代数系の基礎要綱 #4

2002–5–16　　河野

試験による単位取得以外にレポートでも単位取得を可能にする事にしました。次の要領でレポート課題を出します。レポート提出者に簡単な口頭試問を行い，理解を確認したものに対し単位を出します。

(1) 課題：プリント演習問題で「$*$」(星印) が 4 つ以上ついているものから 1 つ選択。

(2) 締切：10 月 31 日 (木)12 時 00 分。

(3) 提出方法：河野に手渡しして下さい

(4) 様式 ：レポート用紙は A4 とする。表紙に「代数系の基礎レポート」と明記した上で，学科・学年・出席番号 (在籍番号ではない)・氏名を書き，ステープラー (ホチキス) 等で左上隅 1ヶ所のみ止める事。

(5) 注意：レポート作成過程での質問等は勿論受け付けます。

小さい位数の群をすべて決定する事を再開しよう。4 まで実行していた。5 は素数なので巡回群しか存在しないので，6 を考えよう。

いままで出てきた位数 6 の群としては，巡回群 $\boldsymbol{Z}_6$, 2 個の巡回群の直和 $\boldsymbol{Z}_3 \bigoplus \boldsymbol{Z}_2$, 2 面体群 D_3, 対称群 S_3 があった。しかしこれらの中には同型なものが存在する。$\boldsymbol{Z}_6 \cong \boldsymbol{Z}_3 \bigoplus \boldsymbol{Z}_2$ は前にあつかったが，$D_3 \cong S_3$ が成立する。

演習問題 2.15　$D_3 \cong S_3$ を示せ。

可換群は定理 2.18 より，$\boldsymbol{Z}_6$ しか存在しない事が分かる。G を位数 6 の任意の群とする。G が位数 6 の元 g を含むと $\boldsymbol{Z}_6$ になるので，G は位数 6 の元を含まないとする。このとき単位元を除くと G の元の位数は 2 または 3 である。シローの定理より位数 2 の元と 3 の元が存在する。g を位数 3 の元，h を位数 2 の元とする。$N = \langle g \rangle$，$H = \langle h \rangle$ とおく。N は指数 2 の部分群なので G の正規部分群である。よって $h^{-1}gh$ は N の元である。$N \cap H$ は部分群なので位数は N 及び H の位数の約数だから $N \cap H = \{e\}$ である。よって命題 2.14 より $G = NH$ が分かる。$h^{-1}gh = e$ なら矛盾なので，$h^{-1}gh = g$ または $h^{-1}gh = g^2$ である。$h^{-1}gh = g$ のとき G は可換群になる。

以上から可換でない位数 6 の群 G は位数 3 の元 g と位数 2 の元 h で $h^{-1}gh = g^2$ の関係を満たすものが存在して，この 2 つの元で生成される事が分かる。この群を $\langle g, h;\, g^3 = e, h^2 = e, gh = hg^2 \rangle$ と表す。演算表で表すと次の様になる。

	e	g	g^2	h	hg	hg^2
e	e	g	g^2	h	hg	hg^2
g	g	g^2	e	hg^2	h	hg
g^2	g^2	e	g	hg	hg^2	h
h	h	hg	hg^2	e	g	g^2
hg	hg	hg^2	h	g^2	e	g
hg^2	hg^2	h	hg	g	g^2	e

演習問題 2.16　S_3(または D_3) $\cong \langle\, g, h\,;\, g^3 = e, h^2 = e, gh = hg^2 \rangle$ を示せ。

次に位数 8 の場合を考える。可換群は $\boldsymbol{Z}_8$, $\boldsymbol{Z}_4 \bigoplus \boldsymbol{Z}_2$, $\boldsymbol{Z}_2 \bigoplus \boldsymbol{Z}_2 \bigoplus \boldsymbol{Z}_2$ のいずれかであるので可換でない場合を考える。一般的に次の補題が成立する。

補題 2.19 群 G の単位元以外の元の位数がすべて 2 であれば可換群である。

証明　g, h を G の任意の元とする。$g^2 = e$, $h^2 = e$ より，$g = g^{-1}$, $h = h^{-1}$ が成立する。また gh の位数も 2 なので $(gh)^2 = e$ より，$gh = (gh)^{-1} = h^{-1}g^{-1} = hg$ が従う。 ∎

