演習問題 *1.8　(星印＊のついた問題は全員に課す問題ではない。興味があり，意欲のある人はチャレンジしてみて下さい。) 剰余群を定義するとき G を可換群として定義したが，一般の群に対しても H がある種の性質をみたすとき定義できる。G を群とし，H を部分群とする。H が次の性質を満たすとき**正規部分群** (*normal subgroup*) と呼ぶ。

$$\text{任意の } g \in G \text{ と任意の } h \in H \text{ に対し } g^{-1}hg \in H \text{ が成立する。}$$

次を示せ。G を群とし，H をその正規部分群とする。このとき剰余類 G/H に $[a] \cdot [b] = [ab]$ によって演算を定義できる。

1.7　有限群

定義 1.31 元の個数が有限個の群を**有限群** (*finite group*) という。G が有限群の時，その元の個数を G の**位数** (*order*)[1] と言う。

一般に，有限集合 A に対して，その元の個数を $|A|$ で表すことにする。従って特に，有限群 G に対して，その位数は $|G|$ で表わされる。

G を可換な有限群とし，H をそ部分群とする。H による剰余類 Ha を考えると，$h_1, h_2 \in H$ が $h_1 \neq h_2$ ならば明らかに $h_1a \neq h_2a$ である。従って $|Ha| = |H|$ であり，それぞれの剰余類に含まれる元の個数は全て $|H|$ と同じである。

H に関する剰余類の個数，すなわち $|G/H|$ を

$$|G : H|$$

という記号で表し，H の G における**指数** (*index*) という。

以上のことから，次の定理が成り立つ。

定理 1.32 G を有限群とし H をその部分群とする。このとき，

$$|G| = |G : H| \cdot |H|$$

が成り立つ。

これにより，次の定理が成り立つ。

定理 1.33 [**Lagrange's theorem**] G を有限群とし H をその部分群とする。$|H|$ 及び $|G : H|$ は G の約数である。

これを使うと，例えば，位数が素数の群は，$\{e\}$ と自分自身以外の部分群を持たないということがわかる。

[1] G が有限群でない場合も位数という言葉を使うことがある。G が有限群でないとき「G の位数は無限大である」という言い方をする。

1.8 巡回群

G を有限とは限らない一般の群とし a を G のある元とする。a^n という形の元全体を集めたものを $< a >$ と書く。すなわち，

$$< a >= \{\ a^n \mid n \in \mathbb{Z}\ \} = \{\ \cdots, a^{-3}, a^{-2}, a^{-1}, a^0 = e, a, a^2, a^3, \cdots\ \}$$

この集合は 命題 1.15 の条件を満たしているので，G の部分群となる。これを，a で**生成**される**巡回部分群** (*cyclic subgroup*) という。0 と異なるある n で $a^n = e$ となる場合もあるので，$< a >$ は有限群であることもあり得る。$G =< a >$ である時，G を**巡回群** (*cyclic group*) という。

例 1.34　(1) $\mathbb{Z} =< 1 >$ は巡回群である。

(2) $\mathbb{Z}$ において，$< n >= n\mathbb{Z}$ も巡回部分群である。実は，$\mathbb{Z}$ の部分群としては，$n\mathbb{Z}$ 以外のものは存在しないことを後で示す。

(3) 絶対値 1 の複素数全体 $\mathbb{S}^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ は，積に関して群になる。$z \in \mathbb{S}^1$ に対して，$< z >= \{z^n \mid n \in \mathbb{Z}\}$ は巡回部分群である。

$\mathbb{S}^1$ 自身は巡回群ではない (証明はちょっと難しい。)

$\theta_n = e^{\frac{2\pi}{n} i}$ を 1 の n-乗根とすると，

$$< \theta_n >= \{\ 1,\ \theta_n,\ \theta_n^2,\ \theta_n^3,\ \cdots,\ \theta_n^{n-1}\ \}$$

は巡回群であり，位数が n の有限群である。

$\eta_\alpha = e^{2\pi\alpha\, i}$ として α を無理数とすると，ある $n \in \mathbb{Z}$ $(n \neq 0)$ で $\eta_\alpha^n = 1$ となることはないから，$< \eta_\alpha >$ は巡回群であり，位数は無限大である。

演習問題 *1.9　　乗法群 $\mathbb{S}^1$ が巡回群でないことを示せ。

定理 1.35 巡回群の部分群はまた巡回群である。

証明　$G =< a >$ を巡回群とし，H をその部分群とする。G の元は a^i という形をしている。$a^i \in H$ となる自然数 i のうち，最小のものを h とする。$H =< a^h >$ であることを証明する。

