イデアルとは何か

はじめに

この小論は，高木貞治博士の著書「**初等整数論講義**[1)]」（以下「**講義**」）に依拠して代数的整数論の端緒である**イデアル**について，できるだけ初等的に述べようとするものである．「**講義**」の著書名には「初等的」と銘打ってあるものの，それは戦前帝大での専門課程における講義では初等的であっても，昭和・平成の高校１,２年程度の数学知識の読者にはなかなか「高等的」といえる．そこで数学好きの初学者にぜひイデアルの精妙さを知っていただきたいという熱意だけを頼りに書き綴ったものである．この立場を「**初学的**」と言い表すことにしている．

イデアルとは，ひとことでいえば，整数における「倍数」概念の拡張である．一般に或る整数の倍数の集合A（例えば3の倍数の集合）には次のような性質がある．

（１）Aの任意の二つの要素a, bの和，差はまたAの要素である．

（２）任意の整数xとAの任意の要素aの積xaもAの要素である．

このうち（１）の性質には格別な問題はなく，二つの3の倍数，例えば$3a$と$3b$の和・差はそれぞれ$3(a+b)$, $3(a-b)$でまた3の倍数になることに何の違和感もない．だから3の倍数はそれ自身で新たな一つの独立した「整数の世界」を作り上げることができるのである（近年（１）のような集合は「環」と呼ばれる）．

ところが（２）の方は，Aだけの問題ではなく，大もとの整数全体の集合（これをZとしよう）の要素との積もまたAに含まれるというのである．すなわち，Aは（１）でいうような独自の世界を持ちながら，一方ではZに依存している，あるいはZの性質を引き継ぐということを主張しているのである．このような「倍数」の性質は，単に倍数であるだけの時には注目されなかったのであるが，これがイデアルになると俄然異彩を放ってくるのである．

すなわち，**イデアルとは，（拡張された）「整数」と呼ばれる集合の中で，上記の**（１），（２）**の性質を持つ部分集合のことをいうのである．**だから例えばZにおいてはイデアルは普通の倍数として振る舞うだけで，イデアルとしての格別な働きをすることはない．しかし，「整数」の概念が拡張されるに伴って「倍数」の概念も変貌せざるを得ず，特に上記（２）の性質においてイデアルは自分の出生地である「拡張された整数」の世界の本質を見せてくれるよすがとなるのである．

イデアルが生まれるにはクンマーやデデキントといった天才的数学者たちの苦労があったことが「**講義**」に簡潔に述べられている．また高木博士は同書の或る注釈内で，「筆者はイデヤルママ論を世界的に普及せしめるために，ドイツ文字専用の慣例をやめて欲しいと思う．」と，イデアル論の普及を願っておられることをさりげなく，しかし熱意を込めて述べている．この小論が博士のその思いに少しでも寄与できることでもあれば望外の喜びとなるのだが．

冒頭に述べたように，イデアル論は代数的整数論の入り口であり，その先は高木博士の創設になる「高木類体論」に直接につながっている．この小論の筆者は類体論が究極の目標なのであっ

---

1) 共立出版株式会社 1994年7月1日 第2版28冊 発行をもとにした．

て，どうかイデアル論だけで生涯を終えることのないようにというのが残り少ない人生の課題である．

本論の議論の進め方として，文字通り初等的ないわゆる整数の整除に関する問題の解き方から始めているが，次には直ちに二次体の整数論の有用性を解き，ごく自然に読者をイデアルの導入に導いていくことを予定している．お手本はもちろん「**講義**」であるが，設問や証明・解答などはすべて筆者が独自に書き下ろしたもので，あくまで本論の中身についての責任は全て筆者（福沢正男）が負うことはいうまでもない．

2017年2月9日

目　次

1．整数に関する諸問題と合同式

整数に関する問題には難問が多いことで知られる．最たるものは「フェルマーの最終定理[2)]」や「ゴールドバハの予想[3)]」等であるが，そんな「雲の上」の問題でなくても初等的な整数に関する問題の中にも解法が一筋縄ではいかないものがあるので，それらを解くためにどのような方法があるかを主として代数的に追ってみようというのがこの章の趣旨である．以下では，整数・有理数・実数および複素数の四則計算については既知とし，用語も重要なものは定義を述べるが，それ以外には常識的な意味で用いられているものと考えて差し支えない（例：約数・倍数，最大公約数・最小公倍数など）[4)]．

【問題 1.1】２で割っても３で割っても割り切れる最小の正整数は何か．また，一般解はどうか．

【解】２と３の最小公倍数は６であり，余りはないので求める最小の正整数は６である．任意の整数を n とすれば一般解は $6n$．（n は以下も同様）‖

【問題 1.2】２で割っても，３で割っても１余る最小の正整数は何か．また，一般解はどうか．

【解】２と３の最小公倍数に１を足したものが求める解になるから７である．一般解は $6n+1$．‖

【問題 1.3】２で割ったら１余り，３で割ったら２余る最小の正整数は何か．また，一般解はどうか．

【解】求める数を x とする．x を２と３の最小公倍数６で割った時の余りは，

$$(1-1)\quad 0,1,2,3,4,5$$

のいずれかである．この0,1,2,3,4,5 を２で割った時の余りは，

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

であり，同じく３で割った時の余りは，

$$(1-3)\quad 0,1,2,0,1,2$$

である．この時，(1−2)の行が 1 で，(1−3)の行が 2 になっているのは，(1−1)の 5 のところである．すなわち，x を６で割った余りが５になる数が求める数である．よって求める最小の正整数は５である．一般解は $6n+5$ ‖

---

2) n≥3の自然数に対し，$x^n+y^n=z^n$を満たす自然数 x, y, z はないという定理．1994年ワイルズが証明．

3) 「2より大きい偶数は二つの素数の和で表すことができる」という予想．未解決．

4) 「付録１」を参照．

問題 1.3で，これがもう少し大きな数になった場合には，すでにこのような解法では甚だ困難になる．そこで今度は二元一次不定方程式を解くという，代数的な方法を用いて次のような問題を解いてみよう．

【問題 1.4】43で割ると21余り，52で割ると37余る最小の正整数は何か．一般解も求めよ．

まず，問題 1.3の解答と同じように考えてみよう．求める整数を x とする．43と52の最小公倍数は（43が素数だから）43×52=2236 であるから，x を2236で割った余りは，0〜2235のいずれかである．この中に，43で割った余りが21，52で割った余りが37のものがあれば，それが x（または x に関係のある数）であるが，2236個の中からこのような数を逐一「探す」のは労多くして無益な方法である．これを二元一次不定方程式で解いてみよう．

x を43で割った商を a，52で割った商を b とすれば，

$$x = 43a + 21 = 52b + 37$$

$$(1-4) \quad \therefore\ 43a - 52b = 16$$

この二元一次不定方程式(1−4)に**整数解が存在するのか**という問題もあるが，今はとにかく存在するものと前提して先に進むことにする．

この方程式の整数解を求めるには，大きい係数を小さい係数で割って商と余りを出し，別の文字に置き換えながら係数が 1 の文字が出るまで続けるのである．まず，52=43+9だから，

$43a - (43b + 9b) = 16$　　$\therefore\ 43(a-b) - 9b = 16$　…①

$a - b = c$ に置き換えて，　$43c - 9b = 16$　…②

43=9×4+7だから　　$4 \times 9c + 7c - 9b = 16$，$\therefore\ 9(4c-b) + 7c = 16$．

$4c - b = d$ とおいて　　$9d + 7c = 16$　…③

9=7+2だから　　$7d + 2d + 7c = 16$　$\therefore 7(d+c) + 2d = 16$．

$d + c = e$ とおいて　　$7e + 2d = 16$　…④

7=6+1だから　　$6e + e + 2d = 16$　$\therefore\ 2(3e+d) + e = 16$

$3e + d = f$ とおいて　　$2f + e = 16$．

やっと係数が 1 の文字 e が出てきたので，$e = 16 - 2f$ を④に代入して整理すると，

$$d = 7f - 48.$$

これを③に代入して整理すると，

$$c = 64 - 9f.$$

これを②に代入して整理すると，

$$b = 304 - 43f \quad \cdots⑤$$

そして最後にこれを(1−4)に代入して整理すると，

$$a = 368 - 52f \quad \cdots⑥$$

こうしてやっと，a, b の整数解が求められたのである．⑤，⑥で，f は任意の整数を表している．例えば，$f = 1$ ならば，$a = 316$, $b = 261$ となり，ゆえに x は，$x = 43a + 21 = 52b + 37$ より，

$$x = 43\times 316 + 21 = 52\times 261 + 37 = 13609$$

となる．これは(1−4)を満たすが「最小の正整数」ではない．そのためには f を適当に選定する必要がある．すなわち，最適値は $f = 7$ で，この時，$a = 4,\ b = 3$．よって求める x は，

$$x = 43\times 4 + 21 = 193$$

である．一般解は $2236n + 193$．‖

このように，数字が大きくなると計算が面倒になる．では次に同じ問題を「合同式」を用いて解いてみよう．

一般に整数 $a,\ b$ の差が m の倍数である時，「$a,\ b$ **は** m **を法として合同である**」といい，

$$a \equiv b \pmod{m}$$

と表す．これを「**合同式**」という．

この記号はドイツの19世紀の数学者 **C.F.ガウス**が著書「Disquisitiones Arithmeticae」（通称「**ガウス整数論**」）で初めて用いた（参考：「ガウス整数論」高瀬正仁訳　朝倉書店 2003年3月1日第5刷）．

これによれば，「x を43で割った余りが21」ということは，「x から21を引いた差が43の倍数」ということになるから，

$$(1-7)\quad x \equiv 21 \pmod{43}$$

と表せる．合同式では，加・減・乗法については，**法が同じならば**，普通の等式と同様に扱えるという特徴がある[5]．

（例）(1−7)の両辺に5を足したり引いたり掛けたりすると，

(1−7)の両辺に 5 を足す　　$x + 5 \equiv 21 + 5 \quad \therefore\ x + 5 \equiv 26 \pmod{43}$

(1−7)の両辺から 5 を引く　$x - 5 \equiv 21 - 5 \quad \therefore x - 5 \equiv 16 \pmod{43}$

(1−7)の両辺に 5 を掛ける　$5x \equiv 21\times 5 \quad \therefore 5x \equiv 105 \pmod{43}$

もう一つ，普通の等式にはない性質として，法となっている数の倍数ならば一方の辺だけに加減しても合同式が成り立つのである．

(1−7)の右辺に43を足す　　$x \equiv 21 + 43 \quad \therefore\ x \equiv 64 \pmod{43}$

(1−7)の右辺から43×2を引く　$x \equiv 21 - 43\times 2 \quad \therefore\ x \equiv -65 \pmod{43}$

合同式では**整数の除算の意味が拡張**されているので商とか余りという用語を用いないが，両辺を「**剰余**」と呼ぶことが多い[6]．

同様に「x を52で割ると37余る」は，

$$(1-8)\quad x \equiv 37 \pmod{52}$$

---

5) 両辺を同じ数で割る時には若干条件がある（後述）．

6) ガウスは合同式の両辺は互いに剰余と呼ばれると言っているが，もちろん拡張された意味である．

となる．これらの式には２元方程式を用いた時のような文字a, bがない．とはいえ，(1−7)や(1−8)のような合同式から直ちに一般の等式を導くこともまた必要である．(1−7)からは，任意の整数tを用いて，

$$(1-9)\quad x=21+43t$$

と表される．同様に(1−8)から任意の整数uを用いて，

$$(1-10)\quad x=37+52u$$

と表される．さて，(1−10)の式を(7)に代入すると，

$$(1-11)\quad 37+52u\equiv 21\ (\mathrm{mod}.43).$$

このような合同式を$u\equiv a\ (\mathrm{mod}.\ m)$のような形にすることを，方程式を解くことに因んで「合同式を解く」という．そのために次のような技法を用いる．

両辺から37を引いて，

$$52u\equiv -16\ (\mathrm{mod}.43).$$

ここで，普通の等式ならば両辺を４で割りたいところだが，合同式では両辺の除算には条件がある．すなわち，**両辺を割り切る整数と法（上の例では43）が「互いに素」であるならば割ってもよいが，互いに素でないときは法も同じ整数で割らなければならない**．この式では法が素数なので両辺を４で割ることができる．ゆえに，

$$13u\equiv -4\ (\mathrm{mod}.43).$$

両辺を３倍すると，

$$39u\equiv -12\ (\mathrm{mod}.43).$$

左辺だけから$43u$を引くことができるので，

$$-4u\equiv -12\ (\mathrm{mod}.43).$$

両辺を–4で割って，

$$(1-12)\quad u\equiv 3\ (\mathrm{mod}.43).$$

これで合同式(11)が解けたことになる．こうした技法は工夫によってはもっと早く解けることがある．

(1−12)式のuは，「43で割ると３余る数」を意味している．任意の整数nを使って一般的に表すと，$u=43n+3$である．最小正整数解を求めるために$n=0$とすれば$u=3$．これを(10)に代入すると，求めるxは，

$$x=37+52\times 3=193$$

である．一般解は43と52の最小公倍数 2236より，$x=193+2236n$．‖

(1−10)の式を(1−7)に代入したところでは，(1−9)の式を(1−8)に代入しても同様の結果となることはもちろんである．$u=3$ の代わりに $t=4$ が得られ，$x=21+43\times 4=193$となる．

