$h_{a^{-1}}$ が h_a の，$k_{a^{-1}}$ が k_a の逆写像であることを示せばよい．任意の $x \in G$ について

$$(g_a \cdot g_{a^{-1}})(x) = g_a(xa^{-1}) = xa^{-1}a = x$$

$$(g_{a^{-1}} \cdot g_a)(x) = g_{a^{-1}}(xa) = xaa^{-1} = x$$

$$(h_a \cdot h_{a^{-1}})(x) = h_a(a^{-1}x) = aa^{-1}xx = x$$

$$(h_{a^{-1}} \cdot h_a)(x) = h_{a^{-1}}(ax) = a^{-1}axx = x$$

$$(k_a \cdot k_{a^{-1}})(x) = k_a(axa^{-1}) = a^{-1}axa^{-1}a = x$$

$$(k_{a^{-1}} \cdot k_a)(x) = k_{a^{-1}}(a^{-1}xa) = aa^{-1}xaa^{-1} = x$$

なので，すべて正しいことがわかる．

問 4.4 (i) 単位元は 1 であるが，$0 \in \mathbf{Q}$ には $0a = 1$ となる逆元 a がないので $\mathbf{Q}$ は乗法について群ではない．

(ii) 単位元は 1 であるが，$2 \in \mathbf{Z}^\sharp$ には $2a = 1$ となる逆元 $a \in \mathbf{Z}^\sharp$ がないので $\mathbf{Z}^\sharp$ は乗法について群ではない．

問 4.6 $n \geqq 2$ または $n \leqq -2$ であれば $nn' = 1$ となる n' は $\mathbf{Z}$ には存在しない．1 の逆元は 1 で -1 の逆元は -1 であるから，単数群は $\{1, -1\}$ となる．

問 4.8 $X = \{x_1, x_2, \ldots, x_n\}$ とする．このとき $\sigma \in S_n$ に対して $x_1^\sigma, x_2^\sigma, \ldots, x_n^\sigma$ は $x_1, x_2, \ldots, x_n$ の並べ替えである．逆に任意の並べ替え $y_1, y_2, \ldots, y_n$ について $x_i^\sigma = y_i$ で置換 σ が定義出来る．$x_1, x_2, \ldots, x_n$ の並べ替え全体は $n! = n \times \cdots \times 1$ 個であるから，S_n の位数は $n!$ である．

問 4.10 (i)

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

とすれば

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

となり $\sigma\tau \neq \tau\sigma$ であるから S_3 はアーベル群ではない．$n \geqq 4$ の場合も $i \geqq 4$ について $i^\sigma = i$, $i^\tau = i$ と σ, τ を拡張して定義すれば，同様に $\sigma\tau \neq \tau\sigma$ であるから S_n はアーベル群ではない．

(ii)

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

とすれば

$$AB = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}, \quad BA = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$$

となり $AB \neq BA$ であるから $GL(2, \mathbf{Q})$ はアーベル群ではない．$n \geqq 3$ の場合も $A = [a_{ij}]$, $B = [b_{ij}]$ を $i \geqq 3$ または $j \geqq 3$ なら，

$$a_{ij} = b_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

と拡張して定義すれば，同様に $AB \neq BA$ であるから $GL(n, \mathbf{Q})$ はアーベル群ではない．

問 5.5 環 R の元 a が正則とすると逆元 a^{-1} が存在する．$ab = 0$ であれば，$b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0$ となり，a は左零因子ではない．$ca = 0$ とすると，$c = c(aa^{-1}) = (ca)a^{-1} = 0a^{-1} = 0$ となり，a は右零因子ではない．R が斜体であれば 0 以外の元は正則なので，先に示したように左零因子でも右零因子でもない．

問 6.3 剰余定理の証明：R は一般の可換環でよい．f を $x-\alpha$ で割れば，$x-\alpha$ が 1 次であることから余りは R の元となる．この余りを β として

$$f(x) = (x-\alpha)q(x) + \beta$$

と書ける．ここで x に α を代入すると $f(\alpha) = \beta$ となる．したがって，剰余定理の式が得られる．

因数定理の証明：$x-\alpha | f(x)$ であれば剰余定理において上記の β が 0 なので，$f(\alpha) = 0$ となる．また $f(\alpha) = 0$ であれば $\beta = 0$ であるから $x-\alpha | f(x)$ となる．

問 6.4 $\alpha_1, \ldots, \alpha_d$ を方程式 $f(x) = 0$ の相異なる解とする．因数定理により $f(x) = (x-\alpha_1)f_1(x)$ となる．$i = 2, \ldots, n$ について，この x に α_i を代入すると $(\alpha_i - \alpha_1)f_1(\alpha_i) = 0$ となり，$\alpha_i - \alpha_1 \neq 0$ で R が整域であることから $f_1(\alpha_i) = 0$, すなわち $\alpha_2, \ldots, \alpha_d$ は $f_1(x) = 0$ の解である．したがって，また因数定理により $f_1(x) = (x-\alpha_2)f_2(x)$ となり，先と同様に $\alpha_3, \ldots, \alpha_d$ が $f_2(x) = 0$ の解となる．これを α_d まで繰り返せば

$$f(x) = (x-\alpha_1)f_1 = (x-\alpha_1)(x-\alpha_2)f_2(x) = \cdots = (x-\alpha_1)\cdots(x-\alpha_d)f_d(x)$$

となる．$(x-\alpha_1)\cdots(x-\alpha_d)$ は d 次で $f_d(x)$ は 0 でない多項式なので，$f(x)$ は d 次以上である．よって $d \leqq n$ がわかる．

問 6.5 0 でない多項式 $h(x) = f(x) - g(x)$ が n 次とすると問 6.4 により $h(x) = 0$ の解は n 個以下である．R が無限個の元を含むので解でない $\alpha \in R$ が存在する．このとき $f(\alpha) - g(\alpha) = h(\alpha) \neq 0$ であるから，f^* と g^* の α での値は等しくない．

問 6.6 R が整域であれば 1 変数多項式環 $R[x]$ も整域となることを示す．$f(x), g(x) \in R[x]$ が 0 でないとする．$f(x)$ の最高次の項が ax^m で $g(x)$ の最高次の項が bx^n

とすると，$f(x)g(x)$ の $m+n$ 次の項は $abx^{m+n} \neq 0$ であるので，$f(x)g(x) \neq 0$ がわかる．したがって $R[x]$ は整域である．また，$f(x), g(x)$ のどちらかが 1 次以上であれば積も 1 次以上となるので，積が 1 となるのは $f(x), g(x) \in R$ の場合であり，$R[x]$ の単数は R の単数となる．R の単数が $R[x]$ の単数となるは明らかなので，$R[x]$ の単数群は R の単数群に等しい．$R[x_1, x_2] = (R[x_1])[x_2]$, $R[x_1, x_2, x_3] = (R[x_1, x_2])[x_3]$ のように考えて，これを繰り返せば n 変数多項式環の場合も証明される．

