となります．$\mathbf{F}_p=\mathbf{Z}/p\mathbf{Z}$ は体の構造を持つため，$\overline{y}$ には乗法の逆元 $\overline{y}^{-1}$ が存在します．そこで，この元を用いて等式を変形すると，

$$(\overline{x}*\overline{y}^{-1})^2=\overline{-1}$$

となります．$\mathbf{F}_p$ の乗法群は位数 $p-1$ の巡回群と同型です[5]．g を乗法群の生成元とすると，$g^{\frac{p-1}{2}}=\overline{-1}$ であり，n に関する方程式 $(g^n)^2=\overline{-1}=g^{\frac{p-1}{2}}$ の解は $2n=\dfrac{p-1}{2}$ となります．したがって，$p\equiv 3 \bmod 4$ のときは整数解 n を持たないため，$(\overline{x}\cdot\overline{y}^{-1})^2=\overline{-1}$ となる $\overline{x}$, $\overline{y}$ は存在しません．

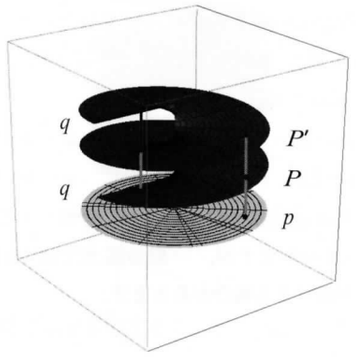
$p\equiv 1 \bmod 4$ のとき，$r=g^{\frac{p-1}{4}}$ として，p と $r-i$ の公約数 $x+iy$ を $\mathbf{Z}[i]$ での割り算を用いて求めることができます．このとき，$(x+iy)(x-iy)=x^2+y^2$ は $p(r-i)$, $p(r+i)$, p^2 の約数です．したがって，x^2+y^2 は $p(r+i)-p(r-i)=2ip$ を割り切り，しかも p^2 の約数でもあるので，$x^2+y^2=1$ または $x^2+y^2=p$ のいずれかです．もし $x^2+y^2=1$ であるとすると，$x+iy$, $x-iy$ は単元であり，p と $r-i$, p と $r+i$ は互いに素となります．しかし，$(r-i)(r+i)=r^2+1$ は p で割れるので，それらは成立しません．以上より，$x^2+y^2=p$ となることが分かりました．□

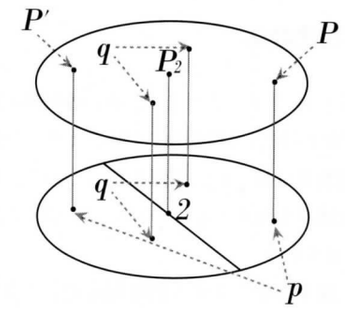
$p=2$ または $p\equiv 1 \bmod 4$ のときは，解 x, y を用いて $p=(x+iy)(x-iy)$ と表されます．この場合，素数 p は R の素元ではなく，代わりに $P=x+iy$ および $P'=x-iy$ が素元となります．また，$P=uP'$, $u\in\{\pm 1, \pm i\}$ となるのは $p=2$ の場合に限ります．$P_2=1+i$ とすると，$2=-iP_2^2$ が成立します．一方，$q\equiv 3 \bmod 4$ のとき，q は R においても素元です．これは，前節の拡大では見られなかった現象であり，素元に変化がないため「惰性」と呼ばれます．

$$G(K/K_0)\simeq C_2$$

$$\begin{cases} p=PP' & p\equiv 1 \bmod 4 & \cdots\text{分解} \\ q=q & q\equiv 3 \bmod 4 & \cdots\text{惰性} \\ 2=-iP_2^2 & p=2 & \cdots\text{分岐} \end{cases}$$

前節のように概念図を描くと以下のようになります．ただし，「惰性」の状況が正確には表現されていません．





一変数代数関数体と代数体の K に関する比較は，以下の表のようになります．

	一変数関数体	代数体
K	$\mathbf{C}(Z)$	$\mathbf{Q}$
R	$\mathbf{C}[Z]$	$\mathbf{Z}[i]$
R の単元	$u\in\mathbf{C}\setminus\{0\}$	$u\in\{\pm 1, \pm i\}$
R の素元	$u(Z-A)$	uP, uP', uq, uP_2