ずいぶん長い解答のように見えるが，それは合同式を説明しながらだったので，説明を抜きにすれば次のようになる．

【問題 1.4】（再掲）43で割ると21余り，52で割ると37余る最小の正整数は何か．一般解も求めよ．

【解】求める正整数を x とする．題意より，二つの合同式，

$$(1-13) \qquad x \equiv 21 \pmod{43}$$

$$(1-14) \qquad x \equiv 37 \pmod{52}$$

が得られる．(2)より，$x = 37 + 52t$ （t は任意の整数）と置けるから，これを(1)に代入して，

$$37 + 52t \equiv 21 \pmod{43}$$

$$52t \equiv -16 \pmod{43}$$

$$(1-15) \qquad 13t \equiv -4 \pmod{43}$$

両辺を３倍してから，左辺だけから $43t$ を引くと，

$$-4t \equiv -12 \pmod{43}$$

$$\therefore \quad t \equiv 3 \pmod{43}$$

よって，$t = 3 + 43n$ （n は任意の整数）と表されるので $n = 0$ より，$t = 3$．よって求める x は，

$$x = 37 + 52 \times 3 = 193$$

となる．一般解は43と52の最小公倍数 2236より，$x = 2236n + 193$．‖

このように，ほとんど普通の連立方程式と同様の解き方で解が得られる．次に，もう不定方程式で解くのはほとんど無理と思える問題を合同式で解いてみよう．

【問題 1.5】141で割ると73余り，251で割ると137余り，さらに76で割ると67余る最小の正整数は何か．一般解も求めよ．

【解】求める正整数を x とする．題意より，三つの合同式，

$$(1-16) \quad x \equiv 73 \pmod{141}$$

$$(1-17) \quad x \equiv 137 \pmod{251}$$

$$(1-18) \quad x \equiv 67 \pmod{76}$$

が得られる．(1−18)より，$x = 67 + 76t$ （t は任意）を(1−17)に代入すると，

$$67 + 76t \equiv 137 \pmod{251}$$

これを解くと，$t \equiv 100 \pmod{251}$．よって，$x = 67 + 76t$ で最適値 $t = 100$ を代入すると，$x = 7667$ となる．また 251と76の最小公倍数は 19076 だから(1−17)と(1−18)を満たす一般解は，

$$(1-19) \quad x = 7667 + 19076u \quad (u \text{ は任意}).$$

次に，(1−18)を(1−16)に代入すると，

$$7667 + 19076u \equiv 73 \pmod{141}$$

これを解くと，$u \equiv 28 \pmod{141}$．よって，$x = 7667 + 19076u$ で最適値 $u = 28$ を代入すると，(1−16), (1−17), (1−18)を満たす最小正整数は $x = 541795$ となる．また19076と141の最小公倍数は2689716だから，一般解は，$x = 541795 + 2689716n$ （n は任意）である．‖

上の問題は要するに，まず(1−17)と(1−18)を満たす解を求め，次にその解と(1−16)を満たす解を求めているのである．したがって連立の合同式がいくつであろうと（それが解を持ちさえすれば）最後には必ず解けることになる．

問題 1.5 のように，３つ以上の合同式で法が全て互いに素である時には，次のような方法もある．これは「ガウス整数論」（第36条）で述べられている方法である．

【問題 1.6】7で割ると2余り，5で割ると1余り，さらに3で割ると2余る最小の正整数は何か．

【解】三つの法 7，5，3 は各々二つずつが互いに素であるからその最小公倍数は 105 である．この数を7で割った商は $s_1 = 15$，5で割った商は $s_2 = 21$，3で割った商は $s_3 = 35$ である．これらから，

$$15t_1 = 1 \ (\mathrm{mod}.\,7)$$

$$21t_2 = 1 \ (\mathrm{mod}.\,5)$$

$$35t_3 = 1 \ (\mathrm{mod}.\,3)$$

という合同式を作ってそれぞれを解くと，

$$t_1 = 1 \ (\mathrm{mod}.\,7),\quad t_2 = 1 \ (\mathrm{mod}.\,5),\quad t_3 = 2 \ (\mathrm{mod}.\,3)$$

となる．これを用いて，三つの「$s_i \times t_i \times$余り」$(i = 1,2,3)$ の和を求める．すなわち，

$$(1-20)\quad x = (15\times 1\times 2) + (21\times 1\times 1) + (35\times 2\times 2)$$

という計算をすると，$x = 191$ となる．法を 105 として，

$$x \equiv 191 \equiv 86 \ (\mathrm{mod}.\,105).$$

すなわち 86 が問題の最小の正整数解である．‖

上の解法で，(1−20) の $x = (15\times 1\times 2) + (21\times 1\times 1) + (35\times 2\times 2) = 30 + 21 + 140$を，例えば 7で割ると，21と140は割り切れるが最初の30では2余るようになっている．だから x は7で割ると2余るのである．同様に，5で割ると初めの30と最後の140は割り切れるが真ん中の21は1余り，そして3で割れば最初の30と21は割り切れるが最後の140は2余る．t_1, t_2, t_3 がそれぞれ1余るものを求めたのはそれに実際の余りを掛けるためである．こうして x は求める条件を満たす数となるのである．

ガウスや合同式というと「西洋数学」の専売のように聞こえるが，江戸時代に広く読まれた数学の書「塵劫記」に次のような問題と解答が出ている．実は 問題 1.6 はここから取ったのである．

「第十三 百五げんといふ事

▲半ばかりをきゝてかづを云事なり．先七づゝ引時，二つ残ると云．又五つひく時，一つ残ると云．又三づゝ引時，二つ残ると云時に，此半ばかりを聞て惣数を知る．

惣数八十六あるといふなり．

先七づゝ引時の半一つを，十五づゝのさん用に入，三十とおき，又五づゝ引時の半一つを，二十一と入て置．又三づゝの時の半を，一つを七十づゝのさん用にして百四十と入て，三口合百九十一有時，百にあまる時には百五はらい，のこり八十六ありといふなり．」

（引用：岩波文庫「塵劫記」1978年1月30日第３刷「新編塵劫記三目録第十三 百五げんといふ事」より）

文中，「半」とは余りのことで，要するに「7で割ると2余り，5で割ると1余り，3で割ると2余る数はいくつか」という問題 1.6と同じ問題である（解き方が同じであることがわかるように設問を同じにした）．太字で記してあるのが解 86 で，そのあとに解き方が出ている．7，5，3 の最小公倍数 105 を次々に引いていくことで解が得られることが題意のようである．

まず，7で割った時の半一つ（=2）に15を掛けのは，105を7で割った商15に対し15x≡1 (mod.105)の解が x≡**1**だから15×**1**=15を掛けるのである．よって 2×15=30．次に 5で割った時の半一つ（=1） に21をかけるのも105を5で割った商21に対し21x≡1 (mod.105)の解がx≡**1**だから．ゆえに21×**1**=21．最後に 3 で割った時の半一つ（=2）に70を掛けるのは，105を3で割った商が35で，35x≡1 (mod.105)の解がx≡**2**だから 35×**2**=70だから．2×2×35=140.

そして，この三つの数を合わせると（三口合）30+21+140=191になるが，これが100以上の時は105ずつ引いていって残った数が答えであるという．191−105=86.

注目するのは，この解法が「ガウス整数論」に出ているものと同じことである．「ガウス整数論」の出版が1801年であるのに対して，「塵劫記」の出版が1628年（寛永四年）ごろである．

「塵劫記」での解き方の最後の「3 で割った余り 2 に70を掛ける」ところで，説明なしに70を持ち出しているところは当時の読者も「ん？」と思ったことであろう．35x≡1 (mod.105)を解いて，x≡2 (mod.105)を求め，35×2=70となるところがミソである．当時の人々の数学への興味と熱意がひしひしと感じられて頼もしい．

$ax \equiv b \ (\mathrm{mod}.\ m)$ の形の合同式を x の一次合同式という．

実際に一次合同式を解くには他にも若干の約束事があり，それらを全て踏まえてこそ実用に耐えるのであるが，この小論とは目的が異なるため，以下に主だった事項を箇条書きに記すにとどめる．

1） a, b, m に共通因数 c があって，$a = a'c,\ b = b'c,\ m = m'c$ の時は，$a \equiv b \ (\mathrm{mod}.\ m)$ の両辺を c で割るとき，$a' \equiv b' (\mathrm{mod}.\ m')$ になる（前述）．

2) 合同式 $ax \equiv b \ (\mathrm{mod}.\ m)$ は，a と m が互いに素なら，ただ一つの解が存在する．a と m の最大公約数が $d > 1$ の時は，b も d で割り切れなければ解はない．b も d で割り切れる時は解は d 個ある．

(例：$4x \equiv 2 \ (\mathrm{mod}.\ 6)$ の場合には，2 で割って，$2x \equiv 1 \ (\mathrm{mod}.\ 3)$ $\therefore\ x \equiv 2 \ (\mathrm{mod}.\ 3)$．また $x \equiv 5 \ (\mathrm{mod}.\ 3)$ は法が3なら同じ解だが，もともとの法が 6 であるからこれらは別の解になる．ゆえに $x \equiv 2 \ (\mathrm{mod}.\ 6)$ 及び $x \equiv 5 \ (\mathrm{mod}.\ 6)$ の二つが $4x \equiv 2 \ (\mathrm{mod}.\ 6)$ の解である．）

3) 二つの合同式 $x \equiv a \ (\mathrm{mod}.\ m_1),\ x \equiv b \ (\mathrm{mod}.\ m_2)$ で，もし m_1, m_2 に共通因数 m があるとき，すなわち，$m_1 = m_1' m$ ，$m_2 = m_2' m$ の時には $a \equiv b \ (\mathrm{mod}.\ m)$ でなければ共通解は存在しない．

（例：$x \equiv 2 \ (\mathrm{mod}.\ 6),\ x \equiv 3 \ (\mathrm{mod}.\ 8)$ のときは，$2 \not\equiv 3 \ (\mathrm{mod}.\ 2)$ なので共通解は無い．）

4) 合同式 $ax \equiv b \pmod{m}$ で，法が素数の積 $m = pq\cdots$ のときは，まず $ax \equiv b \pmod{p}$ について解き，続いてその解をもとの合同式に代入して次には法 q について解く，…というやり方になる．

(例：$19x \equiv 1 \pmod{12}$ …(A) を解くには，$12 = 2\cdot 2\cdot 3$ であるから

① まず法を 2 に変えて $19x \equiv 1 \pmod{2}$ を解き，$x \equiv 1 \pmod{2}$ から $x = 1 + 2t_1$ と置く．

② (A) に $x = 1 + 2t_1$ を代入する．$19t_1 \equiv -9 \pmod{6}$ …(B) になるので，これもまた法を 2 に変えて解くと $t_1 \equiv 1 \pmod{2}$ になる．これから $t_1 = 1 + 2t_2$ と置く．

③ (B) に $t_1 = 1 + 2t_2$ を代入して，$19t_2 \equiv -14 \pmod{3}$ になる．これは法が 3 なのでそのままとけば良い．これを解いて $t_2 = 1 + 3t_3$ になる．

④ これで法12の素因数を尽くしたから t_3, t_2, t_1, x と順次代入を遡って $x = 7 + 12t_3$ を得る．すなわち $x \equiv 7 \pmod{12}$．これが(A)の解である．

5) 「**講義**」にさりげなく出ていることだが，合同式に「分数表記」を用いることができる[7]．例えば，$6 = 1 \pmod{5}$ という式の両辺は通常 3 では割れないが，これを次のように分数で表すことがある（もちろん，除数と法は互いに素が条件）．

$$2 = \frac{1}{3} \pmod{5}.$$

これだけでは特に分数表記の必要性は感じられないが，次のような計算問題には有効かもしれない．

(例題)

$$\begin{cases} 2x \equiv 3 \\ 5y \equiv -1 \end{cases} \pmod{7}$$

のとき，$x + y$, xy について解け．

【解】$2x \equiv 3$ から $x \equiv \frac{3}{2}$，$5y \equiv -1$ から $y \equiv -\frac{1}{5}$ だから，

$$x + y \equiv \frac{3}{2} - \frac{1}{5} = \frac{13}{10}, \quad xy \equiv \frac{3}{2}\cdot\left(-\frac{1}{5}\right) = -\frac{3}{10} \pmod{7} \quad \|$$