位数 8 の群 G の単位元以外の元の位数は 2,4,8 のいずれかである。位数 8 の元が存在すると巡回群なので，位数は 2 または 4 とする。単位元以外の元の位数が 2 であれば可換群になる。よって位数 4 の元が存在する場合を考える。g の位数を 4 とし，$N = \langle\, g \,\rangle$ とする。N は正規部分群なので $h \notin N$ となる元 h に対し $h^{-1}gh = g^n$ となる。g と $h^{-1}gh$ の位数は等しいので $n = 1$ または 3 である。$n = 1$ なら G は可換群になるので，$n = 3$ の場合を考える。h の位数は 2 または 4 であるが，2 のとき G は D_4 と同型になる。4 のときは今までででてきていない群になる。$|N \cap H| = 2$ となるので，$g^2 = h^2$ が従う。

以上をまとめると位数 8 の群は $\boldsymbol{Z}_8$, $\boldsymbol{Z}_4 \bigoplus \boldsymbol{Z}_2$, $\boldsymbol{Z}_2 \bigoplus \boldsymbol{Z}_2 \bigoplus \boldsymbol{Z}_2$, D_4, または $\langle\, g, h\,;\, g^4 = e, h^4 = e, gh = hg^3, h^2 = g^2 \rangle$ に同型になる。

演習問題 2.17　h の位数が 2 のとき D_4 と同型になる事を示せ。

最後に位数 9 の群を調べよう。実は位数 9 の群は可換群 $\boldsymbol{Z}_9$ 及び $\boldsymbol{Z}_3 \bigoplus \boldsymbol{Z}_3$ である事が次の様に分かる。

位数 9 の群 G が位数 9 の元を含めばそれは $\boldsymbol{Z}_9$ なので，単位元以外の元の位数は 3 とする。単位元以外の元 h を任意に選んで固定する。G 上の同型写像 J_h を $J_h(g) = h^{-1}gh$ で定義する。G に次の関係を定義すると同値関係になる。

$$g \sim g' \Longleftrightarrow \exists n \in \boldsymbol{Z}; J_h^n(g) = g'$$

$J_h^2(g) = h^{-2}gh^2$, $J_h^3(g) = h^{-3}gh^3 = g$ より，g を含む同値類の元の個数は高々3 個である。e を含む同値類の元の個数は 1 個である。よって他の同値類で元の個数が 1 個または 2 個のものが存在する。g を含む同値類の元の個数が 1 個のとき $J_h(g) = g$ が成立している。このとき G は可換群になる。g を含む同値類の元の個数が 2 個のとき $J_h^2(g) = g$ が成立している。即ち h^2 と g は可換である ($gh^2 = h^2g$ が成立する)。これから $hg = gh$ が従うので矛盾。 ∎

演習問題 2.18　上で定義した関係「 $\sim$ 」が同値関係になる事を示せ。

演習問題 **2.19　9 の場合と同様に p が素数のとき位数 p^2 の群は可換群である事を示せ。
演習問題 ***2.20　位数 12 の群をすべて決定せよ。
演習問題 ****2.21　位数 24 の群をすべて決定せよ。
演習問題 *******2.22　位数 120 の群をすべて決定せよ。

RSA 暗号等公開鍵暗号理論にも使われるフェルマーの小定理およびその一般化について述べる。
フェルマーの小定理と呼ばれるのは次の定理である。

定理 2.20 [フェルマーの小定理] p を素数とする。p で割り切れない自然数 a に対し a^{p-1} を p で割った余りは 1 である。

この定理の一般化を述べるためにオイラーの関数を定義する。自然数 m に対し 0 以上 $m-1$ 以下の m と互いに素な自然数の個数を $\varphi(m)$ で表し，オイラーの関数という。

定理 2.21 自然数 m と，m と互いに素な自然数 a に対し $a^{\varphi(m)}$ を m で割った余りは 1 である。

定理 2.21 から定理 2.20 は出てくる。次の命題が示されれば，系 2.12 から定理 2.21 は従う。

命題 2.22 n を 2 以上の自然数とする。$\boldsymbol{Z}_n^* = \{x \in \boldsymbol{Z}_n \mid \ x \text{ と } n \text{ は互いに素}\}$ とする。$\boldsymbol{Z}_n^*$ 上の演算を $x \cdot y = \mathrm{rem}(xy, n)$ で定義すると群になる。