問 6.7 (i) $h(x_1, \ldots, x_n) \neq 0$ であれば $h(\alpha_1, \ldots, \alpha_n) \neq 0$ となる $\alpha_1, \ldots, \alpha_n \in R$ が存在することをいえば，$h = f - g$ として証明される．n についての数学的帰納法で証明する．$n = 1$ はすでに問 6.5 で示した．$n \geqq 2$ として $n-1$ まで正しいと仮定する．$h(x_1, \ldots, x_n)$ を x_n についての多項式と考えれば，係数は整域 $R[x_1, \ldots, x_{n-1}]$ の元である．最高次の項を $h_m(x_1, \ldots, x_{n-1})x_n^m$ とする．帰納法の仮定から $h_m(\alpha_1, \ldots, \alpha_{n-1}) \neq 0$ となる $\alpha_1, \ldots, \alpha_{n-1} \in R$ が存在する．このとき $h(\alpha_1, \ldots, \alpha_{n-1}, x_n)$ は最高次が $h_m(\alpha_1, \ldots, \alpha_{n-1})x_n^m$ の 0 でない 1 変数多項式であるから，$n = 1$ の場合の結果から $h(\alpha_1, \ldots, \alpha_{n-1}, \alpha_n) \neq 0$ となる $\alpha_n \in R$ が存在する．したがって，数学的帰納法によりすべての n について正しいことがわかる．

(ii) $h = fg_1 \cdots g_r$ と置く．$g_1 \cdots g_r \neq 0$ で $R[x_1, \ldots, x_n]$ は整域であるから $f \neq 0$ であれば $h \neq 0$ であるが，仮定から $g_1 \cdots g_r$ が 0 でない所では f が 0 となるので，h はすべての $(\alpha_1, \ldots, \alpha_n) \in R^n$ で 0 となる．これは (i) に矛盾する．したがって $f = 0$ である．

問 7.1 H を G の部分群とすると，$a, b \in H$ であれば教科書の (7.2) より $b^{-1} \in H$ となり，これに $a \in H$ と合わせて (7.1) を使えば $ab^{-1} \in H$ がわかる．

逆に，G の空でない部分集合 H が任意の $a, b \in H$ について $ab^{-1} \in H$ を満たすとする．空でないので $c \in H$ をとり，$c, c \in H$ と考えれば $1 = cc^{-1} \in H$ がわかる．したがって，任意の $b \in H$ について $1, b \in H$ であるから $b^{-1} = 1b^{-1} \in H$ となり，(7.2) が成り立つ．また，$a \in H$ と $b^{-1} \in H$ についてこれを適用すると $ab = a(b^{-1})^{-1} \in H$ となり，(7.1) も成り立つ．したがって H は G の部分群である．

問 7.2 一般に群 G の部分集合 A, A', B, B' について $A' \subset A$ であれば $A'B \subset AB$

であり，$B' \subset B$ であれば $AB' \subset AB$ となる．特に $a \in A$ であれば $aB \subset AB$ で，$b \in B$ なら $Ab \subset AB$ である．

HH, H^{-1}, HH^{-1} が H に含まれることは，それぞれ (7.1), (7.2), 問 7.1 からわかる．HH が H を含むことは $1 \in H$ なので $H = 1H \subset HH$ でわかり，$H^{-1} \subset H$ から $H = (H^{-1})^{-1} \subset H^{-1}$ がわかり，$1 = 1^{-1} \in H^{-1}$ より $H = H1 \subset HH^{-1}$ もわかる．

問 7.3 仮定から (7.1) は成り立つので (7.2) を示せばよい．問 4.1, (iv) により，任意の $a \in H$ について $x \mapsto ax$ は G から G への全単射である．$aH \subset H$ であるから，この写像の H への制限は H への単射となる．H が有限集合なので問 1.1 により全単射となる．$1 \in H$ であるから，ある $a' \in H$ について $aa' = 1$ となる．両辺の左から a^{-1} を掛ければ $a' = a^{-1}$ となり，$a^{-1} \in H$ がわかる．

問 7.4 (i) HK が G の部分群であれば，問 7.2 より $HK = (HK)^{-1}$ となる．H, K も部分群であるから

$$HK = (HK)^{-1} = K^{-1}H^{-1} = KH$$

となる．

次に $HK = KH$ が成り立つとする．このとき

$$(HK)(HK) = H(KH)K = H(HK)K = (HH)(KK) = HK$$

となり (7.1) がいえる．また，$(HK)^{-1} = K^{-1}H^{-1} = KH = HK$ より (7.2) も成り立つ．したがって HK は G の部分群である．

(ii) $H, K \cap L \subset L$ で L は部分群であるから $H(K \cap L) \subset LL = L$ となる．また $K \cap L \subset K$ より $H(K \cap L) \subset HK$ も成り立つ．したがって $H(K \cap L) \subset (HK) \cap L$ となる．

次に，$h \in H$ と $k \in K$ の積 $l = hk$ が L に含まれるとする．$H \subset L$ より h は群 L の元なので $k = h^{-1}l$ は $K \cap L$ に含まれる．したがって $l = hk \in H(K \cap L)$ となる．これで逆の $(HK) \cap L \subset H(K \cap L)$ もわかる．

問 7.6 群の元 a の位数は $a^n = 1$ となる最小の自然数 n のことである．長さ r の巡回置換 $\sigma = (i_1, i_2, \ldots, i_r)$ により $i_1 \mapsto i_2 \mapsto i_3 \mapsto \cdots \mapsto i_r \mapsto i_1$ と置換されるので，i_1 が最初に i_1 に戻るのは σ を r 回行ったときである．他の $i_2, \ldots, i_r$ も同様で，これら以外の文字は不変であるから，σ の位数は r である．

問 7.9 等式

$$(i_1, i_2, \ldots, i_r) = (i_1, i_2)(i_1, i_3)\cdots(i_1, i_r)$$

が成り立つので，この巡回置換は $r-1$ 個の互換の積に書ける．したがって，r が偶数なら奇置換で奇数なら偶置換である．

なお，この教科書では置換の積は一番左の成分から順に置換を行ってそれらを合成したものとして定義される．線形代数の教科書では逆に右から順に置換を行う流儀の書き方が多いので，注意が必要である．この流儀の場合は，上の等式の右辺は互換が逆の順序に表示されている．

問 7.10 $\sigma = (1,2)(3,4)$, $\tau = (1,3)(2,4)$ と置けば $\sigma\tau = \tau\sigma = (1,4)(2,3)$ および $\sigma^2 = \tau^2 = (\sigma\tau)^2 = 1$ が計算ですぐに確かめられる．その他の積は $(\sigma\tau)\sigma = \sigma(\tau\sigma) = \sigma(\sigma\tau) = \tau$, $\tau(\sigma\tau) = (\tau\sigma)\tau = (\sigma\tau)\tau = \sigma$ ですべて可換で積も V に入っている．またすべて同じ元がその逆元となっている．したがって V は G の可換な部分群である．

問 7.11 n についての数学的帰納法で示す．$n = 1, 2$ の場合は明らかである．$n \geqq 3$ として S_{n-1} の場合は主張が正しいとする．

$\sigma \in S_n$ を任意の元とする．$\sigma(n) = n$ とすると，σ は $\{1, 2, \ldots, n-1\}$ の置換と考えられるので，帰納法の仮定により互換 $(1,2), (2,3), \ldots, (n-2, n-1)$ の積に書ける．$i = \sigma(n) < n$ とする．$\tau = \sigma(i, i+1)(i+1, i+2)\cdots(n-1, n)$ と置けば $\tau(n) = n$ となり，τ は帰納法の仮定により互換 $(1,2), (2,3), \ldots, (n-2, n-1)$ の積に書ける．したがって，$\sigma = \tau(n-1, n)(n-2, n-1)\cdots(i, i+1)$ は互換 $(1,2), (2,3), \ldots, (n-1, n)$ の積に書ける．これで S_n の場合も正しいことがわかる．