通常の解法では，2x≡3 から x≡5，5 y≡−1 から y≡4．よって x+y≡5+4=9≡2，xy≡5・4=20≡6 (mod.7) と解く．分数表記での解は，x+y≡13/10 であるが，これは10(x+y)≡13 のことだから，x+y≡2 と解ける．xy の方も，xy≡−3/10より，10xy≡−3 ∴ xy≡6 (mod.7) となって同じ解になる．

[7] 「**講義**」第 1 章 §6 [注意] 参照．

2．平方剰余，フェルマーの小定理

この章では p を２以外の素数とする．

ある整数 x を素数 p で割ると，必ず $0,1,2,\cdots,p-1$ のどれかが余りとなる．これら p 個の余りを「p **の剰余類**」と呼ぼう．これに対して x^2 や x^3 ,…を p で割れば，当然 p の剰余類の中のどれかが剰余になるが，その中のいくつかは現れないことがある．よって x の累乗数を p で割る場合には p の剰余類の中で x の累乗数に対して剰余となるものとならないものを区別する必要がある．

一般に，n 次の合同式，

$$x^n \equiv a \pmod{p}$$

に解があるならば，a を「n べき剰余[8]」という．解がないならば，a は「非剰余」であるという．0 は常に n べき剰余である．

特に，次数が２のとき，

$$x^2 \equiv a \pmod{p}$$

に解があれば，a を（p の）「**平方剰余**」，なければ「**平方非剰余**」という．

【問題 2.1】法が３のときの 0 以外の平方剰余を求めよ．また平方非剰余を求めよ．

【解】整数を３で割った時の余り 0,1,2 で類別すると，$3n$，$3n+1$，$3n+2$．これらを二乗すると，$(3n)^2 = 3\cdot 3n^2$，$(3n+1)^2 = 3(3n^2+2n)+1$，$(3n+2)^2 = 3(3n^2+4n+1)+1$．ゆえにこれらを３で割った時の余りは，0 以外には 1だけである．よって平方剰余は１，すなわち3で割った時の余りが１の整数全て．平方非剰余は２，すなわち余りが２の整数全てとなる．合同式で表せば，$x^2 \equiv a \pmod{3}$ の平方剰余は $a \equiv 1 \pmod{3}$，平方非剰余は $a \equiv 2 \pmod{3}$．‖

【問題 2.2】１は（２を含む）すべての素数 p の平方剰余であることを証明せよ．

【証明】$(p+1)^2 = p(p+2)+1$ だから $(p+1)^2 \equiv 1 \pmod{p}$．‖

（例）p=5の時，$(5+1)^2=5\times 7+1$ だから，$36\equiv 1 \pmod{5}$.

素数 p の平方剰余を全て求めるには，１～$p-1$ までの整数をそれぞれ二乗し，それらを p で割った剰余を求めればよい．これらが１～$p-1$ のどれかになるのは当然だが，その個数は $p-1$ の半分，$(p-1)/2$ 個になることを次に証明する．

例えば p=11の場合，1～10をそれぞれ二乗すれば，1，4，9，16，25，36，49，64，81，100 となる．これらを11で割ると，その剰余は 1，4，9，5，3，3，5，9，4，1となるから，結局 1，4，9，5，3 の5

---

8) べきは「冪」の読み．「**講義**」が「巾」を使用しているのに準じてこの句を「かな」で用いた．

個が2個ずつ現れるだけである．これが平方剰余である，それ以外の 2，6，7，8，10 が平方非剰余である．（もちろん正確には「平方剰余は a≡1,4,9,5,3 (mod.11) 」と表さなくてはならない．）

【定理 2.1】素数の法 p の（0を除く）剰余類 $p-1$ 個のうち，平方剰余は $(p-1)/2$ 個あり，平方非剰余も $(p-1)/2$ 個である．

【証明】$(p-x)^2 = p^2 - 2px + x^2$ であるから p を法とすれば p^2，$-2px$ の項は消えて x^2 が剰余になる．ゆえに $x^2 \equiv (p-x)^2 \pmod{p}$ が成り立つ．すなわち，$x^2 \equiv a \pmod{p}$ で，もし a が平方剰余なら $a^2 \equiv (p-a)^2 \pmod{p}$ で $p-a$ も平方剰余である．a が平方剰余でなければ $p-a$ もそうでない．つまり0 以外の p の剰余 $p-1$ 個全てを調べなくても $1, 2, 3, \cdots, (p-1)/2$ の $(p-1)/2$ 個の剰余を調べれば，平方剰余のすべてが得られる．すなわち平方剰余の個数は $(p-1)/2$ 個である．
よって $1 \sim p-1$ のうちから平方剰余の $(p-1)/2$ 個を除いた残り（同じ $(p-1)/2$ 個）が平方非剰余となる．‖

n べき剰余及び平方剰余についてはこれ以上詳しく述べないが，のちに必要な公式を導くため，「フェルマーの小定理」のみ取り上げることにする．

【定理 2.3】（フェルマーの小定理[9]） p を素数，r を p と互いに素である整数とすると，

$$r^{p-1} \equiv 1 \pmod{p}.$$

【証明】整数 x を p で割った剰余類のうち，0 以外の $p-1$ 個の剰余は p と互いに素である(重要)．これら $p-1$ 個の剰余にそれぞれある整数 r を掛けると，r, $2r$, $3r$, …, $r(p-1)$ となる．これらは当然始めの $p-1$ 個の剰余たちとは違う数になるが，これらの数のそれぞれの p の剰余は必ず $1,2,\cdots,p-1$ のうちのどれかと一致し，全体としては同じものになるはずである．だから，$1,2,\cdots,p-1$ のすべての積 $(p-1)!$（$=p-1$ の階乗）と r, $2r$, $3r$, …, $r(p-1)$ のすべての積は（積としては異なるが）p で割った時の剰余は同じになる，すなわち合同になるはずである．よって，

$$r \cdot 2r \cdot 3r \cdot \cdots \cdot r(p-1) \equiv (p-1)! \pmod{p}$$
$$\therefore\ r^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$$

両辺を $(p-1)!$ で割ると，

$$r^{p-1} \equiv 1 \pmod{p}.\ \text{‖}$$

例を挙げると，

$3^{10} \equiv 1 \pmod{11}$,　$3^{10} - 1 = 59048 = 5368 \times 11$.
$10^6 \equiv 1 \pmod{7}$,　$10^6 - 1 = 999999 = 142857 \times 7$.

---

[9] フェルマーの最終定理（注 1 参照）と区別するためこう呼ばれることがある．

フェルマーの小定理はrとpが互いに素でないと成り立たない．例えば，$10^4-1=9999$は5の倍数ではない（10と5が互いに素でない）．よって $10^4\not\equiv 1 \pmod 5$．しかし，$r^{p-1}\equiv 1 \pmod p$ の両辺にrをかけて，

$$r^p \equiv r \pmod p$$

とすれば，これはいつでも成り立つ．だから，$10^4\not\equiv 1 \pmod 5$の両辺に10をかければ，$10^5\equiv 10 \pmod 5$ となって合同式が成り立つ．

フェルマーの小定理を使って，さっそく次の章で用いる重要な公式を証明しておく．

【定理 2.4】素数が$p=4n+1$の型（nは自然数）なら，-1が平方剰余になる整数が存在する．すなわち，$r^2\equiv -1 \pmod p$に解がある．

【証明】フェルマーの小定理により，$r^{p-1}\equiv 1 \pmod p$であるが，素数が$p=4n+1$の型であるから$p-1=4n$．ゆえに $r^{4n}\equiv 1 \pmod p$．つまり，

$$r^{4n}-1\equiv 0 \pmod p.$$

左辺は数式の因数分解によって，

$$r^{4n}-1=(r^2+1)(r^2-1)(r^{4(n-1)}+r^{4(n-2)}+\cdots+r^4+1)\equiv 0 \pmod p.$$

両辺を $(r^2-1)(r^{4(n-1)}+r^{4(n-1)}+\cdots+r^4+1)$ で割って，$r^2+1\equiv 0 \pmod p$．よって $r^2\equiv -1 \pmod p$となる整数rが存在する．‖

素数pが$4n+1$型であれば，$p-1$が4の倍数になるので，定理 2.1 によって平方剰余が$(p-1)/2$個得られるが，それは偶数個である．そしてその中の二個ずつが和がpになる対(ツィ)として現れる（その証明は略す）．ゆえにpが$4n+1$型であれば，（1は必ず平方剰余なので）その対である$p-1$が平方剰余となるのである．これが定理 2.4 の意味である．

例えば，素数 13 は4n+1型の素数である．13の平方剰余は，1,4,9,3,12,10 の 6 個で，このうち1と12，3と10，4と9が対になっていて和が13になる（平方非剰余2,5,6,7,8,11も対になっている）．そして 1 は必ず平方剰余であるから 1 と対になっている12が13の平方剰余である．よって $x\equiv 12-13\equiv -1 \pmod{13}$．例えば $r=5$ は $r^2\equiv -1 \pmod{13}$の解．

11のような 4n−1 の型の素数ではこれが成り立たない．11の平方剰余（前述）は 1，4，9，5，3 で，和が11になるような対は現れない．よって $r^2\equiv -1 \pmod{11}$となる r は存在しない．

3. 不定方程式 $x^2+y^2=a$

有名なフェルマーの最終定理は，「$n\geq 3$の自然数に対し，$x^n+y^n=z^n$を満たす自然数x, y, zはない」というものであるが，よく知られているように，$x^2+y^2=z^2$，すなわち $n=2$ の時には解が無数にある．これを「ピタゴラス数」と呼ぶ．

$$(x,\ y,\ z)=(3,\ 4\ ,\ 5\ ),\ (5,\ 12,\ 13\ ),\ (7,\ 24,\ 25\ ),\ (8,\ 15,\ 17\ ),\ \cdots.$$

まずはピタゴラス数を初等的な方法で求めたのち，この小論の眼目である「整数の拡張」を行ない，再度取り上げることにする．

【問題 3.1】x, yが互いに素であるとき，$x^2+y^2=z^2$を満たす自然数の組は，

$$x=m^2-n^2,\quad y=2mn,\quad z=m^2+n^2$$

であることを証明せよ．ただし，m, n は$m>n$かつ一方は偶数で一方は奇数の自然数である．

【証明】 まず，x, yが 2 以下の場合はありえないから，$x>2$, $y>2$ とする（$z\geq 3$となる）．x, yは互いに素であるから両方が偶数ということはない．ゆえに次の三つの場合が考えられる．

(1) xが奇数でyが偶数の場合には，x^2は奇数，y^2は偶数になる．したがって和z^2は奇数，ゆえにzも奇数である．そこで，$x=2s+1$，$z=2u+1$と置くと（s, u は自然数），

$$\begin{aligned} y^2&=z^2-x^2\\ &=(2u+1)^2-(2s+1)^2\\ &=4(u+s+1)(u-s)\ . \end{aligned}$$

ここでy^2が平方数であるから$4(u+s+1)(u-s)$も平方数でなければならない．すなわち，

$$u+s+1=m^2,\quad u-s=n^2$$

と置ける．ここから $2s=m^2-n^2-1$ ，$2u=m^2+n^2-1$ が出てくる．よって，

$$x=2s+1=m^2-n^2$$

$$z=2u+1=m^2+n^2$$

また，$y^2=4(u+s+1)(u-s)=4m^2n^2$から，

$$y=2mn$$

となる．$x=m^2-n^2>0$でなければならないから，$m>n$．またxは奇数であるから，

$$x=m^2-n^2=(m+n)(m-n)$$

が奇数になるためには，m, n の一方は奇数で一方は偶数でなければならない．

(2) yが偶数でxが奇数の場合は (1) の設定でx, y を入れ替えればよい．

(3) x, yがともに奇数の場合は，$x=2s+1$，$y=2t+1$と置くと（t も自然数），

$$x^2=(2s+1)^2=4s^2+4s+1=4(s^2+s)+1$$

$$y^2=(2t+1)^2=4t^2+4t+1=4(t^2+t)+1$$

となって，x^2, y^2はともに4で割ると1余る数になる．一方z^2はx^2, y^2の和であるから，偶数であってかつ 4 で割ると 2 余る数になるが，それは不可能である．なぜならz^2が偶数ならば z自身も偶数でなければならないが，偶数の二乗は4の倍数であって「4で割ると2余る数」にはならないからである．したがって「x, yがともに奇数」というのはありえない．‖