証明の前に n が小さい場合どうなっているかを見よう。
$n = 5$ **の場合：** $\boldsymbol{Z}_5^* = \{1, 2, 3, 4\}$ である。$2 \cdot 2 = 4$, $2^3 = (2 \cdot 2) \cdot 2 = 4 \cdot 2 = 3$, $2^4 = 3 \cdot 2 = 1$ である。$\boldsymbol{Z}_5^*$ は 2 によって生成される位数 4 の巡回群になっている。
$n = 10$ **の場合：** $\boldsymbol{Z}_{10}^* = \{1, 3, 7, 9\}$ である。$3^2 = 3 \cdot 3 = 9$, $3^3 = 9 \cdot 3 = 7$, $3^4 = 7 \cdot 3 = 1$ である。$\boldsymbol{Z}_{10}^*$ は 3 によって生成される位数 4 の巡回群である。このとき $3^9 = (3^4)^2 \cdot 3 = 3$ なので，フェルマーの小定理は素数でない数には必ずしもあてはまらない事が分かる。
$n = 21$ **の場合：** $\boldsymbol{Z}_{21}^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$ である。$2^2 = 4$, $2^3 = 4 \cdot 2 = 8$, $2^4 = 8 \cdot 2 = 16$, $2^5 = 16 \cdot 2 = 11$, $2^6 = 11 \cdot 2 = 1$ である。また $20^2 = 1$ である。$H = \langle 2 \rangle$, $K = \langle 20 \rangle$ と置くと，$H \cong \boldsymbol{Z}_6$, $K \cong \boldsymbol{Z}_2$ であり，$\boldsymbol{Z}_{21}^* \cong H \bigoplus K$ なので，$\boldsymbol{Z}_{21}^* \cong \boldsymbol{Z}_6 \bigoplus \boldsymbol{Z}_2$ である。

n が素数のとき $\boldsymbol{Z}_n^*$ が巡回群である事が知られている。しかし逆は正しくない。
演習問題 ****2.23　n が素数のとき $\boldsymbol{Z}_n^*$ が巡回群である事を示せ。
演習問題 2.24　$n \leqq 20$ のとき $\boldsymbol{Z}_n^*$ を巡回群の直和で表せ。

証明　$\boldsymbol{Z}_n^*$ は 1 を含むので空集合ではない。$(x \cdot y) \cdot z = \mathrm{rem}((xy)z, n)$ となるので，結合法則は整数の積の結合法則より従う。1 が単位元になる。逆元は次の命題を必要とする。命題の成立を仮定すると，$\boldsymbol{Z}_n^*$ の任意の元 p に対し，整数 q, r が存在して $pq + rn = 1$ となる。このとき $p(q-n) + (r+p)n = 1$, $p(q+n) + (r-p)n = 1$ が成立するので，$0 \leqq qn$ と仮定してよい。$q = 0$ なら $n = 1$ となるので，$q \neq 0$ である。また q と n の公約数 d で 1 が割り切れるので，q と n は互いに素である。よって $q \in \boldsymbol{Z}_n^*$ である。$pq + rn = 1$ を $\boldsymbol{Z}_n^*$ で考えると $p \cdot q = 1$ を意味している。よって逆元 q が存在する。

命題 2.23 整数 p,n の最大公約数が d である必要十分条件は次の様な整数 q, r が存在する事である。

$$pq + rn = d$$

演習問題 ****2.25　命題 2.23 を証明せよ。

次は RSA 暗号計算のとき必要になる性質である。

命題 2.24 p が素数のとき $\varphi(p) = p - 1$ である。
$n = pq$ で，p 及び q が素数のときまた $\varphi(n) = \varphi(p)\varphi(q)$ が成立する。

演習問題 *2.26　命題 2.24 を証明せよ。

以上を準備として公開鍵暗号としての RAS 暗号を紹介しよう。

自分への mail 等を暗号化して欲しい人 (Alice としよう) は次の様にする。2 つの巨大な素数 p,q を選ぶ。素数は通常 10 進数で 100 桁から 300 桁ぐらいのものを選ぶ。$n = pq$ とおき，$\boldsymbol{Z}_n^*$ の元 e を 1 つ固定する。次に $ed = k\varphi(n) + 1$ となる d を求める。(n, e) を公開鍵として公開し，(n, d) は秘密鍵とする。

Alice に暗号化して情報を送りたい他人 (Bob としよう) は次の様に暗号化を行う。何らかの coding により情報は数字化されていると仮定する。暗号化の関数 f は $f(P) = \mathrm{rem}(P^e, n)$ である。$Q = \mathrm{rem}(P^e, n)$ を計算し Alice に送る。

