基本定理 [1]．n 次対称群 $(S_n, \circ)$ は位数 $n!$ の群 (有限群) である．(← p.16 参照)

復習部分．次の 3 つの命題は $G = S_n$ の場合に証明した．しかし，その証明に使った事実は正に $(S_n, \circ)$ が (G1),(G2),(G3) を満たすということである．よって，一般の群 $(G, \circ)$ に対しても (G1),(G2),(G3) を用いて全く同様に証明することができる (← 各自納得できるまで考えること！)：(← p.16 参照)

命題 [2] (単位元，逆元の一意性)．G を群とする．
(1) (G2) を満たす単位元 $e \in G$ は一意的に定まる (唯 1 つである)
(2) $a \in G$ に対して，(G3) を満たす $a' = a^{-1}$ は一意的に定まる (unique である)．

命題 [3]．有限群 $G = \{a_1, \ldots, a_n\}$ とその元 $a_i \in G$ に対して，$a_iG := \{a_ia_1, \ldots, a_ia_n\}$, $Ga_i := \{a_1a_i, \ldots, a_na_i\}$ とする．このとき，$G = a_iG = Ga_i$ が成り立つ．

命題 [4]．有限群 $G = \{a_1, \ldots, a_n\}$ の演算表 (群表) の各行 (列) には，G の全ての元が (1 回) 現れる．

• $(G, \circ)$ が群ではないが，群に近い性質を持つ場合には次のように呼ぶ (← **半**人前の**群**=**半群**？)

定義 (半群，単位的半群=モノイド)．$(G, \circ)$ が (G1) を満たすとき，**半群**という．さらに，$(G, \circ)$ が (G1) かつ (G2) を満たすとき，**単位的半群**または**モノイド**という．

例 (半群，単位的半群)．
(1) $X = \{1, a, b, c\}$ に対して，積 $\circ$ を以下の演算表で定めれば，$(X, \circ)$ は半群となる．
(2) $\mathbb{N}$ に対して，$(\mathbb{N}, \cdot)$ は単位的半群であり，単位元は 1 である．
(3) $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$ に対して，$(\mathbb{N}_0, +)$ は単位的半群であり，単位元 (ゼロ元) は 0 である．

(1)

$\circ$	1	a	b	c
1	a	a	a	a
a	a	a	a	a
b	a	a	a	a
c	a	a	a	a

(2)

$\cdot$	1	2	3	$\cdots$
1	1	2	3	$\cdots$
2	2	4	6	$\cdots$
3	3	6	9	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

(3)

$+$	0	1	2	$\cdots$
0	0	1	2	$\cdots$
1	1	2	3	$\cdots$
2	2	3	4	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

• 半群 $(X, \circ)$ の演算表は上の (1) の様にきれいになることもあるが，これは数学的に「美しい」というよりは「構造がない」ように見える．有限**群** G の様に，各行各列に G の元が一回づつ現れるのは，(G1),(G2),(G3) の 3 つの条件がそろって初めて起こることがよく分かる．

• 代数における 3 つの重要な概念**「群・環・体」**が何であるかを，やっと述べることができる．

定義 (環，体)．(1) 集合 R に 2 つの演算，加法 $(+)$ と乗法 $(\cdot)$ が定義されていて，
以下の条件を満たすとき $(R, +, \cdot)$ を**環** (ring) という (← 単に環 R とかく)：
(R1) $(R, +)$ は加法群, (← この中に (G1),(G2),(G3) が入っている事に注意)
(R2) $(R, \cdot)$ は単位的半群, (← この中に (G1),(G2) が入っている事に注意)
(R3) 加法 $(+)$ と乗法 $(\cdot)$ は分配法則を満たす：

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (a + b) \cdot c = a \cdot c + b \cdot c, \quad (\forall a, b, c \in R).$$

(2) 環 R の 0 (=加法に対する単位元) 以外の元 $\forall x \in R \backslash \{0\}$ に (乗法に関する) 逆元 $x^{-1} \in R$ が存在するとき，R を**体** (field) という．すなわち，$R \backslash \{0\}$ が乗法群をなすとき，R を**体**という．