いささか冗漫になったが，以上が「ピタゴラス数」の求め方の初等的な証明である[10]．次に同じ問題を整数の「範囲」を広げることで考えてみよう．範囲を広げるとは，言い換えれば整数の概念を拡張するのである．

まず，普通に行われる「整数」は次のような性質を持っている．
[1] 整数どうしの和，差，積はまた整数である．
[2] 整数を素数の積に一意的に分解できる（素因数分解の一意性）．

そこで今度はこの[1][2]の性質を持つ数の集合があれば，それも「整数」と呼んでいいことにするのである[11]．そのためこれまでの普通の整数を「有理整数」と呼ぶことにし，そのすべての集合をＺとしておく．

さて，新たに設けられる「整数」として次のような集合をあげよう．

$$\left\{x+yi \mid x\in Z,\ y\in Z,\ i=\sqrt{-1}\right\}$$

これはガウスが初めて用いたもので，「**複素整数**」と（ガウス整数とも）言われている[12]．要するに，複素数$x+yi$のうち，x, yが有理整数であるものの集合である．なぜこのような数を考えるかといえば，式 $x^2+y^2=z^2$ の左辺は整数・有理数の範囲では因数分解できないが，複素数$x+yi$を使ってもいいのならば，

$$(3-1)\quad x^2+y^2=(x+yi)(x-yi)$$

のように「因数分解」できるのである．そこでこのような集合を考え，これが上記[1][2]の性質を持つことを確かめた上で新たに「整数」と認めようというのである．

まず[1]であるが，これはほとんど自明であろう．任意の複素整数を$a+bi$，$c+di$とすれば，

和，差：$(a+bi)\pm(c+di)=(a\pm c)+(b\pm d)i$

積：$(a+bi)(c+di)=(ac-bd)+(ad+bc)i$．

右辺の結果は明らかに複素整数である．

---

10) もちろんこれが唯一の証明ではない．

11) 現在では整数の性質を抽象化した集合を「環」と呼ぶが，この小論ではそこには立ち入らない．

12) Wikipediaには，複素整数は「今日ではこの呼称は一般的ではない」と出ている（「ガウス整数」の項参照）が，本論では「**講義**」に即しているのでこの用語を用いている．.

次に [2] については，しばらくはその成立を前提として，問題 3.1 を考えるにあたって必要な複素整数独自の性質をいくつか取り上げる．複素整数の有効性を知ってこそ整数の概念拡大の意味が理解されるからである． [2] の証明は次章で取り上げられる．

上記の複素整数の集合は，いわば有理整数の集合Zに虚数単位iを「付け加えた」ものと考えられるので，記号として$Z[i]$が用いられる．

$$Z[i]=\left\{x+yi \mid x\in Z,\ y\in Z,\ i=\sqrt{-1}\right\}.$$

注意すべきことは，Zと$Z[i]$とは，集合としては$Z\subset Z[i]$という関係にあり，有理整数とは複素整数$x+yi$において$y=0$の場合のこととするのである．この意味で，複素整数は有理整数の拡張になっている．

$x^2+y^2=z^2$は，これまでは有理整数の等式として見てきたが，これからは複素整数の等式として見ることにより，前述 (3−1) のように因数分解される．左辺右辺を逆にすれば，

$$(x+yi)(x-yi)=x^2+y^2.$$

これは二つの複素整数の積が有理整数になったものと見ることができる．この$x+yi$および$x-yi$のように実数部は同じ，虚数部は符号だけが逆になっている複素数を互いに「共役（複素）数」という．複素数αの共役数を一般に$\overline{\alpha}$で表す．$\alpha=x+yi$のとき，$\overline{\alpha}=\overline{x+yi}=x-yi$．その積$\alpha\overline{\alpha}$を複素数$\alpha$の「**ノルム**」と呼び，記号 $|\alpha|^2$,$N\alpha$, $N(x+yi)$ 等で表す[13]．

$$\alpha\overline{\alpha}=|\alpha|^2=N(x+yi)=N(x-yi)=x^2+y^2.$$

ノルムについては，$\overline{\alpha+\beta}=\overline{\alpha}+\overline{\beta}$, $\overline{\alpha\beta}=\overline{\alpha}\,\overline{\beta}$ が成り立つ．

有理整数aを複素整数と見るとき，$a=a+0\cdot i$の共役数は$a-0\cdot i=a$である．

ノルムは複素数一般では実数であるが，複素整数のノルムは常に有理整数である．また，有理整数aのノルムは，$Na=(a+0\cdot i)(a-0\cdot i)=a^2+0^2=a^2$である．

なお，「**講義**」に倣い，以後は複素整数にはギリシア小文字$\alpha,\beta,\cdots$を，有理整数にはアルファベット小文字$a,b,c,\cdots,x,y,\cdots$等を用いることにする．

ノルムについては次の性質が重要である．

【定理 3.1】二つの複素整数をα，βとする時，

$$N(\alpha\beta)=N\alpha\cdot N\beta.$$

【証明】$\alpha=x_1+y_1i$，$\beta=x_2+y_2i$ とする．

$$\text{左辺}=N(\alpha\beta)=N\left((x_1x_2-y_1y_2)+(x_1y_2+x_2y_1)i\right)=(x_1x_2-y_1y_2)^2+(x_1y_2+x_2y_1)^2$$
$$=x_1^2x_2^2+x_1^2y_1^2+x_2^2y_1^2+y_1^2y_1^2$$

---

13) ノルムは，いわゆる複素数平面上では，原点と複素数の表す点の距離の二乗で表される．

右辺＝$N\alpha\cdot N\beta=(x_1^2+y_1^2)\cdot(x_2^2+y_1^2)=x_1^2x_2^2+x_1^2y_1^2+x_2^2y_1^2+y_1^2y_1^2$.

よって，$N(\alpha\beta)=N\alpha\cdot N\beta$．‖

定理 3.1 より，$\alpha=\beta\gamma$ なら$N\alpha=N(\beta\gamma)=N\beta\cdot N\gamma$．

定理 3.1 を繰り返し用いることで三つ以上の複素整数の積においても，

$$N(\alpha\beta\gamma\cdots)=N\alpha\cdot N\beta\cdot N\gamma\cdots.$$

$\alpha=\beta\gamma$ のとき，α をβの「倍数」，βをαの「約数」という（γも同様）．β,γをαの「因数」ということもある．当然，公約数・公倍数も存在する．さらに最大公約数や最小公倍数も次のように定義される．

【定義 3.1】複素整数α,βの共通の約数を公約数といい，公約数の中でノルムの最も大きいものを最大公約数という．また，共通の倍数を公倍数といい，そして公倍数の中でノルムの最も小さいものを最小公倍数という．

例：3+i=(1–i)(1+2i)，5+i=(1–i)(2+3i) の最大公約数は 1–i，積 14+8i=(1–i)²(1+2i)(2+3i) は公倍数の一つ，そして 3+11i=(1–i)(1+2i)(2+3i)は最小公倍数である．ちなみにそれぞれのノルムは|3+i|²=10，|5+i|²=26，積のノルムは|14+8i|²=196+64=260，最小公倍数のノルムは|3+11i|²=9+121=130 である．

複素整数の因数分解で，それが一意的に「素因数分解」できることを示すには，複素整数における「素数」を説明する必要があるが，そのために「単数」を定義しなくてはならない．

【定義 3.2】複素整数において，1 の約数となる四つの数（$\pm1,\pm i$）を「単数」という．任意の二つの整数においてその商が単数の場合，その二つの整数を互いに「同伴数」という．

単数はεで表される．$\varepsilon=\pm1,\pm i$．もし$\varepsilon=i$ならば，$Ni=N(0+1\cdot i)=0^2+1^2=1$である．他の単数も同様．$\varepsilon$がどれでも $N\varepsilon=1$．単数どうしは互いに同伴数である．一般の複素整数に単数を掛ければ「別の」複素整数になるが，ノルムは変わらない．$N(1+2i)=5$，$N(i(1+2i))=N(-2+i)=5$．一般に，$N\{\varepsilon(a+bi)\}=N\varepsilon\cdot N(a+bi)=1\cdot(a^2+b^2)=a^2+b^2$．

単数以外に公約数をもたない複素整数を**互いに素**という．

有理整数の場合と同様に，複素整数についても次の定理が成り立つ．

【定理 3.2】複素整数α,βの最大公約数をM (ミュー)，最小公倍数をΛ (ラムダ)とすると，

$$\alpha\beta=\mathrm{M}\Lambda.$$

【証明】Λはα,βの公倍数であるから，$\Lambda=\alpha\beta'=\beta\alpha'$．$\alpha,\beta$の積$\alpha\beta$は最小公倍数の倍数だから$\alpha\beta=\delta\Lambda$とおける．$\Lambda$に代入してまず$\alpha\beta=\delta\beta\alpha'$から$\alpha=\delta\alpha'$，同様に$\alpha\beta=\delta\alpha\beta'$から

$\beta=\delta\beta'$．すなわちδはα, βの公約数，したがって最大公約数Mの約数であるから，$\mathrm{M}=\delta\mu$とおける．すると$\alpha=\delta\alpha'$は$\mathrm{M}=\delta\mu$で割り切れるからα'はμで割り切れる．同様に$\beta=\delta\beta'$も$\mathrm{M}=\delta\mu$で割り切れるからβ'もμで割り切れる．よって，$\alpha'=\mu\alpha''$，$\beta'=\mu\beta''$．これを$\Lambda=\alpha\beta'=\beta\alpha'$に代入すれば，

$$\Lambda=\alpha\mu\beta''=\beta\mu\alpha''.$$

ここでもし$|\mu|>1$とすればΛが単数以外の複素整数μで割り切れることになり，

$$\Lambda/\mu=\alpha\beta''=\beta\alpha'',\quad |\Lambda/\mu|<|\Lambda|$$

となってノルムが最小公倍数Λよりも小さいΛ/μがα, βの公倍数となるので，不合理．ゆえに$|\mu|=1$，すなわち$\mu=\varepsilon$（単数）でなければならない．よって$\mathrm{M}=\delta\mu$より$\mathrm{M}=\varepsilon\delta$．ゆえに$\varepsilon\mathrm{M}=\delta$．$\varepsilon\mathrm{M}$とMは同伴数だから$\varepsilon$を適当に選ぶことで同一視できる．ゆえに$\delta=\mathrm{M}$として$\alpha\beta=\delta\Lambda$より$\alpha\beta=\mathrm{M}\Lambda$．‖

有理整数においても ab=(最大公約数)×(最小公倍数）の証明はだいたい同じ．美しい性質であるが，証明はなかなか難しい．

有理整数と同様，複素整数でも多くの性質を定理 3.2から導くことができるが，実用的であることでは「**講義**」にも頻繁に出てくる次の定理の方が便利である．

【定理 3.3】互いに素である複素整数α, βについて，βと任意の複素整数γとの積$\beta\gamma$がαで割り切れるならば，γがαで割り切れる．

【証明】α, βが互いに素であるから定理 3.2 で$\mathrm{M}=\varepsilon$と置けば，その最小公倍数は積$\alpha\beta$である．仮定により$\beta\gamma$がαの倍数だから$\beta\gamma$はα, βの公倍数である．ゆえに$\beta\gamma$は$\alpha\beta$の倍数である．よって$\beta\gamma=\alpha\beta\cdot\mu$．両辺を$\beta$で割れば$\gamma=\alpha\cdot\mu$．すなわち$\gamma$が$\alpha$で割り切れる．‖

さて，素数とは，有理整数では，２以上の整数で1 と自分以外に約数を持たない正整数のことである．これが無限に存在することは古代ギリシアの時代から知られていた[14]．

2，3，5，7，11，13，17，19，23，29，31，37，41，43，47，53，59，61，….