問 7.13 (i) $A, B \in O(n)$ とすると

$$(AB)\,{}^t(AB) = AB\,{}^tB\,{}^tA = AI\,{}^tA = A\,{}^tA = I$$

および

$${}^t(AB)(AB) = {}^tB\,{}^tAAB = {}^tBIB = {}^tBB = I$$

より $AB \in O(n)$ となる．また ${}^t(A^{-1})A^{-1} = ({}^tA)^{-1}A^{-1} = (A\,{}^tA)^{-1} = I^{-1} = I$ および $A^{-1}\,{}^t(A^{-1}) = A^{-1}({}^tA)^{-1} = ({}^tAA)^{-1} = I^{-1} = I$ より逆行列 A^{-1} も $O(n)$ に含まれる．よって $O(n)$ は $GL(n, \mathbf{R})$ の部分群となる．

(ii) $A, B \in U(n)$ とすると

$$(AB)\,{}^t(\overline{AB}) = AB\,{}^t\overline{B}\,{}^t\overline{A} = AI\,{}^t\overline{A} = A\,{}^t\overline{A} = I$$

および

$${}^t(\overline{AB})(AB) = {}^t\overline{B}\,{}^t\overline{A}AB = {}^t\overline{B}IB = {}^t\overline{B}B = I$$

より $AB \in O(n)$ となる．また ${}^t(\bar{A}^{-1})A^{-1} = ({}^t\bar{A})^{-1}A^{-1} = (A\,{}^t\bar{A})^{-1} = I^{-1} = I$ および $A^{-1}\,{}^t(\bar{A}^{-1}) = A^{-1}({}^t\bar{A})^{-1} = ({}^t\bar{A}A)^{-1} = I^{-1} = I$ より逆行列 A^{-1} も $U(n)$ に含まれる．よって $U(n)$ は $GL(n, \mathbf{C})$ の部分群となる．

問 7.14 $A \in M(n, R)$ が正則であれば $A' \in M(n, R)$ が存在して $AA' = A'A = I$ となる．$\det A \det A' = \det(AA') = \det I = 1$ と $\det A' \det A = \det(A'A) = \det I = 1$ から，$\det A'$ が $\det A$ の逆元となり $\det A$ は正則元である．逆に，$d = \det A$ が正則元で逆元 d^{-1} をもてば，$A' = d^{-1}\tilde{A}$ は $AA' = d^{-1}A\tilde{A} = d^{-1}((\det A)I) = I$ と $A'A = d^{-1}\tilde{A}A = d^{-1}((\det A)I) = I$ を満たし A の逆元である．したがって A は $M(n, \mathbf{R})$ の正則元で，$A^{-1} = (\det A)^{-1}\tilde{A}$ ある．

問 8.1 (i) $Ha = Hb$ であれば $a = 1a \in Hb$ なので，$x \in H$ が存在して $a = xb$ となる．したがって $ab^{-1} = x \in H$ である．逆に $ab^{-1} \in H$ とすると $ba^{-1} = (ab^{-1})^{-1} \in H$ であるから，任意の $h \in H$ について $hb = h(ba^{-1})a \in Ha$ より $Hb \subset Ha$ で，また任意の $h \in H$ について $ha = h(ab^{-1})b \in Hb$ より $Ha \subset Hb$ となり $Ha = Hb$ がわかる．

(ii) $aH = bH$ であれば $b = b1 \in aH$ なので，$x \in H$ が存在して $b = ax$ となる．したがって $a^{-1}b = x \in H$ である．逆に $a^{-1}b \in H$ とすると $b^{-1}a = (a^{-1}b)^{-1} \in H$ であるから，任意の $h \in H$ について $ah = b(b^{-1}a)h \in bH$ より $aH \subset bH$ で，また任意の $h \in H$ について $bh = a(a^{-1}b)h \in aH$ より $bH \subset aH$ となり $aH = bH$ がわかる．

問 8.2 右合同が同値関係であることは，同値性の満たすべき条件が集合の等式 $Ha = Hb$ であることから明らかであるが，一応確認しておく．

反射律：任意の $a \in G$ について集合の等式 $Ha = Ha$ は明らか．

対称律：$Ha = Hb$ とすると，これは集合の等式なので $Hb = Ha$ となる．

推移律：$Ha = Hb$ と $Hb = Hc$ から集合の等式 $Ha = Hc$ が出る．

となり正しい．左合同も同様に

反射律：任意の $a \in G$ について集合の等式 $aH = aH$ は明らか．

対称律：$aH = bH$ とすると，これは集合の等式なので $bH = aH$ となる．

推移律：$aH = bH$ と $bH = cH$ から集合の等式 $aH = cH$ が出る．

となり同値関係である．

問 8.3 a_i $(i \in I)$ はどの 2 つも右合同ではなく，またすべての $a \in G$ はある a_i と右合同となる．a_i^{-1} と a_j^{-1} が左合同とすると $a_i a_j^{-1} = (a_i^{-1})^{-1} a_j^{-1} \in H$ となるので $a_i \equiv_r a_j \pmod{H}$ となり，$a_i = a_j$ しかあり得ない．したがって $a_1^{-1}, \ldots, a_n^{-1}$ はどの 2 つも左合同ではない．また，任意の $x \in G$ について $x^{-1} \in G$ はある a_i と右合同である．つまり $h \in H$ があって $x^{-1} = h a_i$ となる．このとき，$x = a_i^{-1} h^{-1} \in a_i^{-1} H$ となり x は a_i^{-1} と左合同である．よって $\sum_{i \in I} a_i^{-1} H$ は G の左分解である．

問 8.6 σ は奇置換であるから σ^{-1} も奇置換である．$S_n \setminus A_n$ は奇置換全体の集まりであるから，任意の奇置換 τ がある偶置換 $\rho \in A_n$ により $\tau = \rho\sigma$ となることを示せばよい．$\rho = \tau\sigma^{-1}$ とおけば，右辺は 2 つの奇置換の積で偶置換となり条件を満たす．したがって $S_n = A_n + A_n\sigma$ で剰余類の数は 2 である．

問 8.7 群 G の位数が素数 p とする．$p > 1$ であるから，単位元以外の元 $a \in G \setminus \{1\}$ が存在する．a で生成される部分群 $H = (a)$ は位数が 2 以上の巡回群であるが，位数は素数 $p = |G|$ の 1 以外の約数であるから p しかあり得ない．よって $G = (a)$ であり，G は巡回群である．

問 8.8 まず，任意の元 $c \in G$ が部分群 K についてある $b_j a_i$ と右同値であることを見る．$\{a_i\}$ が $H \backslash G$ の完全代表系であるから，ある a_i について $c a_i^{-1} \in H$ となる．また，$\{b_j\}$ は $K \backslash H$ の完全代表系であるから，ある b_j について $(c a_i^{-1}) b_j^{-1} = c(b_j a_i)^{-1} \in K$ となる．これは c が $b_j a_i$ と右同値であることを示す．

あとは，$b_j a_i$ と $b_l a_k$ が K について右同値のとき $i = k$ かつ $j = l$ であることを示せばよい．$K \subset H$ であるから，$b_j a_i$ と $b_l a_k$ は H についても右同値である．$b_j, b_l \in H$ より $b_j a_i$ と a_i および $b_l a_k$ と a_k はそれぞれ H について右同値であるから，a_i と a_k が右同値となり $i = k$ がわかる．$b_j b_l^{-1} = b_j a_i (b_l a_i)^{-1} =$