例 (群)[再掲]．群の例：$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q}^\times, \cdot)$, $(\mathbb{R}^\times, \cdot)$, $(\mathbb{C}^\times, \cdot)$, $(S_n, \circ)$.
但し，$\mathbb{Q}^\times := \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^\times := \mathbb{R} \setminus \{0\}$, $\mathbb{C}^\times := \mathbb{C} \setminus \{0\}$ (← $\{0\}$ を除いた集合 (差集合)) とする．

例 (環，体)．
(1) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ は体である．$\mathbb{Q}$ を**有理数体**，$\mathbb{R}$ を**実数体**，$\mathbb{C}$ を**複素数体**という．
(2) $(\mathbb{Z}, +, \cdot)$ は環であるが，体ではない (← $n \in \mathbb{Z} \backslash \{0\}$ の逆元 $\frac{1}{n} \notin \mathbb{Z}$)．$\mathbb{Z}$ を**整数環**という．
(3) $(\mathbb{N}, +)$ は群ではない (← 単位元 $0 \notin \mathbb{N}$, $n \in \mathbb{N}$ の逆元 $-n \notin \mathbb{N}$) $(\mathbb{N}, +, \cdot)$ は**環でも体でもない**.

なぜ体 $(K,+,\cdot)$ を考えるのか． 代数学の 1 つの目的は (連立) 方程式の解を求めることである．実際，線形代数では連立一次方程式の解法を学ぶ (← 線形代数=linear algebra=1 次式の代数)．線形代数は $\mathbb{R}$ や $\mathbb{C}$ 上だけでなく，一般の体 K 上において理論を展開できる (← 体 K には四則演算があり，分配法則もある)．一方で，$a \in K$ に対して，加法 $+$ に対する逆元 $-a$，乗法 $\cdot$ に対する逆元 a^{-1} がない集合 K 上では，$ax+b=0$ の解 $x=-b/a$ を考えることは出来ない．(← 両辺に $-b$ を足して $ax=-b$ とし，両辺に左から a^{-1} をかけて $x=a^{-1}(-b)$，交換法則で $x=-b/a$ とすることは，加法及び乗法の逆元がない世界では出来ないことである！)

定義 (準同型写像)． 群 $(G,\circ)$ から群 $(G',*)$ への写像 $f : G \to G'$ が

$$\forall a,b \in G \text{ に対し，} f(a\circ b) = f(a) * f(b)$$

を満たすとき，f を G から G' への**準同型写像**という．

定義 (群の同型)[無限群も含んだ一般の場合]． 群 G から群 G' への全単射である準同型写像が存在するとき，G **と** G' **は同型**といい，$G \cong G'$ と書く．また全単射な準同型写像を**同型写像**という．

注意 (群表による同型との関係)． 群 G と群 G' が同型であるとは，1 対 1 対応があり，かつ二項演算 (積) の構造が同じという事である．特に，有限群 G に対しては，群表による同型の定義と準同型写像による同型の定義は同じ概念である．

• しかし，いきなり 2 つの演算を兼ね備えた体 $(K,+,\cdot)$ を考えるのは難しい．そこで，1 つの演算加法 $(+)$ または乗法 $(\cdot)$ に着目し，**群 $(G,\circ)$ の研究を行う**．(← 来年度の後期の内容！)

以下では**群** (group) を G で表し，群論でどのような事を学ぶのかを見てみる．
(← ちなみに，**環** (ring) は R，**体** (field) は K と表すことが多い (体はドイツ語で **K**örper))

• 群論を学ぶには，まず**どのような群が存在するのか**，その具体例をたくさん知ることが重要である．さらには，与えられた群 G がどのような群なのか，位数 (元の数) はいくつか，可換群か非可換群か，**どのような性質を持つのか**を調べるには，その**中身 (部分群)** を見ないといけない．

定義 (部分群)． 群 $(G,\circ)$ に対して，部分集合 $H \subset G$ が再び同じ積 $\circ$ に関して群をなすとき，H を G の**部分群** (subgroup) であるという．