これに倣って複素整数における素数は次のように定義される．

【定義 3.3】複素整数において，ノルム２以上の整数で単数と自分以外に約数を持たない数を素数という．単数は素数とはしない．

複素整数における素数はどのようにして判定すればよいかを見てみよう．

有理整数の最初の素数 2 は複素整数としては素数とはいえない．なぜなら，

---

[14] ユークリッド「原論」第９巻 命題20 参照．（共立出版株式会社 昭和46年7月30日 初版１刷発行　訳・解説 中村幸四郎，寺坂英孝，伊東俊太郎，池田美恵 ）

$$(3-2)\quad 2=(1+i)(1-i)$$

のように「因数分解」されるからである．つまり２は二つの互いに共役数である整数の積で表される．では，２の約数 $1+i$, $1-i$ は素数であろうか．例えば，$1+i=-i(-1+i)$，$1-i=-i(1+i)$ などが考えられるが，これは単数×同伴数に過ぎない．

複素整数の素数については，次の二つの定理が重要である．

【定理 3.4】複素整数の素数 π は有理素数 p の約数である．

【証明】π を複素整数における素数とする．π で割り切れる有理整数が存在するから（π とその共役数 $\overline{\pi}$ との積は有理整数），その中の最小のものを p とする．p が有理素数であることを示す．

π は単数ではないので $p\neq 1$．もし $p=ab$ となる有理正整数 a, b が存在すれば $1<a<p$，$1<b<p$ である．a と π の最大公約数は 1 または π であるが，もし最大公約数が π なら a は π で割り切れ，もし 1 なら $p=ab$ が π で割り切れるから b が π で割り切れなければならない（定理 3.3）．何れにしてもそれは p が最小の有理整数であることに反する．よって p は有理素数である．したがって π は有理素数の約数である．‖

【定理 3.5】複素整数 π のノルム $N\pi$ が有理素数なら，π は複素整数としても素数である．

【証明】単数も含めればどんな整数も分解は可能であるから，仮に π を二つの複素整数 κ, μ の積に分解したとして，

$$\pi=\kappa\cdot\mu$$

とする．両辺のノルムを取ると，

$$N\pi=N(\kappa\cdot\mu)=N\kappa\cdot N\mu \quad \text{（定理 3.1）．}$$

このとき，κ, μ のどちらも単数でなければ，ノルム $N\kappa$, $N\mu$ はいずれも 1 より大きい有理整数になり，したがって $N\pi$ は有理素数ではないことになる．この対偶をとると，$N\pi$ が有理素数ならば，κ, μ のどちらかは単数になり，したがって π は複素整数としても素数である．‖

定理 3.3によれば，$N(1+i)=2$，$N(1-i)=2$ であることから，$1+i$，$1-i$ は複素整数として素数である．そのほか，$2+3i$（ノルム13），$1-4i$（ノルム17）等も素数である．一方，$3+i$ や $5+i$ は，

$$3+i=(1-i)(1+2i),\ \text{ノルム}\ N(3+i)=3^2+1^2=10=2\times 5$$

$$5+i=(1-i)(2+3i),\ \text{ノルム}\ N(5+i)=5^2+1^2=26=2\times 13$$

のように複素素数の積に分解される．素因数分解の一意性を前提にしているので，これらは唯一の分解としてよい（同伴数による分解は無視する）．ノルムも合成数になっている．このようにして複素整数における素数が決定される．

単数と自分以外の約数を持つ複素整数を「（複素）合成数」と呼ぶことにする．

有理整数で 2 の次の素数は 3 である．3 を複素整数と考えて，3 を割り切る複素整数を α とし，商を κ とすると $3=\alpha\cdot\kappa$ と書ける．3 のノルムは，$N(3+0\cdot i)=3^2+0^2=9$．よって，

$$N(3)=N(\alpha\kappa)=N\alpha\cdot N\kappa$$
$$\therefore\ 9=N\alpha\cdot N\kappa$$

ここで，$N\alpha,\ N\beta$ は有理整数であるから，$N\alpha=3,\ N\beta=3$ または $N\alpha=9,\ N\beta=1$ であるが，前者は $\alpha=x+yi$（$x,\ y$ は有理整数）としたとき，$N\alpha=x^2+y^2=3$ でなければならないので不可能．よって $N\alpha=9$，$N\beta=1$ でなければならない．すなわち，3 は複素整数としては単数でしか割り切れないので素数である．2 は複素整数として因数分解できるのに，3 はできないのである．このように，有理素数には，複素整数として因数分解できるものとできないものがある．

【定理 3.6】有理素数 p が，互いに素である二つの有理整数の二乗の和で表されるならば，p は 2 または $4n+1$ の型の素数である．

【証明】まず，$2=1^2+1^2$ であるから，1 と 1 は互いに素とすれば成り立つ．

次に $p\neq 2$ とする．互いに素である二つの有理整数を $x,\ y$ とすれば，①一方は偶数，他方は奇数，または②両方とも奇数の場合がある．

① 一方は偶数，他方は奇数ならば，$x=2s$，$y=2t+1$ とおけるから，

$$p=x^2+y^2=(2s)^2+(2t+1)^2=4(s^2+t^2+t)+1.$$

ゆえに p は $4n+1$ の型でなければならない．

② 両方とも奇数の場合，$x=2s+1$，$y=2t+1$ とおけば

$$p=x^2+y^2=(2s+1)^2+(2t+1)^2=2(2s^2+2s+2t^2+2t+1)$$

となって p は素数ではあり得ない．

以上の結果，互いに素である二つの有理整数の二乗の和で表される素数は，2 または $4n+1$ の型の素数である．‖

定理 3.6 の対偶を取れば，

【定理 3.6.1】有理素数 p が 2 でも $4n+1$ の型でもない場合には，p を互いに素である二つの有理整数の二乗の和で表すことはできない．

有理素数のいくつかを複素整数として見てみよう．

① 2 または $4n+1$ 型の素数は，

$2=1^2+1^2=(1+i)(1-i)$，

$5=4\times 1+1=1^2+2^2=(1+2i)(1-2i)$

$13=4\times 3+1=2^2+3^2=(2+3i)(2-3i)$

② 複素整数としても素数であるもの：3，7，11，…

定理 3.6 は逆も成り立つ．すなわち，

【定理 3.5】有理素数 p が，2または $4n+1$ 型であれば，$p=x^2+y^2$ が成り立つような，互いに素である有理正整数 x, y の組がただ一通りある．

【証明】まず，$p=2$ は，$2=1^2+1^2$ であるから有理整数の二乗の和で表される（1 と 1 は互いに素とする）．

次に，p が $4n+1$ 型の素数であれば，前章の定理 2.2 により合同式 $r^2\equiv -1 \pmod{p}$ の解となる有理整数 r が存在する．$r^2+1=0 \pmod{p}$ すなわち $r^2+1=mp$ となる有理整数 r がある（m は有理整数）．左辺を複素整数で因数分解すると，

$$(3-3)\quad (r+i)(r-i)=mp$$

つまり，p が $4n+1$ 型の有理素数であれば，等式 (3−3) が成り立たなければならない．

ここで $r-i$ と p の複素数としての最大公約数を γ とすれば，γ は p の約数だから，まず① $\gamma=1$，次に② $\gamma=p$ の場合を調べる．

① $\gamma=1$ ならば，$r-i$ と p は互いに素となり，したがって $r+i$ と p も互いに素，よって $(r+i)(r-i)$ とも互いに素となって $r^2+1=mp$ に反する．

② $\gamma=p$ ならば，$r-i$ が p で割り切れて商が複素整数にならなければならないが，i の係数が− 1 なので，p では割り切れず，したがって不可能．

以上の結果，$\gamma=1$ でも $\gamma=p$ でも (3−3) は成り立たない．つまり，p が複素整数としても素数であるなら (3−3) は成り立たない．したがって (3−3) が成り立つためには p が互いに共役な二つの複素数の素数に分解される以外にはない．すなわち，

$$p=(x+yi)(x-yi)=x^2+y^2 \quad （x,\ y は互いに素である有理正整数）．$$

以上の結果，p が $4n+1$ の型ならば $p=x^2+y^2$ が成り立つような互いに素である x, y の組がただ一通りある．‖

例：p=5 なら，5=4×1+1，このとき r≡2 (mod. 5)．仮に(2でなくあえて) r=7とすれば，m=10．∴ $7^2+1=10\times5$, $(7+i)(7-i)=10\times5$．7–iと5の最大公約数 γ を求めると，7–i=(1+i)(2–i)²，5=(2+i)(2–i) だから，γ =2–i が存在する．

定理 3.5 の証明の特徴は，pが4n+1型なら合同式 r²≡–1 (mod. p) に解が存在することを利用し，$r-i$ が p で割り切れないことで γ =p が排除されるところが眼目である．この合同式が初学者にはややハードルが高いので何とかして避けたいと努力したができなかった．そのため前もって平方剰余についてある程度説明することが必要になった（第３章）．これを使わずしては証明できないということなのであろうか．

「**講義**」の 294 ページには「**平方剰余の相互法則**[15]**が二次整数論において基本的**」であることが述べられているが，合同式 r²≡–1 (mod. p) はこの相互法則の「**第一補充法則**」というものからの直接の帰結なのである．

---

15) 「平方剰余の相互法則」については第10章参照．

定理 3.5 では，素数としては 2 または $4n+1$ 型の素数のみが $p=x^2+y^2$ に表現されることを述べているが，当然，有理整数の合成数についても二乗の和となるものが存在する．例えば，26=13×2では，$26=1^2+5^2$ となる．また，65=5×13 については，$65=4^2+7^2=1^2+8^2$ のように二通りの二乗の和が存在するものがある．

有理合成数の二乗の和への分解については「**講義**」に明快な結論が簡潔な証明とともに述べられているが，やはり初学的とは言い難いので，ここでは多少冗漫にはなるけれども逐一順を追って説明してみよう．以下，$p\neq 2$ とする．

まず，ある有理素数 p が互いに素である有理正整数の二乗の和に分解されていることを前提とする．すなわち $p=x^2+y^2$ が成り立っているとすると，定理 3.5 によりこの p は $4n+1$ 型であり，x, y は互いに素である．p にいろいろな数をかけて「合成数」を作ってみよう．

[1] $p=x^2+y^2$ の両辺に 2 を掛けると，$2=(1+i)(1-i)$ だから，

$$\begin{aligned}2p&=2(x^2+y^2)=(1+i)(1-i)(x+yi)(x-yi)\\&=\{(1+i)(x+yi)\}\{(1-i)(x-yi)\}\\&=\{(x-y)+(x+y)i\}\{(x-y)-(x+y)i\}\\&=(x-y)^2+(x+y)^2\end{aligned}$$

通常 x, y が互いに素でも $x+y$, $x-y$ が互いに素とは限らないが，$p=x^2+y^2$ の場合には $x+y$, $x-y$ も互いに素である（【付録 1】参照）．

例：$5=2^2+1^2$ の両辺に2を掛けると，

$$2\times 5=2(2+i)(2-i)=(1+i)(2+i)(1-i)(2-i)=(2-1)^2+(2+1)^2=1^2+3^2=10.$$

[2] 2 を二個以上掛けるとどうなるか．

$p=x^2+y^2$ の両辺に 2^n $(n\geq 2)$ を掛けると，n が偶数 $n=2m$ なら，

$$2^{2m}p=2^{2m}(x^2+y^2)=(2^m x)^2+(2^m y)^2=x'^2+y'^2$$

となって，二乗の和にはなるが x', y' には 2^{2m} という共通因数があるので互いに素ではなくなる．

例：$5=2^2+1^2$ に $4=2^2$ をかけると，$2^2\times 5=2^2(2^2+1^2)=(2\times 2)^2+(2\times 1)^2=4^2+2^2$.

また，n が奇数 $n=2m+1$ でも，

$$\begin{aligned}2^{2m+1}p&=2^{2m+1}(x^2+y^2)\\&=2\{2^{2m}(x^2+y^2)\}\\&=2\{2^m x+2^m yi\}\{2^m x-2^m yi\}\\&=(1+i)(2^m x+2^m yi)(1-i)(2^m x-2^m yi)\\&=\{(2^m x-2^m y)+(2^m y+2^m x)i\}\{(2^m x-2^m y)-(2^m y+2^m x)i\}\\&=\left(2^m x-2^m y\right)^2+\left(2^m y+2^m x\right)^2\\&=2^{2m}(x-y)^2+2^{2m}(x+y)^2\end{aligned}$$

となって，やはり互いに素ではない数の二乗の和となる．

例：$5=2^2+1^2$ に $8=2^3$ をかけると，$2^3\times 5=2^2(2-1)^2+2^2(2+1)^2=2^2+6^2$.