$b_j a_i (b_l a_k)^{-1} \in K$ より，H の元 b_j と b_l は K について右同値となり，$j = l$ もわかる．

最後の等式は $\{b_j a_i\}$ の元の個数が両辺の元の個数に等しいことからわかる．

問 8.9 反射律：任意の $a \in G$ について $a = 1a1$ であり，1 は H にも K にも含まれるので $a \equiv a \pmod{(H,K)}$ である．

対称律：$a \equiv b \pmod{(H,K)}$ であれば，ある $h \in H$ と $k \in K$ について $b = hak$ であるから，$h^{-1} \in H$ かつ $k^{-1} \in K$ で $a = h^{-1}bk^{-1}$ となり，$b \equiv a \pmod{(H,K)}$ がわかる．

推移律：$a \equiv b \pmod{(H,K)}$ かつ $b \equiv c \pmod{(H,K)}$ であれば，ある $h_1, h_2 \in H$ と $k_1, k_2 \in K$ について $b = h_1 a k_1$ および $c = h_2 b k_2$ となる．このとき，$c = h_2 h_1 a k_1 k_2$ で $h_2 h_1 \in H$ かつ $k_1 k_2 \in K$ であるから，$a \equiv c \pmod{(H,K)}$ となる．

a に同値な元は定義から $hak \in HaK$ の形になり，また HaK の元 hak は a に同値なので，HaK が a を含む同値類である．

問 9.2 $x = a^i$ とすると $x^m = a^{mi}$ であるから $x^m = 1$ となるのは $n | mi$ の場合である．$n = ml$ の仮定より，これは i が l の倍数となることだから，$0 \leqq i < n$ なら $i = 0, l, 2l, \ldots, (m-1)l$ となる．したがって，このような x 全体は $\langle a^l \rangle$ であり，元の個数は m である．

問 9.6 $0 \leqq i < n$ を満たす整数 i について (n,i) は n の約数であるから，$m = n/(n,i)$ も n の約数である．n の各約数 m について

$$A_m = \{i \,;\, 0 \leqq i < n \text{ かつ } m = n/(n,i)\}$$

と置く．$i \in A_m$ について，i は最大公約数 $(n,i) = n/m$ の倍数であるから $j = i/(n/m) = im/n$ は整数で，同じく最大公約数で割った $n/(n/m) = m$ と互いに素である．また，逆に $0 \leqq j < m$ なる j が m と互いに素であれば $i = (n/m)j$ と $n = (n/m)m$ は $(n,i) = n/m$ をみたし i は A_m の元となる．このような j の個数が $\phi(m)$ 個であるから，A_m の元の個数も $\phi(m)$ 個となる．$0 \leqq i < n$ を満たす任意の整数 i について，ある n の約数 m があって $i \in A_m$ となるのだから，すべての n の約数 m について A_m の元の個数 $\phi(m)$ を足し合わせれば $0 \leqq i < n$ を満たす整数の個数である n となる．

問 9.7 p^e の素因子は p だけなので，整数 n が p^e と互いに素なのは n が p を素因子に持たない場合である．$0 \leqq n < p^e$ とすると，n が p の倍数となるのは $0, p, 2p, \ldots, (p^{e-1}-1)p$ の p^{e-1} 個であるから，p で割り切れない n の個数は $p^e - p^{e-1} = p^{e-1}(p-1)$ となる．したがって $\varphi(p^e) = p^{e-1}(p-1)$ となる．

問 9.9 G を $K^\sharp$ の有限部分群とする．例題 9.8 により，任意の自然数 m について $x^m = 1$ となる G の元 x の個数が m 以下であることを示せばよい．$a_1, a_2, \ldots, a_d \in G$ を $x^m = 1$ を満たす相異なる元とする．これは m 次の方程式 $x^m = 1$ が体 K において d 個以上の相異なる解を持つことを示すので，問 6.4 により $d \leqq m$ がわかる．

問 10.1 (i) $1 \in H$ より $1 = t^{-1}1t \in t^{-1}Ht$ だから $t^{-1}Ht \neq \emptyset$ である．$t^{-1}at, t^{-1}bt \in t^{-1}Ht$ に対して $(t^{-1}at)(t^{-1}bt) = t^{-1}(ab)t \in t^{-1}Ht$ であり，また $t^{-1}at \in t^{-1}Ht$ に対して $(t^{-1}at)^{-1} = t^{-1}a^{-1}t \in t^{-1}Ht$ となるので $t^{-1}Ht$ は G の部分群である．

(ii) $b^{-1}ab = a$ であれば両辺の左から b をかけて $ab = ba$ となる．また，$ab = ba$ であれば両辺の左から b^{-1} をかけて $b^{-1}ab = a$ となる．

問 10.3 任意の $a \in G$ について $a^{-1}Na = N$ を示せばよいが，仮定から $a^{-1}Na \subset N$ であるから $N \subset a^{-1}Na$ を示せばよい．$a^{-1} \in G$ より $aNa^{-1} = (a^{-1})^{-1}Na^{-1} \subset N$ であるから，この包含関係の左から a^{-1} をかけて右から a をかけることにより $N = a^{-1}(aNa^{-1})a \subset a^{-1}Na$ となる．

問 10.4 (i) 問 10.3 により，任意の $a \in G$ に対して $a^{-1}Ha \subset H$ を示せばよい．各 i について，$H \subset H_i$ より $a^{-1}Ha \subset a^{-1}H_ia$ であるが，H_i は G の正規部分群であるから $a^{-1}H_ia = H_i$ であり $a^{-1}Ha \subset H_i$ となる．したがって $a^{-1}Ha \subset \bigcap_{i=1}^h H_i = H$ である．(注意) この問題は対応 $x \mapsto a^{-1}xa$ が自己同型という 11 節の項目を習得した後は，単に $a^{-1}Ha = \bigcap_{i=1}^h a^{-1}H_ia = \bigcap_{i=1}^h H_i = H$ と計算してよい．

(ii) (1) 任意の $a \in H$ に対して，N が正規部分群であることから $a^{-1}Na = N$ であり，また a が 部分群 H の元であるから $a^{-1}Ha = H$ となる．よって $a^{-1}(H \cap N)a \subset (a^{-1}Ha) \cap (a^{-1}Na) = H \cap N$ となる．したがって，問 10.3 により $H \cap N$ は H の正規部分群である．

(2) $x \in N$ と $y \in H$ に対して N の正規性から $x' = y^{-1}xy \in N$ であるから，$xy = y(y^{-1}xy) = yx' \in HN$ となる．これで $NH \subset HN$ がわかる．また，$x'' = yxy^{-1} = (y^{-1})^{-1}xy^{-1} \in N$ より $yx = (yxy^{-1})y = x''y \in NH$ だから，$HN \subset NH$ も成り立つ．よって $NH = HN$ である．$(NH)(NH) = NHNH = NNHH = NH$ および $(NH)^{-1} = H^{-1}N^{-1} = HN = NH$ だから NH は G の部分群である．

(3) この場合，任意の $a \in G$ について $a^{-1}NHa = (a^{-1}Na)(a^{-1}Ha) = NH$ で，(2) より NH は部分群であるから，NH は G の正規部分群となる．

問 10.6 この問題には 12 節の例題 12.10 を用いるのが適当である．すなわち，クラインの 4 元群 V は S_4 の 2^2 型の元全体からなる部分群であるから，任意の $a \in S_4$ について $a^{-1}Va$ は例題 12.10 により V に含まれる．したがって V は S_4 の正規部分群である．