定義 (自明な部分群)． 群 G の部分集合のうち，$\emptyset$ は (定義から) 部分群ではなく，自明群 $\{1\}$ と G 自身は G の部分群である．そこで，2 つの部分群 $\{1\}$ と G 自身を G の**自明な部分群**，$\{1\} \subsetneq H \subsetneq G$ なる部分群 H を G の**非自明な部分群**という．

• 一般に，二項演算 $\circ$ が定義されている**集合 $(X,\circ)$ が群であることを示すのは結構大変**なことである (← つまり S_n の時のように (G1),(G2),(G3) を示さないといけない)．

群の例 [5] (一般線形群 GL_n)． $M_n(K)$ を体 K の元を係数とする $n\times n$ 行列全体の集合とする．(← $K=\mathbb{R}$ または $K=\mathbb{C}$ としてよい)，このとき，

$$\mathrm{GL}_n(K) := \{A \in M_n(K) \mid \det(A) \neq 0\}$$

は n 次正則行列全体の集合であり，行列の積に関して群をなす．この群 $(\mathrm{GL}_n(K),\cdot)$ は K 上の**一般線形群** (general linear group) と呼ばれる．

• しかし，実は**既に群 G に含まれている集合 $H \subset G$ が (部分) 群であることを示すのは，はるかに簡単**である．つまり，すでに親玉のような大きな群 G に含まれている部分集合 $H \subset G$ に関しては，(部分) 群になっていることを示すのは簡単である (次のような裏技のような定理が存在する)：

定理 [6](部分群の判定条件)． もし群 G の**部分集合** $H \subset G$ が次の (i),(ii) を満たすならば，
H は G の**部分群**である：
(i) $\forall a, b \in H$ に対して，$a \cdot b \in H$, (← 最初から $a \cdot b \in G$ なので，$a \cdot b \in H$ が重要)
(ii) $\forall a \in H$ に対して，$a^{-1} \in H$, (← 最初から $a^{-1} \in G$ なので，$a^{-1} \in H$ が重要)
逆に，**部分群** $H \subset G$ は (i),(ii) を満たす. (← つまり部分群となる必要十分条件である)

定義 (演算について閉じている)． 群 $(G, \circ)$ の部分集合 $H \subset G$ が上の条件 (i) $\forall a, b \in H$ に対して，$a \circ b \in H$ を満たすとき，H は演算 $\circ$ について**閉じている**という．

例． $H := \{(1), (1\,2\,3)\} \subset S_3$ とする．このとき，$(1\,2\,3) \circ (1\,2\,3) = (1\,3\,2) \notin H$ であるから，H は演算 $\circ$ では閉じていない．よって，H **は** S_3 **の部分群ではない** (← 定理 [6] より)．

問題 [7](特殊線形群, アフィン変換群)． $\mathbb{R}$ 上の一般線形群 $\mathrm{GL}_2(\mathbb{R})$ の次の部分集合を 2 つとる：

$$\mathrm{SL}_2(\mathbb{R}) := \{A \in M_2(\mathbb{R}) \mid \det(A) = 1\}, \quad (\leftarrow \text{特殊線形群 (special linear group) という})$$

$$H := \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \;\middle|\; a \in \mathbb{R}^\times,\ b \in \mathbb{R} \right\}. \quad (\leftarrow \text{アフィン (affine) 変換群という})$$

(1) $(\mathrm{SL}_2(\mathbb{R}), \cdot)$ は $(\mathrm{GL}_2(\mathbb{R}), \cdot)$ の部分群である事を示せ．(← 部分群の判定条件を使う)
(2) $(H, \cdot)$ は $(\mathrm{GL}_2(\mathbb{R}), \cdot)$ の部分群である事を示せ．(← 部分群の判定条件を使う)

• 群 G の部分群 $H \subset G$ を調べる為に，もう少し準備をする：

命題 [8] (積の逆元)． 群 G の元 $a_1, \ldots, a_n \in G$ に対して，
(i) $(a_1 a_2)^{-1} = a_2^{-1} a_1^{-1}$, (ii) $(a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}$ が成立つ．