Alice は Q を受け取る。d を知っているので，$\mathrm{rem}(Q^d, n)$ を計算すると，$Q^d = (P^e)^d = P^{ed} = P^{k\varphi(n)+1} = (P^{\varphi(n)})^k \cdot P^1$ なので $\mathrm{rem}(Q^d, n) = \mathrm{rem}(P^{\varphi(n)}, n)^k \,\mathrm{rem}(P^1, n) = P$ となり P が得られる。

この情報を盗み見た第 3 者 (Catherine としよう) は公開鍵を知っている。Q から P を解読できないのだろうか? 解読するためには d を知らなければならない。そのためには $\varphi(n) = (p-1)(q-1) = pq - p - q + 1 = n + 1 - p - q$ を知らなくてはならない。即ち n の因数 p, q を知らなくてはならない。しかし因数を求める効果的なアルゴリズムは知られていないので，しらみつぶしに調べるしかない。

この RSA 暗号の安全性は次の 2 つの仮定に基づいている。
(1) d を求めるためには n の因数 p, q を求めなくてはならない。即ち，他の d を求める方法はない。
(2) 素因数を求める効果的なアルゴリズムはない。

この 2 つとも証明されているわけではない。私の個人的予想をいうと証明する事ができないと思われる。証明することは出来ていないが状況証拠から (1)，(2) を仮定するのは許されよう。

具体的に計算してみよう。$n = 46927, e = 39423$　とする。公開鍵は $(46927, 39423)$ とする。勿論この程度の大きさだと容易に解読されてしまうが，テストケースとして実験してみよう。データはアルファベットで書かれていて，長さが 3 の倍数であるものとする。例えば「AHO」というデータを暗号化して送る事を考える。$A \to 0, B \to 1, C \to 2, \ldots, Z \to 25$ に対応させる。データを 26 進数と考えると，$AHO = 0 \times 26^2 + 7 \times 26 + 14 = 196 = P$ である。P^{39423} を計算する必要がある。

$Q_n = P^{2^n}$ を順に計算する。

n	2^n	Q_n	n	2^n	Q_n
0	1	$Q_0 = P^1 = 196$	8	256	$Q_8 = Q_7^2 = 23298$
1	2	$Q_1 = Q_0^2 = 38416$	9	512	$Q_9 = Q_8^2 = 39122$
2	4	$Q_2 = Q_1^2 = 28760$	10	1024	$Q_{10} = Q_9^2 = 6779$
3	8	$Q_3 = Q_2^2 = 2298$	11	2048	$Q_{11} = Q_{10}^2 = 13308$
4	16	$Q_4 = Q_3^2 = 24980$	12	4096	$Q_{12} = Q_{11}^2 = 366$
5	32	$Q_5 = Q_4^2 = 12081$	13	8192	$Q_{13} = Q_{12}^2 = 40102$
6	64	$Q_6 = Q_5^2 = 7591$	14	16384	$Q_{14} = Q_{13}^2 = 29041$
7	128	$Q_7 = Q_6^2 = 43852$	15	32768	$Q_{15} = Q_{14}^2 = 7637$

$39423 = 2^{15} + 2^{12} + 2^{11} + 2^7 + 2^6 + 2^5 + 2^4 + 2^3 + 2^2 + 2^1 + 1$ なので

$$P^{39423} = Q_{15}Q_{12}Q_{11}Q_7Q_6Q_5Q_4Q_3Q_2Q_1Q_0$$

である。これを実行すると $P^{39423} = 22842 = 1 \times 26^3 + 7 \times 26^2 + 20 \times 26^1 + 14$ となる。変換した結果は 26 進数 4 桁で表す。この暗号系では

$$AHO \quad \rightarrow \quad BHUO$$

と暗号化される。

演習問題 **2.27　公開鍵が $(46927, 39423)$ で与えられている。暗号化したコードが BFIC であった。この暗号を解読せよ。

演習問題 ****2.28　前の問題は電卓があれば実行可能であった。今度はもう少し n を大きくする。公開鍵を $(536813567, 3602561)$ とする。平文はアルファベット 6 文字で暗号文は 7 文字のブロックで構成されているものとする。暗号 BNBPPKZAVQZLBJ を解読せよ。プログラムを書くことで可能になるであろう。