[1]，[2]の結果より，素数pに２をかける場合は一つだけなら互いに素である有理正整数の二乗の和に分解できるが，二つ以上かけると二乗の和にはなるが互いに素ではないことになる．

[3] 次に，$p=x^2+y^2$の両辺にもう一つの$4n+1$型の素数qをかけてみよう．

qは$4n+1$型なので$q=z^2+w^2=(z+wi)(z-wi)$と分解できる（もちろん$z\pm wi$は複素素数）．ゆえに，

$$\begin{aligned}pq&=(x^2+y^2)(z^2+w^2)\\&=(x+yi)(x-yi)(z+wi)(z-wi)\\&=(x+yi)(z+wi)(x-yi)(z-wi)\\&=\{(xz-yw)+(xw+yz)i\}\{(xz-yw)-(xw+yz)i\}\\&=(xz-yw)^2+(xw+yz)^2\end{aligned}$$

または，

$$\begin{aligned}pq&=(x^2+y^2)(z^2+w^2)\\&=(x+yi)(x-yi)(z+wi)(z-wi)\\&=(x+yi)(z-wi)(x-yi)(z+wi)\\&=\{(xz+yw)+(-xw+yz)i\}\{(xz+yw)-(-xw+yz)i\}\\&=(xz+yw)^2+(-xw+yz)^2\end{aligned}$$

結果は異なったものになる．つまり，二つの$4n+1$型の素因数の積は二通りの二乗の和に分解が可能である．すなわち，各々の素因数が二つ個ずつ複素素数に分解されるので，組み合わせが2通りできるわけである．したがって$4n+1$型の素因数が三つになれば，各素因数の複素分解をそれぞれA$\overline{\text{A}}$，B$\overline{\text{B}}$，C$\overline{\text{C}}$で表せば（$\overline{\text{A}},\overline{B},\overline{C}$はA,B,Cの共役数），複素因数の組み合わせは，

$$(\text{A}\overline{\text{A}})(\text{B}\overline{\text{B}})(\text{C}\overline{\text{C}})=(\text{ABC})(\overline{\text{A}}\overline{\text{B}}\overline{\text{C}}),\ (\overline{\text{A}}\text{BC})(\text{A}\overline{\text{B}}\overline{\text{C}}),\ (\text{A}\overline{\text{B}}\text{C})(\overline{\text{A}}\text{B}\overline{\text{C}}),\ (\text{AB}\overline{\text{C}})(\overline{\text{A}}\overline{\text{B}}\text{C})$$

の４通りあることになる．それぞれが別の有理整数の二乗の和になる．その組み合わせ数は「おのおの二個ずつ三組のものから，一個ずつ取り出して三個の組を作る場合の数」であるから，

$$\frac{2^3}{2}=2^{3-1}=2^2=4$$

である．これを一般化して$4n+1$型の素因数がk個の場合は2^{k-1}通りの解があるが，その証明は数学的帰納法による（【付録３】参照）．

[4] 最後に，上記[1]～[3]の方法で$a=X^2+Y^2$（a,X,Yは有理整数）という分解ができているところに，$4n+3$型の有理素数qをかけたらどうなるであろうか．

定理 3.6.1によって，$4n+3$型の有理素数は複素整数としても素数であるから複素素数に分解することができない．よって$aq=q(X^2+Y^2)$は有理整数の二乗の和にはならない．しかしもしqの偶数乗q^{2m}を掛けるのであれば$aq^{2m}=(q^mX)^2+(q^mY)^2$となるから二乗の和に分解できる．当然，互いに素である有理整数によるものではない．

以上が有理整数の二乗の和への分解に置ける一般的結論である．これらをまとめると（「**講義**」におけるp.250の定理 4.3 と同じ）次の定理となる．

【定理 3.6】有理整数aが$4n+3$の形の素因数を含まず，素因数２を含めば，それをただ１個含むときにのみ，aを互いに素なる二つの平方数の和に分解することができる．aに含まれる互いに相異なる$4n+1$の形の素因数の数をkとすれば，分解は2^{k-1}通りにできる．

さて，ここに至っていよいよ「ピタゴラス数」に関する 問題 3.1 に，複素整数による解答を与えることにしよう．

【問題 3.1】（再掲）x, yが互いに素であるとき，$x^2+y^2=z^2$を満たす自然数の組は，

$$x=m^2-n^2,\quad y=2mn,\quad z=m^2+n^2$$

であることを証明せよ．ただし，m, nは$m>n$かつ一方は偶数で一方は奇数の自然数である．

【証明】$x^2+y^2=z^2$を複素整数の等式と考えることで，

$$x^2+y^2=(x+yi)(x-yi)=z^2$$

となるが，これは$x+yi$がz^2の約数であることを示しているから，有理整数zを複素整数として分解し，$z=(m+ni)(m-ni)=m^2+n^2$と置く（m, nは自然数）．

$$(x+yi)(x-yi)=\{(m+ni)(m-ni)\}^2=(m+ni)^2(m-ni)^2.$$

したがって，$x+yi=(m+ni)^2$，または$x+yi=(m-ni)^2$でなければならない．

$x+yi=(m+ni)^2$ならば，$x+yi=(m+ni)^2=(m^2-n^2)+2mni$．よって$x=m^2-n^2$，$y=2mn$．これは題意に適する．

一方，$x+yi=(m-ni)^2$ならば，$x+yi=(m-ni)^2=(m^2-n^2)-2mni$．よって$x=m^2-n^2$，$y=-2mn$．しかし，$m, n$は自然数だから$y<0$．これは不適当．

以上の結果，$x=m^2-n^2$，$y=2mn$．そして，$z=m^2+n^2$となる．

$x=(m+n)(m-n)>0$より$m>n$．また，もし$m=m'd$, $n=n'd$，$d>1$ならば，

$$x=m^2-n^2=(m'd)^2-(n'd)^2=d^2(m'^2-n'^2),\quad y=2mn=2\cdot m'd\cdot n'd=2m'n'd^2$$

となってx, yに共通因数$d^2>1$があることになって条件に反する．‖

これがピタゴラス数の問題に対する複素整数による解答である．有理整数のみを用いる証明と比べるとかなり簡潔に行われる．

4. 二次体の整数

複素整数の集合，

$$Z[i]=\left\{x+yi \mid x\in Z,\ y\in Z,\ i=\sqrt{-1}\right\}$$

が各要素間における加・減・乗法について閉じていることは説明済みであったが，もう一つ重要な前提があった．$Z[i]$が「整数」を名乗るには「素因数分解の一意性」が必須である．この章でこれを証明し，それを手がかりに二次体における整数を定義する．

一般に，有理数の集合をQとするとき，Qの内部では四則計算が自由に行われる（0で割ることを除く）．このように四則計算の結果がまた同じ集合に属する集合を**体**という．この意味でQを**有理数体**という．同様に実数の集合Rを実数体，複素数の集合Cを複素数体という．集合としての包含関係で言えば，$Q\subset R\subset C$である．

有理数体Qは数を要素とする体としては「最小の」体である．このQに平方因数を含まない整数mから数$\sqrt{m}$を作り，Qの要素a, bと$\sqrt{m}$から

$$a+b\sqrt{m}$$

という数の集合を考えると，これは体になる．これを二次の数体または**二次体**といい，$Q(\sqrt{m})$と表す[16]．「二次」というのは有理数を二つ用いて一つの数を表していることを示す．

$$Q\left(\sqrt{m}\right)=\left\{a+b\sqrt{m} \mid a\in Q,\ b\in Q\right\}$$

$Q(\sqrt{m})$が実際に体となることは，その要素間の加減乗除の結果がまた$Q(\sqrt{m})$の要素になることを確かめればよい[17]．要は四則の結果には$a+b\sqrt{m}$の形以外の数は出てこないのである．

有理整数の集合Zは有理数体Qの部分集合である．では，一般の二次体$Q(\sqrt{m})$の要素$a+b\sqrt{m}$のうち，a, bが整数であるものだけから一つの集合を作るとき，これらを「二次体の整数」と呼んで差し支えないであろうか．それは前にも示したように，有理整数の持つ次の性質を満たすものであれば可であり，そうでなければ不可となるであろう[18]．

（再掲）有理整数は次のような性質を持っている．
[1] 整数どうしの和，差，積はまた整数である．
[2] 整数を素数の積に一意的に分解できる（素因数分解の一意性）．

---

16) Q( )とZ[ ]の( )と[ ]は体と整数の違いを表しているつもりである．

17) 付録３を参照．

18) 「**講義**」における二次体の整数の定義はこの小論とは全く異なり，もっと深く，広く，精密である．ここでの定義は換骨奪胎も甚だしいことをご承知願いたい．

まず，[1]に関しては，$Q(\sqrt{m})$ が体であることから$Q(\sqrt{m})$ の要素どうしの加・減・乗算の結果がまた$Q(\sqrt{m})$ の要素になることは明らかである．

さしあたって$Q(\sqrt{m})$ の部分集合としての．$Z[\sqrt{m}]$ を次のように定義しておこう．

$$Z[\sqrt{m}]=\left\{a+b\sqrt{m} \mid a+b\sqrt{m}\in Q(\sqrt{m}),\ a\in Z,\ b\in Z\right\}.$$

前章で展開した複素整数$Z[i]$は$m=-1$の場合であった．二次体の整数を構成するにあたって，「素因数分解の一意性」の条件を満たすことが必須でありながら，これについては複素整数どころか有理整数についてもこれまでまだその証明を与えてはいなかった．

そこで，まず有理整数について素因数分解の一意性の成り立つことを証明しておこう．有理整数における素因数分解の一意性は「**講義**」では次のようにして証明されている[19]．すなわち，最小の正の有理整数である 4=2×2 は素因数分解の一意性が成り立っているので，それ以降の合成数についてを数学的帰納法によって証明するのである（以下は「**講義**」の証明の丸写しではない）．

【定理 4.1】有理整数の集合Z では素因数分解の一意性が成り立つ．

【証明】4=2×2 については成り立つ．ある有理合成数$a\in Z$ より小さい数までは素因数分解の一意性が成り立っているものと仮定し，a に至って初めて一意性が成り立たないものとする．したがってa には次のようにふた通りの素因数分解があることになる．

$$(4-1)\quad a=pp'p''\cdots \quad \text{または} \quad a=qq'q''\cdots,$$

$$(p,p',p'',\cdots;\ q,q',q'',\cdots \text{は素数}).$$

このとき，もし$p=q$ ならa をp で割った数（$p'p''\cdots$ または$q'q''\cdots$，a より小さい）がふた通りに素因数分解されたことになり，仮定に反する．よって$p\neq q$ である．そこで$p>q$ として$a=pp'p''\cdots$の因数のうちp をq に変えた $qp'p''\cdots$ という数を作り，(4−1) のそれぞれのa から$qp'p''\cdots$を引いたものをa' とすると明らかに$a'<a$ であるが，

$$(4-2)\quad a'=pp'p''\cdots-\ qp'p''\cdots=(p-q)p'p''\cdots$$

$$(4-3)\quad a'=qq'q''\cdots-\ qp'p''\cdots=q(q'q''\cdots-\ p'p''\cdots).$$

これはa より小さいa' がふた通りに分解されたことを示す．なぜなら，もし (4−2) の$p-q$ および(4−3) の$q'q''\cdots-\ p'p''\cdots$が素数でないならこれらをすべて素因数分解して改めて(4−2)と(4−3)を比較したとき，次の理由からこれらは明らかに異なる分解となるからである．

① もし$p-q$ と$q'q''\cdots-\ p'p''\cdots$が同じ分解となっても(4−2)の中の$p',p'',\cdots$のいずれも(4−3)の$q$ とは異なる．

② $p-q$ とq が互いの約数になることはありえない．

以上の結果，a より小さいa' がふた通りに素因数分解されたことになり，仮定に反する．よってa より小さい数までは成り立つ素因数分解の一意性がa でも成り立つ．‖

---

19) 「**講義**」補遺 2) (p411) 参照．「(Zelmeroの着想)」という但書がついている．Zelmero(ツェルメロ)はドイツの数学者．

複素整数に限らず，$Z[\sqrt{m}]$ においては有理整数のように要素を大小の順に並べることが一般にはできないため数学的帰納法を用いて一括に証明することができない．そこでまず複素整数の素因数分解の一意性の証明のみを記す．そのためには 定理 3.3 （前出，証明済）が必須となる．

【定理 3.3】（再掲）互いに素である複素整数α, β について，β と任意の複素整数γ との積$\beta\gamma$ がα で割り切れるならば，γ がα で割り切れる．

定理 3.3 の応用として次の定理を導く．これは素因数分解の一意性を直接証明するために役に立つ．

【定理 4.1】複素整数の積$\alpha\beta\gamma\cdots$ が素数π で割り切れるなら，$\alpha,\beta,\gamma,\cdots$ の少なくとも一つがπ で割り切れる．

【証明】まず$\theta=\alpha\beta$ とする．π が素数であるからα とπ の最大公約数はπ か 1 である．

最大公約数がπ なら，α はπ の倍数になるからπ で割り切れる．

最大公約数が 1 なら，α とπ は互いに素だから，$\alpha\beta$ がπ で割り切れるならβ がπ で割り切れる（定理 3.3）．よってα, β の少なくとも一方がπ で割り切れる．