問 11.1 (i) $\sigma = (1,2)(3,4)$, $\tau = (1,3)(2,4)$ と置けば $\rho = \sigma\tau = (1,4)(2,3)$ となり $V = \{1, \sigma, \tau, \rho\}$ である．乗積表は

	1	σ	τ	ρ
1	1	σ	τ	ρ
σ	σ	1	ρ	τ
τ	τ	ρ	1	σ
ρ	ρ	τ	σ	1

となる．

(ii) $1 = (1,1)$, $\sigma' = (1,-1)$, $\tau' = (-1,1)$, $\rho' = (-1,-1)$ とすると乗積表は

	1	σ'	τ'	ρ'
1	1	σ'	τ'	ρ'
σ'	σ'	1	ρ'	τ'
τ'	τ'	ρ'	1	σ'
ρ'	ρ'	τ'	σ'	1

となる．$1 \mapsto 1$, $\sigma \mapsto \sigma'$, $\tau \mapsto \tau'$, $\rho \mapsto \rho'$ と対応させると群の同型が得られる．

問 11.3 (i) 準同型だから $f(1) = 1$ となり，$1 \in \mathrm{Ker}\, f$ である．f が単射であれば $f(x) = 1$ となる x は 1 以外にないので $\mathrm{Ker}\, f = \{1\}$ である．次に，$\mathrm{Ker}\, f = \{1\}$ であるとする．$f(x) = f(y)$ なら $f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} = 1$ と

なるので，$xy^{-1} \in \mathrm{Ker}\, f$ であり $xy^{-1} = 1$ となる．右から y をかけて $x = y$ となるので f は単射である．

(ii) H は空でないので $f(H)$ も空でない．$f(H)f(H) = f(HH) = f(H)$ および $f(H)^{-1} = f(H^{-1}) = f(H)$ より $f(H)$ は G' の部分群である．H の元 a, b について，$f_H(ab) = f(ab) = f(a)f(b) = f_H(a)f_H(b)$ より f_H は準同型である．また，$\mathrm{Ker}\, f_H = \{x \in H\ ;\ f_H(x) = 1\} = \{x \in H\ ;\ f(x) = 1\} = H \cap \mathrm{Ker}\, f$ となる．

(iii) $H \subset G$ より $f(H) \subset f(G)$ であり，(ii) よりこれらは G' の部分群である．任意の $x' = f(x) \in f(G)$ について $x'^{-1}f(H)x' = f(x)^{-1}f(H)f(x) = f(x^{-1}Hx) = f(H)$ であるから $f(H)$ は $f(G)$ の正規部分群である．

(iv) $x, y \in f^{-1}(H')$ であれば $f(x), f(y) \in H'$ であるから $f(xy) = f(x)f(y) \in H'$ であり $xy \in f^{-1}(H')$ がわかる．また，$x \in f^{-1}(H')$ であれば $f(x^{-1}) = f(x)^{-1} \in H'$ であるから $f^{-1}(H')$ は G の部分群である．また，H' が G' の正規部分群であれば，任意の $x \in G$ と $y \in f^{-1}(H')$ について $f(x^{-1}yx) = f(x)^{-1}yf(x) \in H'$ となり，$x^{-1}yx \in f^{-1}(H')$ となるので，$f^{-1}(H')$ は G の正規部分群となる．

問 11.5 (i) $\overline{G}$ の単位元は $1 \in G$ の含まれる同値類 N であり，$f(x) = 1$ は x がこの同値類の元であることを意味するので $\mathrm{Ker}\, f = N$ である．

(ii) 書かれていないが $\overline{H} = f(H)$ である．$x \in N$ と $y \in H$ に対して $f(xy) = Ny = f(y) \in \overline{H}$ であるから $xy \in f^{-1}(\overline{H})$ となる．よって $NH \subset f^{-1}(\overline{H})$ である．また，$z \in f^{-1}(\overline{H})$ であれば，ある $y \in H$ について $Nz = Ny$ すなわち $z \in Ny$ であり，$Ny \subset NH$ より $f^{-1}(\overline{H}) \subset NH$ もわかる．

問 11.9 $f(m+n) = a^{m+n}$ で $f(m)f(n) = a^m a^n$ であるから，準同型性は指数法則 $a^{m+n} = a^m a^n$ から従う．全射性は a で生成される巡回群の定義が $\{a^n\ ;\ n \in \mathbf{Z}\}$ であることからでる．無限巡回群なら例題 7.5 (ii) より単射で $\mathrm{Ker}\, f = \{0\}$ となる．位数 n なら例題 7.5 (i) より $a^m = 1 \Leftrightarrow n|m$ であるから $\mathrm{Ker}\, f = n\mathbf{Z}$ となる．このとき，準同型定理により $\mathbf{Z}/n\mathbf{Z} \simeq \langle a \rangle$ である．

問 11.13 $(xy)^{\iota(a)} = a^{-1}xya = (a^{-1}xa)(a^{-1}ya) = x^{\iota(a)}y^{\iota(a)}$ であるから準同型である．$(x^{\iota(a)})^{\iota(a^{-1})} = a(a^{-1}xa)a^{-1} = x$ および $(x^{\iota(a^{-1})})^{\iota(a)} = a^{-1}(axa^{-1})a = x$ より $\iota(a^{-1})$ が $\iota(a)$ の逆写像となっており，$\iota(a)$ は同型である．

問 11.14 (i) 任意の $x \in G$ について $x^{\iota(ab)} = (ab)^{-1}x(ab) = b^{-1}(a^{-1}xa)b = (x^{\iota(a)})^{\iota(b)} = x^{\iota(a)\iota(b)}$ となり，$\iota(ab) = \iota(a)\iota(b)$ がわかる．また，問 11.13 の解で見たように $\iota(a^{-1})$ は $\iota(a)$ の逆写像だから，$\iota(a^{-1}) = \iota(a)^{-1}$ である．

(ii) $x^{\sigma^{-1}\iota(a)\sigma} = (x^{\sigma^{-1}})^{\iota(a)\sigma} = (a^{-1}(x^{\sigma^{-1}})a)^{\sigma} = (a^{\sigma})^{-1}(x^{\sigma^{-1}})^{\sigma}a^{\sigma} = (a^{\sigma})^{-1}xa^{\sigma} = x^{\iota(a^{\sigma})}$ が任意の $x \in G$ について 成り立つので，$\sigma^{-1}\iota(a)\sigma = \iota(a^{\sigma})$ である．

問 11.15 ι は問 11.14 (i) により準同型で $\operatorname{Inn} G = \{\iota(a)\ ;\ a \in G\}$ であるから全射である．$a \in \operatorname{Ker}\iota \Leftrightarrow x^{\iota(a)} = x, \forall x \in G$ であるから，これは $xa = ax, \forall x \in G$ すなわち $a \in Z(G)$ と同値となる．準同型定理により $G/Z(G) \simeq \operatorname{Inn} G$ となる．

問 12.1 反射律：$\alpha \in X$ に対して $1 \in G$ をとれば $\alpha = \alpha^1$ となる．よって $\alpha \underset{G}{\sim} \alpha$ である．対称律：$\alpha \underset{G}{\sim} \beta$ とすると，ある $g \in G$ について $\beta = \alpha^g$ となる．このとき $\beta^{g^{-1}} = (\alpha^g)^{g^{-1}} = \alpha^{gg^{-1}} = \alpha^1 = \alpha$ となるので $\beta \underset{G}{\sim} \alpha$ である．推移律：$\alpha \underset{G}{\sim} \beta$ かつ $\beta \underset{G}{\sim} \gamma$ とする．このとき $g, h \in G$ が存在して $\beta = \alpha^g$ かつ $\gamma = \beta^h$ となる．$\gamma = \beta^h = (\alpha^g)^h = \alpha^{gh}$ であるから $\alpha \underset{G}{\sim} \gamma$ となる．