次回は，ガロアの第二論文に関わる一変数関数体の重要な例を紹介する予定です．

(たかはし ひろき／広島大学理学研究科・総合科学部)

[5] 乗法群の位数は $p-1$ なので，全ての $\overline{x}\neq\overline{0}$ に対し，$\overline{x}^{p-1}=\overline{1}$ が成立します．もし乗法群が巡回群でないとすると，$p-1$ のある真の約数 d に対し，全ての乗法群の元 $\overline{x}$ に対し $\overline{x}^d=\overline{1}$ が成立することになります．しかし，方程式 $x^d-\overline{1}=\overline{0}$ の体 $\mathbf{F}_p$ の拡大体における解の個数は d 以下であるため，$p-1$ 個の解があることに矛盾します．

Mathématiques colonne 10

1/998001 =

西山　豊

1 を 998001 で割ると，驚くべき結果になる．こんなメールがインターネットを飛び交ったのは 2012 年の年初のことである．私は，イギリスの知人からのメールで知ったので，この話題はおそらく世界中をかけめぐっていることだろう．1 を 998001 で割ると，小数点以下が 3 桁の数で 000 から 999 まで順番に並ぶ．ただし 998 だけは除くという．そして，その計算結果の画像がインターネットに出回った．

1/998001＝0.000001002003004005006007008009010011012013014015016017018019020021022023024025026027..... 995996997999 ...

長年，数学と関係していると，少々のことには感動しないが，この画像を見て，おやっと思わざるを得なかった．数学が嫌いな人，苦手な人でも，この美しい数字の列に驚くことだろう．998 だけが抜けるのは惜しい．998 も入ればよいのにと残念がるだろう．一方，数学愛好家は，この数字が並ぶ理由を知りたがる．この問題は高校数学の知識で説明できるので，皆さんも考えてみてはどうだろうか．

まず，この計算結果が正しいことをどのようにして確認するのか．紙と鉛筆で，1÷998001 を行ってもよいが，除数が 6 桁の数であり，小数点以下が約 3000 桁も計算しなければならないので，かなりの時間がかかる．電卓を使う方法もあるが，電卓の有効桁はたかだか 14 桁程度であり，これでは歯が立たない．手頃なのは，表計算ソフトを使う方法であろう．まず 1 を 1000000 倍(＝10^6)して，これを 998001 で割ると，商が 1 で余りが 1999 となる．余り 1999 を 1000000 倍して，これを 998001 で割ると商が 2003 で余りが 3997 となる．このような操作を繰り返し，商を順番に並べると，0.000001002003…となっていく．このような方法では小数点以下が 3000 桁でも楽に計算できることになり，冒頭の計算結果が正しいことが確認できる．また，これと同じ方法で計算してくれるインターネットのサイトもある．

999 の次はどうなっているのか．次は 000 である．000 から 999(998 を除く)の循環節が繰り返される．000 から 999 までは規則的な循環節であり，これ自体が循環するので，循環小数である(循環節をもつ循環小数)．では，なぜこのように規則的に並ぶのだろうか．どうして 998 だけが除かれるのだろうか．それを解くカギは，998001 という数が

$$998001 = 999^2$$

であることに気付くと，ほとんど解けたことになる．1 を 998001 で割るということは，1/999 に 1/999 を掛けたことになる．では 1/999 はどのような数であるのか．

$$1/999 = 0.001001001001001001001...$$

上のような循環小数となる．右辺から左辺を導く方法は，高校数学では馴染みの初項 1/1000，項比 1/1000 の等比級数としてあらわされる．また，掛け算(0.001001001…×0.001001001…)は，足し算(0.001001001… ＋ 0.000001001001…)となり，計算はそれほど難しくはない．1 を位ごとに合計すると

$$997, 998, 999, 1000, 1001$$

と続く．1000，1001 が 3 桁では桁上がりとなり，999 に 1 が足される．999 も 1 が足されるので桁上がりとなる．ところが 998 は 1 が足されても 999 で桁上がりとならない．

$$997, 999, 000, 001, 002$$

このようにして，998 が無いのである．1/998001 の理由を考えるのは，暇つぶしにちょうど良い．

(にしやま　ゆたか／大阪経済大学)