定義 (a^n)． 群 G の元 $a \in G$ と整数 $n \in \mathbb{Z}$ に対して，a の n 乗 a^n, $(n \in \mathbb{Z})$ を

$$a^n := \begin{cases} a \cdots a \ (n \text{ 個}), & (n > 0), \\ 1, & (n = 0), \\ (a^{-1})^{|n|}, & (n < 0) \end{cases}$$

によって定義する．

定義 (元の位数)． 群 G の元 $a \in G$ に対して，$a^n = 1$ となる最小の正整数を**元** a **の位数** (order) といい，$\mathrm{ord}(a)$ と書く．その様な n が存在しない時，a の位数は無限といって $\mathrm{ord}(a) = \infty$ とかく．

命題 [9] (指数法則)． 群 G の元 $a \in G$ に対して，指数法則が成り立つ：
(1) $a^m \cdot a^n = a^{m+n}$, $(\forall m, n \in \mathbb{Z})$,
(2) $(a^m)^n = a^{mn}$, $(\forall m, n \in \mathbb{Z})$.

系 [10]． $G = \{a_1, \ldots, a_n\}$ が可換群ならば，任意の元 $a_i \in G$ に対して，$a_i^n = 1$ が成り立つ．すなわち，位数 n の可換群 G の元の位数は n 以下である．

定義 [11] (生成する部分群). $A \subset G$ を群 G の**部分集合**とする．(← 部分群ではない)
(1) A **で生成される** G **の部分群**とは,

$$\langle A \rangle := \{a_1^{n_1} \cdots a_r^{n_r} \mid r \in \mathbb{N},\ a_i \in A,\ n_i \in \mathbb{Z}\ (i = 1, \ldots, r)\} \qquad \text{のこと.}$$

(2) 1 つの元 $a \in A$ によって生成された部分群 $\langle \{a\} \rangle$ を

$$\langle a \rangle := \{a^n \mid n \in \mathbb{Z}\} \quad (= \langle \{a\} \rangle)$$

を $a \in G$ **で生成された** G **の巡回部分群**であるという.
• 部分群 $H \subset G$ の元 $a, b \in H$ に対して，H は演算について閉じているから，a, b, a^{-1}, b^{-1} を繰り返しかけ合せた元は全て H の元となる：

系 [12]. 群 G の部分群 $H \subset G$ に対して,
(i) $a \in H$ ならば $\langle a \rangle \subset H$, (ii) $a_1, \ldots, a_n \in H$ ならば $\langle a_1, \ldots, a_n \rangle \subset H$.

問題 [13]. $S_n = \langle (1\,2), (2\,3), \ldots, (n-1\,n) \rangle$ を示せ．右辺を H としたとき，$S_n \supset H$ かつ $S_n \subset H$ を示せばよい．(← あみだくじの原理を用いる).

定義 [14] (巡回群 C_n). 群 G がある $a \in G$ に対して，$G = \langle a \rangle$ となるとき，G を**巡回群**という．元 a の位数が n のとき，$\langle a \rangle = \{a, \ldots, a^{n-1}, a^n = 1\}$ となる．この**位数** n **の巡回群を** C_n と書く.

命題 [15]. 巡回群 $G = \langle a \rangle$ はアーベル群 (可換群) である．(← 指数法則による)

なぜ部分群を調べるのか ①. 代数で学ぶ**ガロア理論**によって，あるタイプの 5 次方程式には (ルート $\sqrt[n]{a}$ と四則演算を混ぜ合わせて作る) 解の公式が存在しないという衝撃的なことが判明する (← しかし，解の公式が存在する 5 次方程式も当然ある；$X^5 = 2$ の解の 1 つは $\sqrt[5]{2}$ など). そこでどのようなタイプに解の公式があり，どのようなタイプに解の公式がないのかが問題となる．(← 実は，この様な解の公式の問題を考える中で群の概念が生まれた). 具体例として，2 つの 5 次方程式

$$f(X) = X^5 + X^4 - 4X^3 - 3X^2 + 3X + 1 = 0,$$
$$g(X) = X^5 - X^3 - X^2 + X + 1 = 0$$

を考えてみる．このとき，ガロア理論によって，方程式 $f(X) = 0$ と $g(X) = 0$ からガロア群という群 G がそれぞれ取り出せ，その群 G の性質から解の公式が存在するか，あるいは存在しないかを数学的に証明することができる．また，このガロア群 G は 5 次対称群 S_5 の部分群となることが証明される．よって，S_5 の部分群がどれだけあるかをよく知っていれば，前もってガロア群として現れる G の可能性を予測しておくことが出来るのである.