問 12.2 $\alpha = \alpha^1$ であるから $1 \in G_\alpha$ であり G_α は空でない．$g, h \in G_\alpha$ に対して $\alpha^{gh} = (\alpha^g)^h = \alpha^h = \alpha$ より $gh \in G_\alpha$ がわかる．また，$g \in G_\alpha$ に対して $\alpha^{g^{-1}} = (\alpha^g)^{g^{-1}} = \alpha^{gg^{-1}} = \alpha^1 = \alpha$ より $g^{-1} \in G_\alpha$ もわかる．よって G_α は G の部分群である．

問 12.3 $\beta = \alpha^a$ より $\beta^{a^{-1}} = (\alpha^a)^{a^{-1}} = \alpha^{aa^{-1}} = \alpha^1 = \alpha$ となる．任意の $a^{-1}ga \in a^{-1}G_\alpha a$ を考える．$\beta^{a^{-1}ga \in a^{-1}} = (\beta^{a^{-1}})^{ga} = \alpha^{ga} = (\alpha^g)^a$ であるが，$g \in G_\alpha$ だから，これは $\alpha^a = \beta$ に等しい．したがって $a^{-1}ga \in G_\beta$ であり，$a^{-1}G_\alpha a \subset G_\beta$ がわかる．また，任意の元 $g \in G_\beta$ は $\beta^g = \beta$ を満たすので，$h = aga^{-1}$ とおくと $\alpha^h = \alpha^{aga^{-1}} = (\beta^g)^{a^{-1}} = \beta^{a^{-1}} = \alpha$ となり $h \in G_\alpha$ がわかる．したがって，$g = a^{-1}ha \in a^{-1}G_\alpha a$ となる．これで $G_\beta \subset a^{-1}G_\alpha a$ もわかる．

問 12.5 (i) $\sigma(a^{-1})$ が $\sigma(a)$ の逆写像であることを示せばよい．任意の $x \in X$ について，$\sigma(a^{-1})(\sigma(a)(x)) = \sigma(a^{-1})(x^a) = (x^a)^{a^{-1}} = x^{aa^{-1}} = x^1 = x$ および $\sigma(a)(\sigma(a^{-1})(x)) = \sigma(a)(x^{a^{-1}}) = (x^{a^{-1}})^a = x^{a^{-1}a} = x^1 = x$ より $\sigma(a^{-1})$ が $\sigma(a)$ の逆写像であることがわかる．

(ii) $g, h \in G$ に対して $\sigma(gh) = \sigma(g)\sigma(h)$ を示せばよい．任意の $x \in X$ について，$\sigma(gh)(x) = x^{gh}$ であり，また $\sigma(g)\sigma(h)$ が写像の合成 $\sigma(h)\cdot\sigma(g)$ であるこ

とに注意して $(\sigma(g)\sigma(h))(x) = (\sigma(h)\cdot\sigma(g))(x) = \sigma(h)(\sigma(g)(x)) = \sigma(h)(x^g) = (x^g)^h = x^{gh}$ であるから，求める等式が得られる．

問 12.6 (i) $H\backslash G$ の任意の元 Hx について $(Hx)^1 = Hx1 = Hx$ であるから，(12.1) の条件は満たされる．また，$((Hx)^a)^b = (Hxa)^b = Hxab = (Hx)^{ab}$ であるから (12.2) も満たす．よって，これは群 G の作用である．任意の $Hx, Hy \in H\backslash G$ に対して，$a = x^{-1}y$ とおけば $(Hx)^a = Hxa = Hy$ であるから，この作用は可移である．$(Hx)^a = Hx$ とすると $Hxa = Hx$ より $xa \in Hx$ で $a \in x^{-1}Hx$ となる．すべての $Hx \in H\backslash G$ について $(Hx)^a = Hx$ となる元 a が $\mathrm{Ker}(H\backslash G, G)$ の元であるから $\mathrm{Ker}(H\backslash G, G) = \bigcap_{x\in G} x^{-1}Hx$ となる．

(ii) 等式 $\mathrm{Ker}(H\backslash G, G) = \bigcap_{x\in G} x^{-1}Hx$ より，$\bigcap_{x\in G} x^{-1}Hx$ は G の正規部分群である．N が H に含まれる正規部分群とすると，任意の $x \in G$ について $N = x^{-1}Nx \subset x^{-1}Hx$ となり $N \subset \bigcap_{x\in G} x^{-1}Hx$ となるので，$\bigcap_{x\in G} x^{-1}Hx$ は H に含まれる最大の正規部分群である．

問 13.6 σ を G の任意の自己同型とする．P^σ の元の個数は P の元の個数に等しいので，P^σ も G のシロー部分群となる．シロー部分群はすべて共役なので，ある $t \in G$ について $P^\sigma = t^{-1}Pt$ となるが，P が正規部分群であるから $P^\sigma = P$ となる．したがって P は G の特性部分群である．

問 14.1 任意の $a_i \in G_i$ と $a_j \in G_j$ について $a_i^* a_j^*$ と $a_j^* a_i^*$ は共に第 i 成分が a_i で第 j 成分が a_j であり，その他の成分は 1 となる．したがって $a_i^* a_j^* = a_j^* a_i^*$ がわかり，G_i^* の元と G_j^* の元は可換である．G の元 a の成分が左から $a_1, a_2, \ldots, a_n$ とすると，定義から $a = a_1^* a_2^* \cdots a_n^*$ となる．また，$i = 1, 2, \ldots, n$ について $b_i \in G_i$ をとって $b = b_1^* b_2^* \cdots b_n^*$ と定義すれば b の第 i 成分は b_i であるから，$b = a$ となるためにはすべての i について $b_i = a_i$ でなければならない．したがって，a を与える $a_1, a_2, \ldots, a_n$ の取り方は一意的である．

問 14.4 (i) $[a, b] = a^{-1}b^{-1}ab$ であるから，$[a, b] = 1$ であれば $a^{-1}b^{-1}ab = 1$ であり，両辺の左から ba をかければ $ab = ba$ を得る．逆に $ab = ba$ であれば，両辺の左から $a^{-1}b^{-1}$ をかけて $a^{-1}b^{-1}ab = 1$ となり $[a, b] = 1$ がわかる．

(ii) $a \in A$ で A は正規部分群であるから $b^{-1}ab \in A$ である．これから $[a, b] = a^{-1}b^{-1}ab = a^{-1}(b^{-1}ab) \in A$ がわかる．また，$b^{-1} \in B$ で B は正規部分群であるから $a^{-1}b^{-1}a \in B$ である．これから $[a, b] = a^{-1}b^{-1}ab = (a^{-1}b^{-1}a)b \in B$ も

わかる．したがって $[a,b] \in A \cap B$ である．もし $A \cap B = \{1\}$ であればどのような $a \in A$ と $b \in B$ に対しても $[a,b] = 1$ しかあり得ないので，(i) より A の元と B の元は可換である．

問 14.6 A は正規部分群であるから問 10.4, (ii) より AB は G の部分群である．また A と B は AB の正規部分群でもあるので，定理 14.5 により $A \cap B = \{1\}$ を示せば $AB = A \times B$ がわかる．$A \cap B$ は A と B の部分群であるから，その位数は $|A|$ と $|B|$ の約数である．ところが $(|A|, |B|) = 1$ の仮定から $A \cap B$ の位数は 1 であり，$A \cap B = \{1\}$ がわかる．