次に$\theta'=\alpha\beta\gamma=\theta\gamma$ とする．θ とπ の最大公約数はπ か 1 であるから上記の論議により，θ,γ の少なくとも一つがπ で割り切れる．つまり，α,β,γ のうち少なくとも一つがπ で割り切れる．以下同様にして$\alpha\beta\gamma\cdots$ が素数π で割り切れるなら，$\alpha,\beta,\gamma,\cdots$ の少なくとも一つがπ で割り切れる（複素整数の因数の個数による数学的帰納法）．‖

定理 4.1 を用いて複素整数における素因数分解の一意性が次のようにして証明される．「二次体の整数」は（少なくとも一つは）存在するのである．

【定理 4.2】複素整数の集合$Z[i]$ では素因数分解の一意性が成り立つ．ただし各因数の順序と同伴数による違いは度外視されるものとする．

【証明】複素合成数α が次のように二通りに素因数分解されたとする．

$$\alpha=\pi\pi'\pi''\cdots=\kappa\kappa'\kappa''\cdots \quad (4\text{–}4)$$

もし二通りの分解に共通の素数があるならそれらで割って残ったもので考えることにすればよいから上記$\pi,\pi',\pi'',\cdots$；$\kappa,\kappa',\kappa'',\cdots$ は全て異なるとしてよい．

$\kappa\kappa'\kappa''\cdots$ はπ を含まないが，π で割り切れなければならない．したがって$\kappa,\kappa',\kappa'',\cdots$ のどれかがπ で割り切れなければならない（定理 4.1）．

因数の順序は無視できるのでπ で割り切れるものの一つを改めてκ とする．κ もπ も素数であるから商は単数である．ゆえに$\kappa=\varepsilon\pi$ （ε:単数）と置ける．(4–4)式のκ を$\varepsilon\pi$ に置き換えれば，

$$\alpha=\pi\pi'\pi''\cdots=\varepsilon\pi\kappa'\kappa''\cdots \quad (4\text{–}5)$$

となる．共通因数πで割ったものをα'とすれば，

$$(4-6)\quad \alpha' = \pi'\pi''\cdots = \varepsilon\kappa'\kappa''\cdots$$

$\alpha' = \varepsilon\kappa'\kappa''\cdots$は$\pi'$でも割り切れるはずだから，$\kappa', \kappa'', \cdots$のどれかで割り切れる（定理 4.1）．そこで$\kappa'$が$\pi'$で割り切れることにして$\kappa' = \varepsilon'\pi'$（$\varepsilon'$:単数）と置き，(4−6)の$\kappa'$を$\varepsilon'\pi'$に置き換えて，

$$(4-7)\quad \alpha' = \pi'\pi''\cdots = \varepsilon\varepsilon'\pi'\kappa''\cdots.$$

両辺をπで割ったものをα''とすれば，

$$(4-8)\quad \alpha'' = \pi''\cdots = \varepsilon\varepsilon'\kappa''\cdots.$$

以下同様の議論を進めていけばαの因数の個数がだんだん減っていく．このときもし因数の個数が異なっていたらそれはもともと別の数だったことになるから，因数の個数は同じでなければならない．ゆえにκの仲間は全て$\varepsilon\pi$の仲間に置き換えられるから，αのふた通りの分解は単数εの累乗を掛けただけの違いになる．εの累乗は一個のεになるから，結局ふた通りの分解は同伴数として異なるだけである．すなわち複素整数の素因数分解は順序と同伴数を度外視するならば一意的に成り立つ．‖

以上の結果，$Z[i]$は晴れて「整数」を名乗ることができるようになった．その肝要は定理 3.3 である．これが成り立てば整数であるが，成り立たなければ整数ではないのである．

他の二次体についてはどうであろうか．「**講義**」第 4 章では$Z[\sqrt{-1}]$の他に$Z[\sqrt{-3}]$やωを 1 の三乗根としたときの$Z[\omega]$などが「二次体の整数」として詳述されている[20]．これらの理論の応用によって様々な整数の難問が簡潔に解かれているのである．

しかし，「第 5 章　二次体の整数論」の章においては，素因数分解の一意性が成り立たない例として$Z[\sqrt{-5}]$が取り上げられ，例えば，

$$6 = 2\times 3 = (1+\sqrt{-5})(1-\sqrt{-5}),$$

$$21 = 3\times 7 = (1+2\sqrt{-5})(1-2\sqrt{-5}) = (4+\sqrt{-5})(4-\sqrt{-5}),$$

のように，6 や 21 が同伴数でない二通り，三通りに「素因数分解」されることが紹介されている．

こうして二次体の整数論が「行詰まりになる」（「**講義**」）ことによっていよいよイデアル論への飛躍が始まるのである．

定理 3.3 の成り立たない例は他にも$Z[\sqrt{5}]$や$Z[\sqrt{-7}]$などいくらでも挙げることができる．というより一般の二次体では成り立つことは「むしろ例外である」（「**講義**」）．

もっとも簡単な判定法は上述のように有理整数の因数分解が（同伴数でなく）二通り以上できるものがないかを探してみることである．

$$Z[\sqrt{5}] : 4 = 2\times 2 = (3+\sqrt{5})(3-\sqrt{5})$$

$$Z[\sqrt{-7}] : 16 = (3+\sqrt{-7})(3-\sqrt{-7}) = 2(1+\sqrt{-7})(1-\sqrt{-7})$$

---

20) 「講義」ではZ[√−1]，Z[√−3]，Z[ω]はそれぞれ$K(\sqrt{-1})$，$K(\sqrt{-3})$，$K(\omega)$と表現されている．

5．イデアルの定義

素因数分解の一意性が（一般には）成り立たない二次体の「整数」をなんとかしようという先人たちの努力は「**イデアル論**」の確立を持って実を結んだ．イデアルの概念は二次体のみならずさらに高次の数体における「整数」での「素因数分解」の一意性を保証するものである．だが，さしあたっては二次体の，それも $Z[\sqrt{-5}]$ に限定したイデアルを定義する．

前章の例では，$Z[\sqrt{-5}]$ において，6 という有理整数（同時に $Z[\sqrt{-5}]$ の要素でもある）が，2×3 と $(1+\sqrt{-5})(1-\sqrt{-5})$ の二通りに分解される．この四つの因数は明らかに互いに素であり，したがって「$1+\sqrt{-5}$ と $1-\sqrt{-5}$ との積 6 が 2 で割り切れるのに，$1+\sqrt{-5}$ が 2 で割り切れない」（定理 3.3 が成り立たない）ということが起きている．

「**講義**」によれば，十九世紀のドイツの数学者クンマーはこの難問を「理想数（Ideal Number）という新しい数の概念で乗り越えようとしたが，あまりに難解であったことから，この課題を受け継いだデデキントが「さらに深く問題の根底を究めて」（「**講義**」）現在のイデアルの理論が構築された，とのことである．

クンマーの着想は，あたかも x^2+1 がこれ以上因数分解されるためには「虚数」が必要であったように，$Z[\sqrt{-5}]$ における $6=2\times3$ はまだ分解が終わっていないことからこうした問題が起きているのではないかと考えたようである．そこで 2 はA，Bという二つの理想数の積からなり，3 はC，Dという二つの理想数の積からなっている，そして $1+\sqrt{-5}$ は，2 の因数である理想数Aと 3 の因数であるCの積であり，$1-\sqrt{-5}$ は理想数BとDの積であるというのである．こうすると，

$$2=\mathrm{AB},\ 3=\mathrm{CD},\ 1+\sqrt{-5}=\mathrm{AC},\ 1-\sqrt{-5}=\mathrm{BD},\ 6=\mathrm{ABCD}$$

という関係式が成り立つ．このとき，$(1+\sqrt{-5})(1-\sqrt{-5})$ は「和と差の積」であるから $6=\mathrm{ABCD}$ では無造作すぎるので，A とB は同じ，D はC の共役（理想）数 $\overline{\mathrm{C}}$ ということにすれば，

$$2=\mathrm{A}^2,\ 3=\mathrm{C}\overline{\mathrm{C}},\ 1+\sqrt{-5}=\mathrm{AC},\ 1-\sqrt{-5}=\mathrm{A}\overline{\mathrm{C}},\ 6=\mathrm{A}^2\cdot\mathrm{C}\overline{\mathrm{C}}=\mathrm{AC}\cdot\mathrm{A}\overline{\mathrm{C}}.$$

ここで，$6=\mathrm{A}^2\cdot\mathrm{C}\overline{\mathrm{C}}$ が $6=2\times3$ を表し，$6=\mathrm{AC}\cdot\mathrm{A}\overline{\mathrm{C}}$ が $(1+\sqrt{-5})(1-\sqrt{-5})$ を表している．

これはのちに読み解かれるイデアルによる「素因数分解」と同じものとなる．つまりクンマーは現在のイデアルとほとんど同じものを「発見」していたことになる．

これに対しデデキントは，「理想数」という新たな数を創出するのではなく，当時勃興していた「集合論」の理論を駆使し，二次体の「整数」のある部分集合が理想数と同じ性質を持つことを発見した．現在使われる「イデアル」という名称には「理想数」という意味合いは全くないが，この命名にはデデキントがクンマーに敬意を払っていることが表れている．

イデアルの定義について述べる前に，$Z[\sqrt{m}]$ における「倍数・約数」を定義しておく．

【定義 5.1】$Z[\sqrt{m}]$ の要素α, β $(\alpha \neq 0)$ について，

$$\beta = \alpha\gamma$$

を満たす要素$\gamma \in Z[\sqrt{m}]$が存在するとき，βをαの倍数，αをβの約数という．

定義 5.1 により，要素$\alpha \in Z[\sqrt{m}]$の倍数の集合を(α)で表すと，

$$(\alpha) = \left\{ \alpha\theta \mid \theta \in Z[\sqrt{m}] \right\}.$$

(α)には次のような性質が認められる．

[1] (α)の任意の二つの要素の和，差は(α)の要素である．

[2] $Z[\sqrt{m}]$の任意の整数と(α)の任意の要素の積は(α)の要素である．

（以下では，例えば有理整数２の倍数の集合を強調されたゴシック体の括弧でくくって**(2)**で表し，連番号の(2)と区別する．ローマ字，ギリシア文字や $\sqrt{\ }$ の着いた数は通常の( ) で表す．）

これは倍数の集合として至極当然な性質で何の違和感も不思議さもない．簡単のため$Z[\sqrt{m}]$ ではなく Z で言えば，例えば有理整数６の倍数の集合，

$$\mathbf{(6)} = \{\cdots, -12, -6, 0, 6, 12, \cdots\}$$

の中のどの二つの要素の和，差がまた**(6)**の中のいずれかの要素になることは自明であるし（性質[1]），また性質[2] では，そもそも**(6)**自身が 6 と一般整数との積の集合なのだから当然である．

この「倍数の集合」を使って 6=2×3 を表現してみよう．それぞれの倍数の集合は，

$$\mathbf{(6)} = \{\cdots, -12, -6, 0, 6, 12, \cdots\}$$

$$\mathbf{(2)} = \{\cdots, -12, -10, -8, -6, -4, -2, 0, 2, 4, 6, 8, 10, 12, \cdots\}$$

$$\mathbf{(3)} = \{\cdots, -12, -9, -6, -3, 0, 3, 6, 9, 12, \cdots\}$$

一目見て気づくことは，**(6)**は**(2)**にも**(3)**にも「含まれている」ことである．集合の包含関係を表す記号⊂によれば**(6)**⊂**(2)**，または**(6)**⊂**(3)**である．また積集合を表す記号∩を使うと，

$$\mathbf{(6)} = \mathbf{(2)} \cap \mathbf{(3)}$$

と表すこともできる．6=2×3の形に似ているともいえる．そこでこれを「**(6)**は**(2)**と**(3)**の積」と言ってしまおう．そして，**(6)**⊂**(2)**ならば「**(6)**は**(2)**で割り切れる」といい，これを持って**(2)**は**(6)**の「約数」といってしまおうというのである．さらに**(6)**⊂**(3)**であるから**(6)**は**(3)**で割り切れる，ゆえに**(3)**も**(6)**の「約数」である．ついにはこのことを「**(6)**は**(2)**と**(3)**の公倍数である」とまで言い切るのである．

これは有理整数の整除の関係を倍数の集合間の包含関係に置き換えてみたに過ぎない．いわば単なる言い換えに過ぎないのであるが，これを「拡張された整数＝二次体の整数」に持ち込んだことがデデキントの天才的着眼点であった．