なぜ部分群を調べるのか ②. 上の答えを考えてみる．実は，解の公式が作れるかどうかはガロア群 G がどの位可換群に近いかが密接に関係する．(← 誤解を恐れずにイメージだけを伝えると，G が可換群または可換群に近い性質を持つとき，解の公式が作れる). つまり，ガロア群にとっては可換か非可換かという分類の仕方だけでは十分ではなく (← たった 2 つの元 $x, y \in G$ が存在して $xy \neq yx$ となると (定義から) 非可換群となる)，より可換群に近い性質をもった非可換群なのか，可換群とはかけ離れている非常に強い非可換性を持った群なのかといった，より G の詳細な情報が必要なのである．話しを戻してみよう．方程式 $f(X) = 0$ のガロア群 G は巡回置換 $a = (1\,2\,3\,4\,5)$ に対して，$G = \langle a \rangle \subset S_5$ なる位数 5 の巡回群 C_5 である．巡回群は可換群であり，この場合には解の公式が作れることが分かる．しかし，$g(X) = 0$ のガロア群は S_5 自身であることが分かり，この場合には**解の公式は存在しない**.

定義 (中心化群). 群 G の部分集合 $A \subset G$ に対して,

$$Z_G(A) := \{x \in G \,|\, xa = ax,\ (\forall a \in A)\} = \{x \in G \,|\, xax^{-1} = a,\ (\forall a \in A)\}$$

を A **の中心化群**という．(← A の任意の元と可換な G の元全体の集合)

問題 [16]. (1) A の中心化群 $Z_G(A)$ は (その名の通り) G の部分群を示せ．(← 部分群の判定条件)
(2) G 自身の中心化群 $Z_G(G)$ に対して，G がアーベル群 (可換群) $\iff Z_G(G) = G$ を示せ．

定義 (交換子群). (1) 元 $x, y \in G$ に対して，$[x, y] := xyx^{-1}y^{-1} \in G$ を x と y の**交換子**という．
(2) 交換子全体で生成される G の部分群 $\langle \{[x, y] \mid x, y \in G\} \rangle$ を G **の交換子群**といい，$D(G)$ とかく．

問題 [17]. (1) 交換子群 $D(G)$ は (その名の通り) G の部分群を示せ．(← 生成の定義より)
(2) $x, y \in G$ に対して，$xy = yx \iff [x, y] = 1$ を示せ．
(3) G がアーベル群 (可換群) $\iff D(G) = \{1\}$ を示せ．

なぜ部分群を調べるのか ③. 上の問題から，群 G が可換群に近ければ近いほど，$\{1\} \subset Z_G(G) \subset G$ は G に近く，$\{1\} \subset D(G) \subset G$ は $\{1\}$ に近いことが (容易に) 予想される．すなわち，G の部分集合 $Z_G(A)$ や $D(G)$ は G の「非可換性の強さ」を計るためのバロメーターである．このような部分集合は G の部分群として現れるという所が重要である．よって，そもそも G にどのような部分群が存在しているかを知ることは，G の非可換性の強さを知るという上でも重要な事である．

定義 [18] (交代群 A_n). $\forall \sigma \in S_n$ は互換の積で書ける．このとき互換が偶数個か奇数個かは σ によって一意的に定まる (← これは認めることにする)．$\sigma \in S_n$ が偶数個の互換の積のとき**偶置換**，奇数個の互換の積のとき**奇置換**という，
(1) S_n の偶置換全て集めた集合

$$A_n := \{\sigma \in S_n \mid \sigma\text{は偶置換}\} \subset S_n$$

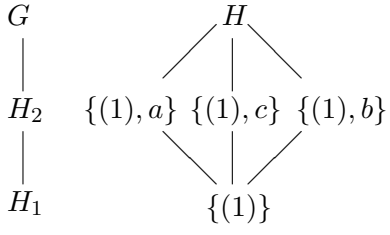
は S_n の部分群をなし，n **次交代群** (alternating group) と呼ばれる．(← 部分群の判定条件を使う)