問 14.7 (i) $x = x_1 x_2 \cdots x_n \in G, x_i \in H_i$ $(i = 1, \ldots, n)$ が $Z(G)$ の元であれば，任意の i と $y_i \in H_i$ について $xy_i = y_i x$ であるが，xy_i の第 i 成分は $x_i y_i$ で $y_i x$ の第 i 成分は $y_i x_i$ であるから $x_i y_i = y_i x_i$ となり，$x_i \in Z(H_i)$ であることがわかる．逆に，$x = x_1 x_2 \cdots x_n$ がすべての i について $x_i \in Z(H_i)$ であれば，任意の $y = y_1 y_2 \cdots y_n \in G, y_i \in H_i$ $(i = 1, \ldots, n)$ について，

$$xy = (x_1 y_1) \cdots (x_n y_n) = (y_1 x_1) \cdots (y_n x_n) = yx$$

となり，$x \in Z(G)$ であることがわかる．

(ii) 任意の $y_i \in K$ と任意の $x = x_1 x_2 \cdots x_n \in G, x_i \in H_i$ $(i = 1, \ldots, n)$ について，$x^{-1} y_i x$ の第 j 成分は $j \neq i$ であれば $x_j^{-1} x_j = 1$ で，第 i 成分は $x_i^{-1} y_i x_i$ である．K が H_i の正規部分群であるから $x^{-1} y_i x = x_i^{-1} y_i x_i \in K$ であり，K は G の正規部分群である．

(iii) $x = x_1 x_2 \cdots x_n \in G, x_i \in H_i$ $(i = 1, \ldots, n)$ と $y = y_1 y_2 \cdots y_n \in G, y_i \in H_i$ $(i = 1, \ldots, n)$ の積は $xy = (x_1 y_1) \cdots (x_n y_n)$ である．したがって，$\varepsilon_i(xy) = x_i y_i = \varepsilon_i(x)\varepsilon_i(y)$ となる．これで ε_i が準同型であることがわかる．$\varepsilon_i(x) = 1$ となるのは $x_i = 1$ が必要十分であるから，

$$\operatorname{Ker} \varepsilon_i = H_1 \times \cdots \times H_{i-1} \times H_{i+1} \times \cdots \times H_n$$

となる．ε_i は明らかに全射であるから準同型定理により最後の同型が得られる．

問 15.5 $\lambda\mu$ が準同型であることを見る．$\mathbf{C}^\sharp$ が可換群であることを使って，$(\lambda\mu)(ab) = \lambda(ab)\mu(ab) = \lambda(a)\lambda(b)\mu(a)\mu(b) = \lambda(a)\mu(a)\lambda(b)\mu(b) = (\lambda\mu)(a)(\lambda\mu)(b)$ となり $\lambda\mu$ が準同型すなわち指標であることがわかる．$\lambda, \mu, \nu \in \hat{A}$ とすれば，

任意の $a \in A$ に対して $((\lambda\mu)\nu)(a) = (\lambda\mu)(a)\nu(a) = \lambda(a)\mu(a)\nu(a)$ および $(\lambda(\mu\nu))(a) = \lambda(a)(\mu\nu)(a) = \lambda(a)\mu(a)\nu(a)$ より $(\lambda\mu)\nu = \lambda(\mu\nu)$ がわかる．また，$(\lambda\mu)(a) = \lambda(a)\mu(a) = \mu(a)\lambda(a) = (\mu\lambda)(a)$ より，可換性 $\lambda\mu = \mu\lambda$ もわかる．$(1_A\lambda)(a) = 1_A(a)\lambda(a) = 1\lambda(a) = \lambda(a)$ より 1_A が指標の積について単位元となる．指標 λ の逆元 λ^{-1} は，$\lambda^{-1}(a) = \lambda(a)^{-1}$ で定義すればよい．実際，$\lambda^{-1}(ab) = \lambda(ab)^{-1} = \lambda(a)^{-1}\lambda(b)^{-1} = \lambda^{-1}(a)\lambda^{-1}(b)$ となり λ^{-1} は指標であり，$(\lambda\lambda^{-1})(a) = \lambda(a)\lambda^{-1}(a) = \lambda(a)\lambda(a)^{-1} = 1$ より $\lambda\lambda^{-1} = 1_A$ もわかる．したがって $\hat{A}$ は可換群となる．

問 15.7 任意の $c \neq 1$ に対して $\lambda(c) \neq 1$ となる λ が存在することを示せば，$c = ab^{-1}$ と置いて $\lambda(ab^{-1}) \neq 1$ より $\lambda(a) \neq \lambda(b)$ となる．$A = \langle a_1\rangle \times \cdots \times \langle a_r\rangle$ とする．$c \neq 1$ の仮定から，ある i について c の $\langle a_i\rangle$ での成分が 1 でない．$o(a_i) = m$ として，A から第 i 成分への射影と $\langle a_i\rangle$ から $\mathbf{C}^\sharp$ への $a_i^j \mapsto \zeta^j$ で定義される準同型との合成を λ とする．ここで ζ は 1 の原始 m 乗根とする．このとき $\lambda \in \hat{A}$ で $\lambda(c) \neq 1$ となる．

問 15.8 $a^*(\lambda\mu) = (\lambda\mu)(a) = \lambda(a)\mu(a) = a^*(\lambda)a^*(\mu)$ であるから a^* は準同型，すなわち $\hat{A}$ の指標である．

$$(ab)^*(\lambda) = \lambda(ab) = \lambda(a)\lambda(b) = a^*(\lambda)b^*(\lambda) = (a^*b^*)(\lambda)$$

より対応 $a \mapsto a^*$ は A から $\hat{\hat{A}}$ への準同型であることがわかる．$a \neq 1$ であれば，問 15.7 よりある $\lambda \in \hat{A}$ について $a^*(\lambda) = \lambda(a) \neq 1$ であるから，$a^* \neq 1$ であり，この対応は単射である．定理 15.6 により $A \simeq \hat{A} \simeq \hat{\hat{A}}$ だから，A と $\hat{\hat{A}}$ の元の個数は等しく，単射性から対応 $a \mapsto a^*$ が A から $\hat{\hat{A}}$ への同型であることがわかる．

問 15.14 (i) $a \in A$ の $A/T(A)$ への像 $\bar{a}$ の位数が有限とする．このとき，ある正の整数 m について $\bar{a}^m = \overline{a^m} = 1$ となる．したがって $a^m \in T(A)$ であり，ある正の整数 n について $(a^m)^n = 1$ となる．$a^{mn} = (a^m)^n = 1$ であるから，$a \in T(A)$ であり $\bar{a} = 1$ がわかる．したがって $A/T(A)$ はトーションのないアーベル群である．

(ii) $A = \langle a_1, a_2, \ldots, a_n\rangle$ として，A の部分群 $A_i = \langle a_1, a_2, \ldots, a_i\rangle$ が有限アーベル群であることを i に関する数学的帰納法で証明する．すべてアーベル群で

あることは A がアーベル群であることからわかる．$i = 0$ なら $\langle\emptyset\rangle = \{1\}$ であるから有限群である．