$H \supseteq < a^h >$ であることは明らかなので，$H \subseteq < a^h >$ であることを示せば良い。

H の任意の元を a^k とする。k と h に対して整数の剰余定理を適用すると，ある整数 q と $0 \leqq r < h$ となる整数 r があって

$$k = hq + r \qquad (0 \leqq r < h)$$

と書ける。

$$a^r = a^{k-hq} = a^k \cdot (a^h)^{-q} \in H$$

となる。h は，$a^i \in H$ となる自然数の中で最小のものだったので，$r = 0$ でなければならない。従って，$a^k \in < a^h >$ である。∎

この定理より，$G =< a >$ を巡回群とすると，G の任意の部分群 H は，$G = H$ でなければ，ある自然数 h があって $H =< a^h >$ となることがわかる。このことから，次の系が成り立つ。

系 1.36 $\mathbb{Z}$ の部分群は $n\mathbb{Z}$ という形のものしかない。

1.9 元の位数

定義 1.37 G を有限とは限らない一般の群とする。$a \in G$ に対して，$a^n = e$ となるような最小の自然数 n を，a の **位数** という。

$a^n = e$ となるような自然数 n が存在しない時は，a の位数は **無限大** であると言う。

定理 1.38 G を群とする。$a \in G$ の位数が n ならば

$$< a >= \{ e = a^0, a, a^2, \cdots, a^{n-1} \}$$

である。特に，$0 \leqq i < j \leqq n-1$ となる任意の $i < j$ に対して $a^i \neq a^j$ である。従って，a の位数が n ならば $| < a > | = n$ である。

証明　k を任意の整数とし，a^k を考える。

$k = qn + r$ となる $q \in \mathbb{Z}$ と $0 \leqq r \leqq n-1$ がある。

$$a^k = a^{qn+r} = a^{qn}a^r = (a^n)^q a^r = e^q a^r = a^r$$

であるから，a^k は $\{ e = a^0, a, a^2, \cdots, a^{n-1} \}$ のどれかと一致する。故に，

$$< a >= \{ e = a^0, a, a^2, \cdots, a^{n-1} \}$$

である。またこれらは全て異なる元である。なぜなら，ある $0 \leqq r_1 < r_2 \leqq n-1$ で $a^{r_1} = a^{r_2}$ ならば，$a^{r_2 - r_1} = e$ となり，$0 < r_2 - r_1 \leqq n-1$ なので，n が $a^n = e$ となる最小の自然数であることに矛盾するからである。 ∎

定理 1.39 G を有限群とし $|G| = g$ とする。G の任意の元の位数は g の約数である。従って，任意の $a \in G$ に対して，

$$a^g = e$$

が成り立つ。

証明　$a \in G$ を任意の元とし，その位数を n とする。位数の定義より，$a^n = e$ である。

定理 1.38 より，$| < a > | = n$ であるが，$< a >$ は部分群であるから，Lagrange's Theorem より，$| < a > | = n$ は g の約数である。すなわち，ある自然数 k があって $g = kn$ となっている。

$$a^g = a^{kn} = (a^n)^k = e^k = e$$

となる。 ∎

例 1.40 G と G' を２つの群とする。これらの積集合 $G \times G'$ に，次のような自然な演算を定義すると，これにより，$G \times G'$ が群になることは簡単にわかる。これを G と G' の **直積** という。

$$(g_1, g_1') \cdot (g_2, g_2') = (g_1 \cdot g_2, g_1' \cdot g_2')$$

ここで，$g_1, g_2 \in G$, $g_1', g_2' \in G'$ である。

$|G \times G'| = |G| \cdot |G'|$ であるのは明らかである。

例えば，$\mathbb{Z}_2 \times \mathbb{Z}_3$ は，

$$(0,0) \quad (0,1) \quad (0,2) \quad (1,0) \quad (1,1) \quad (1,2)$$

という 6 個の元を持ち，演算としては，共に 和 で書いているので，直積 $\mathbb{Z}_2 \times \mathbb{Z}_3$ 上の演算も和で書くと，

$$(0,1)+(1,2)=(1,0) \quad (1,1)+(1,1)=(0,2)$$

などとなる。また，

$$(1,1)+(1,1)=(0,2) \quad (0,2)+(1,1)=(1,0) \quad (1,0)+(1,1)=(0,1)$$
$$(0,1)+(1,1)=(1,2) \quad (1,2)+(1,1)=(0,0)$$

であるので，$6(1,1)=(0,0)$ であり，$1 \leqq k \leqq 5$ となる k では，$k(1,1) \neq (0,0)$ となるので，$(1,1) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ の位数は 6 である。

注意： ここでは，演算は 和 で書いているので，$(1,1)$ に関して k 回の演算を繰り返すことを $(1,1)^k$ とは書かずに，$k(1,1)$ と書いている。