問題 [19]. 単位元 $(1) = (1\,2)(1\,2) \in S_n$ は偶置換であることに注意すること．
(1) $n = 3, 4, 5$ に対して，A_n の位数はいくつか？ つまり，S_n の中に偶置換はいくつあるか?
(2) 一般に A_n の位数 (元の数) はいくつになるか予想せよ．

定義 (二面体群 D_n). 平面上の正 n 角形 ($n \geq 3$) を空間内で動かし，自分自身に重ねる変換全体は群をなし，**二面体群** (dihedral group) といい，D_n とかく．正 n 角形の頂点に時計と同じように番号を付け，頂点 n が一番上に来るようにすると，D_n の元は $\{1, \ldots, n\}$ の置換を与えており，D_n は S_n の部分群である．また，頂点 1 を頂点 i, $(1 \leq i \leq n)$ に動かす n 通りごとに，2 が 1 の右側にあるか左側にあるかの 2 種類がある．よって，D_n の位数 (元の個数) は $2n$ である．

命題 (D_n の構造)[20].
(1) 時計回りの回転 $\sigma = (1\,2 \cdots n)$ と頂点 n を動かさない裏返し $\tau = (1\,n-1)(2\,n-2)\cdots$ を考えれば，$D_n = \{(1), \sigma, \ldots, \sigma^{n-1}, \tau, \sigma\tau, \ldots, \sigma^{n-1}\tau\}$ である，
(2) $D_n = \langle \sigma, \tau \rangle$ となる．

定義 (Hasse 図).
部分群の列 $H_1 \subset H_2 \subset G$ が存在するとき，右図の様に棒を引く．但し，このとき G **と** H_1 **は棒では結ばないこと**とする．G の全ての部分群の包含関係を右図の様に棒で表した図を **Hasse 図**という．



例. $H = \{(1), a, b, c\}$, $a = (1\,2)$, $b = (3\,4)$, $c = (1\,2)(3\,4)$ は S_4 の部分群である．H の部分群は自明な部分群 $\{1\}, H$ の他に 3 つあり，Hasse 図は右図のようになる．

問題 [21]. 巡回群 $C_n = \langle \sigma \rangle = \{(1), \sigma, \ldots, \sigma^{n-1}\}$, $\sigma = (1\,2 \cdots n)$ とする．
$n = 2, \ldots, 5$ に対して，C_n の部分群を全て求め，その包含関係を Hasse 図で表せ．

問題 [22]．3 次対称群 S_3 の部分群を全て求め，その包含関係を Hasse 図で表せ．

問題 [23]．巡回群 $C_n = \langle\sigma\rangle = \{(1), \sigma, \ldots, \sigma^{n-1}\}$, $\sigma = (1\,2\cdots n)$ とする．
$n = 6, \ldots, 11$ に対して，C_n の部分群を全て求め，その包含関係を Hasse 図で表せ．

問題 [24]．$n = 3, 4, 5, 6$ に対し，n 次二面体群 D_n の部分群を全て求め，その包含関係を Hasse 図で表せ．

問題 [25]．$n = 3, 4$ に対して，n 次交代群 A_n の部分群を全て求め，その包含関係を Hasse 図で表せ．

問題 [26]．4 次対称群 S_4 の部分群を全て求め，その包含関係を Hasse 図で表せ．

[1]〜[6] 及びチャレンジ問題 [7]〜[26] の解答のヒント

[1] p.16 の S_n の性質をみる．

[2] (1), (2) ともに p.16 の証明 2. (i), (ii) をみること．

[3] p.16 の演習問題の解答をみる．

[4] これも，p.16 の演習問題の解答．

[5] 結合法則は行列の積の定義から示す (← 線形代数)