$i > 0$ として A_{i-1} が有限群と仮定する．このとき，剰余群 A_i/A_{i-1} は a_i の像で生成される巡回群である．$A = T(A)$ の仮定から a_i の位数は有限であるから，その像である巡回群の位数も有限となる．有限正規部分群 $A_{i-1} \subset A_i$ による剰余群が有限群なので，等式 $|A_i| = |A_i : A_{i-1}||A_{i-1}|$ より A_i も有限である．したがって，数学的帰納法によりすべての A_i は有限アーベル群である．特に $A = A_n$ も有限アーベル群である．

問 16.1 (i) $[x, y] = x^{-1}y^{-1}xy$ だから

$$[x, y]^{-1} = (x^{-1}y^{-1}xy)^{-1} = y^{-1}x^{-1}yx = [y, x]$$

となる．

(ii)

$$yx[x, y] = yx(x^{-1}y^{-1}xy) = xy$$

で正しい．

(ii)

$$x[x, y] = x(x^{-1}y^{-1}xy) = y^{-1}xy$$

で正しい．

(iv)

$$[x, y]^z = z^{-1}(x^{-1}y^{-1}xy)z = (z^{-1}x^{-1}z)(z^{-1}y^{-1}z)(z^{-1}xz)(z^{-1}yz)$$

$$= (z^{-1}xz)^{-1}(z^{-1}yz)^{-1}(z^{-1}xz)(z^{-1}yz) = [x^z, y^z]$$

で正しい．

(v)

$$[x, z]^y[y, z] = (y^{-1}(x^{-1}z^{-1}xz)y)(y^{-1}z^{-1}yz) = (xy)^{-1}z^{-1}xyz = [xy, z]$$

および

$$[x, z][x, y]^z = (x^{-1}z^{-1}xz)(z^{-1}(x^{-1}y^{-1}xy)z) = x^{-1}(yz)^{-1}xyz = [x, yz]$$

で正しい．

問 16.4 $n > i$ について $D_n(G) = D_i(G)$ であることを数学的帰納法で示す．$n = i+1$ の場合は条件から正しい．$n > i+1$ として $D_{n-1}(G) = D_i(G)$ を仮定する．このとき

$$D_n(G) = [D_{n-1}(G), D_{n-1}(G)] = [D_i(G), D_i(G)] = D_{i+1}(G) = D_i(G)$$

で n でも正しい．

問 16.9 G は単純群であるから正規部分群は G と $\{1\}$ だけである．したがって $G \supset \{1\}$ が可解群であることを示す正規列となり $G = G/\{1\}$ はアーベル群である．0 でない元 $a \in G$ をとれば巡回群 $\langle a \rangle$ は G の正規部分群なので $G = \langle a \rangle$ である．a の位数が合成数であれば，約数が位数の G でも $\{1\}$ でもない部分群を持つので G が単純群であることに反する．したがって G は素数位数の巡回群である．

問 16.12 (i) H をべき零群 G の部分群とする．このとき $H = \Gamma_0(H) \subset G = \Gamma_0(G)$ であるが，$i > 0$ について $\Gamma_i(H) = [\Gamma_{i-1}(H), H]$ および $\Gamma_i(G) = [\Gamma_{i-1}(G), G]$ であるから，数学的帰納法で $\Gamma_i(H) \subset \Gamma_i(G)$ であることがわかる．G はべき零群であるからある n について $\Gamma_n(G) = \{1\}$ となるので，これに含まれる $\Gamma_n(H)$ も $\{1\}$ となる．したがって H はべき零である．

N をべき零群 G の正規部分群とする．自然な全射準同型 $\phi : G \to G/N$ については $\phi([x, y]) = [\phi(x), \phi(y)]$ であることと，任意の部分集合 $S \subset G$ について $\phi(\langle S \rangle) = \langle \phi(S) \rangle$ であることを使えば任意の部分群 H について $\phi([H, G]) = [\phi(H), G/N]$ であることがわかる．$\Gamma_i(G) = [\Gamma_{i-1}(G), G]$ および $\Gamma_i(G/N) = [\Gamma_{i-1}(G/N), G/N]$ であるから，任意の $i \geqq 0$ について $\phi(\Gamma_i(G)) = \Gamma_i(G/N)$ であることが数学的帰納法で示される．特に $\Gamma_n(G) = \{1\}$ であれば $\Gamma_n(G/N) = \{1\}$ であり，G/N はべき零である．

(ii) $\Gamma_i(G) = \Gamma_i(G_1) \times \cdots \times \Gamma_i(G_r)$ を使えば，ある i で右辺が $\{1\}$ となるので G がべき零であることがわかる．$G = G_1 \times G_2$ の場合にこの等式を確認しておこう．$H_1 \subset G_1$, $H_2 \subset G_2$ をそれぞれ部分群とする．$x_1 \in H_1$, $x_2 \in H_2$, $y_1 \in G_1$, $y_2 \in G_2$ について G_1 の元と G_2 の元は可換であるから $[x_1x_2, y_1y_2] = [x_1, y_1][x_2, y_2] \in [H_1, G_1] \times [H_2, G_2]$ となる．したがって $[H_1 \times H_2, G_1 \times G_2] \subset [H_1, G_1] \times [H_2, G_2]$ がわかる．右辺の直積因子は左辺に含まれるので，逆の包

含関係も成り立ち等しい．2 つの直積の場合を $G_1 \times G_2 \times G_3 = (G_1 \times G_2) \times G_3$ のように繰り返し使えば一般の r 個の直積の場合もわかる．

問 17.2 (i) $G = H_0 \supset H_1 \supset \cdots \supset H_r = \{1\}$ を組成列とする．$i = 1, \ldots, r$ について H_{i-1}/H_i を見る．可解性から交換子群列 $G = D_0(G) \supset D_1(G) \supset \cdots$ は有限個目で $\{1\}$ となるので，ある $j > 0$ について

$$H_{i-1} \subset H_i D_{j-1}(G)) \text{ かつ } H_{i-1} \not\subset H_i D_j(G)$$

となる．$H_i \subset H_i D_j(G)$ であるから準同型 $H_{i-1}/H_i \to H_i D_{j-1}(G))/H_i D_j(G)$ が存在するが，H_{i-1}/H_i は単純群で像は $\{1\}$ でないので単射準同型である．一方，アーベル群からの全射準同型 $D_{j-1}(G))/D_j(G) \to H_i D_{j-1}(G))/H_i D_j(G)$ が存在するので $H_i D_{j-1}(G))/H_i D_j(G)$ はアーベル群である．したがって H_{i-1}/H_i アーベル単純群となり，素数位数の巡回群である．

(ii) 有限群が組成列を持つことは数学的帰納法で示される．実際，$G = \{1\}$ であれば明らかで，$G \neq \{1\}$ とすれば極大な正規部分群 N をとり，帰納法の仮定から N が組成列を持つことと G/N が単純群となることから組成列が得られる．

非可換無限単純群は存在するので，逆は可解群の仮定が必要である．アーベル単純群は素数位数の巡回群であるから，可解群に組成列 $G = H_0 \supset H_1 \supset \cdots \supset H_r = \{1\}$ が存在すれば，G の位数 $|H_0/H_1| \times \cdots \times |H_{r-1}/H_r|$ は有限である．

問 17.6 これはジョルダン・ヘルダーの定理の証明で (K') を組成列と仮定せず単に正規列とすればよい．細分して長さ r の組成列が得られる．

問 17.7 G が組成列を持てば $G \supset N \supset \{1\}$ に細分定理を用いて組成列に細分できる．これは G/N と N の組成列を与えている．逆に G/N と N に組成列があれば，G/N の 組成列を $G \supset N$ の細分に持ち上げることにより，$G \supset N \supset \{1\}$ の細分として G の組成列が得られる．