[6] (i), (ii) をみたすとき，H が (G1), (G2), (G3) を満たすことをいう．(G1) は G 全体で成立っている．

[7] (1), (2) それぞれ部分群の判定条件を使えばよい．

[8] 実際にかけて 1 になる事を示す．(← カッコは自由に付け替えてよいことにする)

[9] 定義に従って計算する．よって，場合分けが必要．

[10] $G = a_i G$ であることを用いる．

[11] (1), $\langle A\rangle$ が G の部分群を示す, (2) $\langle a\rangle$ が G の部分群を示す．部分群の判定条件と **[8]** を使う．

[12] 積で閉じているの意味を確認する．

[13] $H \subset S_n$ は定義から．$S_n \subset H$ をあみだくじの原理を用いて示す．

[14] なぜ，$\langle a\rangle = \{a, \ldots, a^{n-1}, a^n = 1\}$ なのかを説明する．

[15] 指数法則を使って，$a^i a^j = a^j a^i$ を示す．

[16] (1) 部分群の判定条件から，(2) 定義をよく考える．

[17] (1) 生成の定義を考える, (2) $\Rightarrow$ かつ $\Leftarrow$ を示す ($[x, y]$ の定義を確認)，(3) $\Rightarrow$ かつ $\Leftarrow$ を示す．

[18] A_n が S_n の部分群である事を示す．

[19] (1) A_n の元を実際に書き出してみる．(1) から何が予想できるか？

[20] $(1), \sigma, \ldots, \sigma^{n-1}$ が全て異なり，$\tau, \sigma\tau, \ldots, \sigma^{n-1}\tau$ も全て異なる．(2) $\subset$ かつ $\supset$ に $\tau\sigma\tau^{-1} = \sigma^{-1}$ を使う．

[21] 位数 $1 < k < n$ の部分群を全て求め，Hasse 図を書いてみる．(← 系 **[12]** を使ってみる)

[22] 位数 $1 < k < 6$ の部分群を全て求め，Hasse 図を書いてみる．(← 系 **[12]** を使ってみる)

[23] 位数 $1 < k < n$ の部分群を全て求め，Hasse 図を書いてみる．(← 系 **[12]** を使ってみる)

[24] 位数 $1 < k < n$ の部分群を全て求め，Hasse 図を書いてみる．(← 系 **[12]** を使ってみる)

[25] 位数 $1 < k < n$ の部分群を全て求め，Hasse 図を書いてみる．(← 系 **[12]** を使ってみる)

[26] 位数 $1 < k < 24$ の部分群を全て求め，Hasse 図を書いてみる．(← 系 **[12]** を使ってみる)

pp.24–27 の解説 (イメージによる理解)

• 群 G の**部分集合** $H \subset G$ が**部分群かどうか？** (1 を G の単位元とする)
(まず，G 全体で**結合法則**が成り立っているので，**当然，H でも成り立っている**ことに注意する．)

$H \subset G$ が**部分群**		以下が起こると，$H \subset G$ は**部分群でない**	
H : $\times\forall a \quad \times\forall b \quad \times ab$	(演算が**閉じている**)	H : $\times\exists a \quad \times\exists b$	$\times ab$ (**閉じていない**)
H : $\times 1$	(**単位元**が存在)	H :	$\times 1$ (**単位元がない**)
H : $\times\forall a \quad \times a^{-1}$	(**逆元**が存在)	H : $\times\exists a$	$\times a^{-1}$ (**逆元がない**)

• **[6](部分群の判定条件)**

H : $\times\forall a \quad \times\forall b \quad \times ab$ (演算が**閉じている**) ＋ H : $\times\forall a \quad \times\exists a^{-1}$ (すべての元に**逆元**が存在)

$\Longrightarrow$ H **は** G **の部分群** (すなわち，H は群の条件 (G1), (G2), (G3) を満たす).

• **交代群 A_n について** (A_n は S_n の部分群であることに注意)

$A_3 = \{(1), (1\,2\,3), (1\,3\,2)\}$,
$A_4 = \{(1), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3), (1\,2\,3), (1\,3\,2), (1\,2\,4), (1\,4\,2), (1\,3\,4), (1\,4\,3), (2\,3\,4), (2\,4\,3)\}$.

• **二面体群 D_n について** (D_n は S_n の部分群であることに注意)

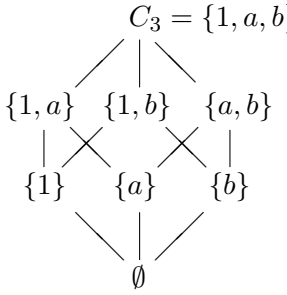
$D_3 = \{(1), \sigma = (1\,2\,3), \sigma^2 = (1\,3\,2), \tau = (1\,2), \sigma\tau = (1\,3), \sigma^2\tau = (2\,3)\} = S_3$,
$D_4 = \{(1), \sigma = (1\,2\,3\,4), \sigma^2 = (1\,3)(2\,4), \sigma^3 = (1\,4\,3\,2), \tau = (1\,3), \sigma\tau = (1\,4)(2\,3), \sigma^2\tau = (2\,4), \sigma^3\tau = (1\,2)(3\,4)\}$.

• **全ての部分群を求め，Hasse 図を書く** (部分集合を全て求めて，その中から部分群を探そう！)

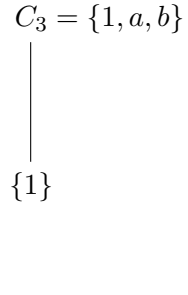
$C_3 = \{1, a, b\}$ の部分集合を全て求め，部分群かどうか判定する．(但し，$a = (1\,2\,3)$, $b = (1\,3\,2)$)
$H = \{1, a, b, c\}$ の部分集合を全て求め，部分群かどうか判定する．(但し，$a = (1\,2), b = (3\,4), c = (1\,2)(3\,4)$)

Hasse 図

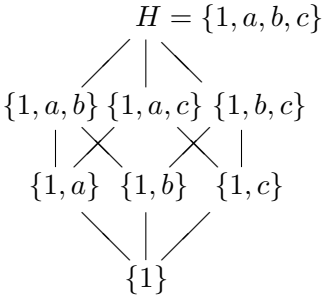
C_3 の部分集合



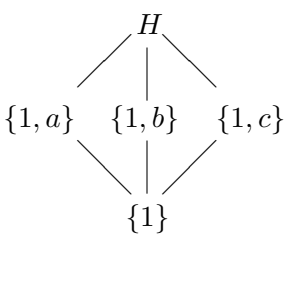
C_3 の部分群



H の 1 を含む部分集合



H の部分群



• しかし，$\#G = n$ のとき，G の全ての部分集合は 2^n 個あり**非常に大変！**．次の定理を使えば，**楽になる**．

定理． $H \subsetneq G$ を有限群 G の部分群とする．このとき，

$$\#H \leq \begin{cases} \frac{\#G}{2}, & (\#G \text{ が偶数}), \\ \frac{\#G-1}{2}, & (\#G \text{ が奇数}). \end{cases}$$

証明のスケッチ． $a_2 \notin H \subsetneq G = \{a_1 = 1, a_2, \ldots, a_n\}$ としても，一般性を失わない．(← 教科書 p.46 参照)
H の群表は G の群表 (右図) から，a_2 の行と列を取り除いて得られる．しかし，群表の内部に a_2 が残っていては H は群にならない．よって，H が群となる為には，$a_3, \ldots, a_n$(のいずれかの行及び列) をさらに削除し，各行各列に (1 つずつ) ある a_2 を消す必要が生じる．しかし，1 つの a_i $(3 \leq i \leq n)$ の削除によって消すことができる群表内部の a_2 は最大 2 つであり，(少なくとも) n が偶数のときは $n/2$ 個，n が奇数のときは $(n+1)/2$ 個の a_i を削除する必要がある． □

$\circ$	a_1	$\boldsymbol{a_2}$	a_3	$\cdots$
a_1	a_1	$\boldsymbol{a_2}$	a_3	$\cdots$
$\boldsymbol{a_2}$	$\boldsymbol{a_2}$	$\boldsymbol{a_s}$	$\boldsymbol{a_t}$	$\boldsymbol{\cdots}$
a_3	a_3	$\boldsymbol{a_u}$	a_v	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$