しかし，「倍数」という用語に縛られている限りこの着想を持ってしても突破口は開かれない．$Z[\sqrt{-5}]$の要素 $1+\sqrt{-5}$ の倍数，例えば$2(1+\sqrt{-5})$ や$(1+\sqrt{-5})(1-\sqrt{-5})$ が $1+\sqrt{-5}$ で割り切れるといってもそこに何かの成果が得られる訳ではない．デデキントが「実数の連続性」という高度に抽象的な概念を「切断」という斬新なアイデアをもって定義したことはあまりにも有名であるが，ここでも彼は「倍数」と言わずにその性質[1] [2]のみをもって，この性質を持つ集合を「無造作に」（「**講義**」）「**イデアル**」と定義付けたのである．

数学では度々起きることであるが，ある数学的概念を究明していくつかの性質を抽出したとき，その性質を満たすものの中にもとの概念を超えるものが現れてくることがある．

有理整数の集合Zでは，一個の整数aの倍数は性質 [1][2] を持ち，逆に [1],[2]の性質を持つ集合は一個の整数の倍数となるのであるが，$Z[\sqrt{-5}]$においてはこの「逆」が成り立たない．その反例を「**講義**」にしたがって以下に掲げる．

$Z[\sqrt{-5}]$の部分集合 **A**[21]，

$$\mathbf{A}=\left\{x+y\sqrt{-5}\ \middle|\ x\equiv y\ (\mathrm{mod}.2),\ x\in Z,\ y\in Z\right\}$$

を考える．具体的にいくつか要素をあげると，

$$1+\sqrt{-5},\ 1+3\sqrt{-5},\ 2,\ 2-6\sqrt{-5},\ 4-2\sqrt{-5},\ 100+50\sqrt{-5},\ \cdots\text{等々}.$$

つまり，$x\equiv y\ (\mathrm{mod}.2)$だから$x-y$が２の倍数であるような$x+y\sqrt{-5}$ の集合である．この集合Aは上記の性質 [1][2] を満たしながら，しかし$Z[\sqrt{-5}]$のある一個の要素の「倍数」にはならないのである．性質 [1][2] を満たすことは後に説明するとして，まず有理整数 2 は$Z[\sqrt{-5}]$の要素としては$2=2+0\cdot\sqrt{-5}$ であるから$2\equiv 0\ (\mathrm{mod}.2)$ を満たすので$2\in\mathbf{A}$．一方，$1+\sqrt{-5}$ も同様に$1\equiv 1\ (\mathrm{mod}.2)$であるからやはり$1+\sqrt{-5}\in\mathbf{A}$となる．つまり 2 と$1+\sqrt{-5}$ は同じ部分集合**A**に属するのである．しかし以前に確かめたように 2 と$1+\sqrt{-5}$ は互いに素であるから（１以外の）同じ一個の数の倍数とは言えない．**A**は性質 [1][2] を満たしながら 2 と$1+\sqrt{-5}$ の両方を要素として持っているため，決してある数の倍数の集合にはならないのである．そしてこの**A**こそがイデアルなのである．

さて，**A** が性質 [1]を満たすことは次のようにして確かめられる．

$\alpha,\beta\in\mathbf{A}$で，$\alpha=x+y\sqrt{-5}$，$\beta=x'+y'\sqrt{-5}$ とする．α,β の和および差は，

$$\begin{aligned}\alpha\pm\beta&=(x+y\sqrt{-5})\pm(x'+y'\sqrt{-5})\\&=(x\pm x')+(y\pm y')\sqrt{-5}\end{aligned}$$

$\alpha\pm\beta$ がAの要素であるためには，$(x\pm x')-(y\pm y')$ が 2 の倍数でなければならないが，

$$(x\pm x')-(y\pm y')=(x-y)\pm(x'-y')$$

で，$x\equiv y,\ x'\equiv y'\ (\mathrm{mod}.2)$ であるから$x-y\equiv x'-y'\ (\mathrm{mod}.2)$，よって$\alpha\pm\beta\in\mathbf{A}$である．

次に性質[2] であるが，$Z[\sqrt{-5}]$の任意の要素を$\theta=p+q\sqrt{-5}$ とすれば，

---

21) 「**講義**」ではイデアルをイタリック大文字で表しているが，この小論ではゴシック大文字にした．

$$\alpha\cdot\theta=(x+y\sqrt{-5})(p+q\sqrt{-5})$$
$$=(px-5qy)+(qx+py)\sqrt{-5}$$

ここでも $(px-5qy)-(qx+py)\equiv 0 \pmod 2$ でなければならないが,

$$(px-5qy)-(qx+py)=p(x-y)-5qy-qx$$
$$=p(x-y)-6qy+qy-qx$$
$$=p(x-y)-q(x-y)-6qy$$
$$=(x-y)(p-q)-6qy\equiv 0 \pmod 2.$$

（この計算の最後，$x-y\equiv 0,\ -6qy\equiv 0 \pmod 2$ に注意）

よって性質 [2] においても，$\alpha\cdot\theta\in\mathbf{A}$．すなわち，$Z[\sqrt{-5}]$ の部分集合 A は性質[1][2]を満たす．これによって**A**には，２の倍数と $1+\sqrt{-5}$ の倍数の和，$2\alpha+(1+\sqrt{-5})\beta=(2\alpha+\beta)+\beta\sqrt{-5}$（$\alpha,\beta\in Z[\sqrt{-5}]$）という要素が属することになる．

こうして $Z[\sqrt{-5}]$ の部分集合の中には，性質[1][2]を満たしながらある特定の要素の倍数とならないものが存在することが確かめられた．よってこれを「倍数の集合」というわけにはいかない．そこで改めてこの「性質[1][2]」をもって「イデアルの定義」とする．

【定義 5.2】集合 $Z[\sqrt{m}]$ の部分集合 **A** で，次の性質を満たすものを**イデアル**という．

[1] **A** の要素 $\alpha,\ \beta$ の和・差はまた **A** に属する．

[2] $Z[\sqrt{m}]$ の任意の要素 θ と **A** の要素との積は **A** に属する．

定義 5.2のうち，集合 $Z[\sqrt{m}]$ とは二次体 $Q(\sqrt{m})$ の要素 $x+y\sqrt{m}$ のうち，$x,\ y$ が有理整数であるものすべての集合を表す（既出）．

$Z[\sqrt{-5}]$ のイデアル $\mathbf{A}=\left\{x+y\sqrt{-5}\ \middle|\ x\equiv y \pmod 2;\ x\in Z,\ y\in Z\right\}$ が定義 5.2 を満たしながら，特定の数の倍数ではないことをどう考えたらよいか．

（p.30の）定義 5.1で，「倍数の集合」を構成した時の条件は特定の数 $(=\alpha)$ を定めていることである．それに対し，上記の定義 5.2では特定の数を定めず，集合の要素間の条件のみを定めているのである．特定の数における整除に関してではなく，いわば整除に関する基本的原理だけを求めているのである．倍数はイデアルであるが，イデアルは倍数ではないのである．

ここで仮に，集合 $Z[\sqrt{-5}]$ の部分集合を性質 [1] だけを条件にして構成してみよう．例えば，

$$\mathrm{A}=\left\{x+x\sqrt{-5}\ \middle|\ x\in Z\right\}$$

は性質 [1] を満たす．A の各要素の和・差はまた A の要素である[22]．言い換えれば A は$1+\sqrt{-5}$の有理整数倍の集合に過ぎず，他の$Z[\sqrt{-5}]$の要素，例えば 2 などは含まれていない．したがって，いまここで必要とする（イデアルとしての）要件を満たせない．

次に，性質 [2] だけを条件としたらどうであろうか．例えば，$\{1+\sqrt{-5}\}$（要素一個だけの部分集合）として，これに性質 [2] を適用して次のような部分集合Aを構成すれば，

$$\mathrm{A}=\left\{\alpha\left(1+\sqrt{-5}\right) \mid \alpha \in Z[\sqrt{-5}]\right\}.$$

となるが，明らかにこれは$Z[\sqrt{-5}]$における$1+\sqrt{-5}$の倍数の集合にすぎない．よってこれもイデアルの要件を満たせない．ここで$\{1+\sqrt{-5}\}$の替わりに要素を二個として$\{2, 1+\sqrt{-5}\}$とし，これに性質 [2] を適用すれば，出来上がる集合は結局（$Z[\sqrt{-5}]$における） 2 の倍数の集合と$1+\sqrt{-5}$の集合との合併集合となる．しかしこの合併集合ではその要素間に何の代数的性質（加法・減法）も設定されていない（性質[1]が設定されていない）ので，例えば，$2\alpha+(1+\sqrt{-5})\beta$（$\alpha,\beta$は$Z[\sqrt{-5}]$の要素）のような数の存在が保証されない．最初の部分集合の要素の個数をもっと多く，例えばn個にしたところで，それはn個の倍数の集合の合併集合に過ぎない．

特定の数の倍数の集合の性質を極めた結果が性質[1][2]であり，今度はその性質だけを条件に集合を構成することでイデアルが生まれた．特定の数が定められていないことで制約が弱くなり，そのぶん属する要素が「増加」したのである．これがイデアルの本質である．

重要なことは，**A**に，2および$1+\sqrt{-5}$（互いに素！）がともに属していることである．$Z[\sqrt{-5}]$の部分集合としての 2 の倍数の集合=**(**2**)**を構成してもその中には$1+\sqrt{-5}$が入ってこないし，逆に$1+\sqrt{-5}$の倍数の集合=$(1+\sqrt{-5})$を構成してもそこに**(**2**)**は入ってこない．しかし，$Z[\sqrt{-5}]$の要素に$x \equiv y \pmod 2$の条件で部分集合**A**を作ると，2 や$1+\sqrt{-5}$が入ってくるのである．つまり**(**2**)**は**A**の部分集合であり，$(1+\sqrt{-5})$も**A**の部分集合である．こうして**(**2**)**$\subset$**A**が成り立ち，同様に$(1+\sqrt{-5})\subset$**A**も成り立つ．前述（p.30）の言い換えを応用すれば，**(**2**)**$\subset$**A**により**(**2**)**は**A**で「割り切れる」し，$(1+\sqrt{-5})\subset$**A**より$(1+\sqrt{-5})$は**A**で「割り切れる」のである．すなわち，**A**は**(**2**)**や$(1+\sqrt{-5})$の「約数」と言っていいことになる．さらには「**(**2**)**や$(1+\sqrt{-5})$が**A**で「割り切れる」のだから，**A**は**(**2**)**や$(1+\sqrt{-5})$の「公約数」のような性質を持つということになる．

では，**(**2**)**が**A**で割り切れるのであれば，その「商」はなんであろうか．その答えは実は**A**自身なのであるが，それを説明するためには今少しイデアルの性質を調べなければならない．また「約数」とか「公約数」などという言い換えにもちゃんとした定義を与えなくてはならない．

一般的な二次体におけるイデアル論は「**講義**」において理想的な形で述べられており，いくら

---

[22] 性質[1]だけを満たす集合は「加群」と呼ばれる代数系の一つである．

「換骨奪胎」をよしとするとしてもそれをここに略述することは筆者のような初学者には不可能である．そこで以後，二次体の「整数」を $Z[\sqrt{-5}]$ に限って論ずることでできるだけ具体例を出しながら，その中でイデアルによる「素因数分解の一意性」がどのように達成されるかを見ていくことにしよう（$Z[\sqrt{-5}]$ に限るのは，これが「整数の素因数分解の一意性」が成り立たない代表例となっているからである．これは「**講義**」でも同じである）．

6．イデアルの性質

次の定義は既出のものであるから特に説明なしに扱う．Q は有理数体，Z は有理整数全体の集合である．

【定義 6.1】二次体$Q\left(\sqrt{-5}\right)$の部分集合,

$$Z[\sqrt{-5}]=\left\{a+b\sqrt{-5} \mid a+b\sqrt{-5}\in Q(\sqrt{-5}),\ a\in Z,\ b\in Z\right\}$$

を$Q\left(\sqrt{-5}\right)$の「整数」といい，$Z[\sqrt{-5}]$の部分集合**A**で以下の二つの条件を満たすものを$Z[\sqrt{-5}]$のイデアルという.

[1] **A**の要素α, βの和・差はまたAに属する.

[2] $Z[\sqrt{-5}]$の任意の要素θとAの要素との積は**A**に属する.

前章までは Z[√m] 一般が素因数分解の一意性を保証できないことで整数を名乗ることを控えてきたが，今後はイデアル論による新しい整数論を展開することを前提に Z[√−5] を「整数」と称する.

有理整数論においても，初めから素因数分解の一意性を前提とするのではなく，素数等いくつかの議論ののち「整数論の基本定理」を導いているのと同じことである．要はイデアル論によって二次整数論に目処がたったので，晴れて初めから「整数」と名乗ることができるのである．なお，イデアルを表す集合をゴシック大文字**A**，**P**等で表す.

まず，（p.31の）定義 5.1 に従い，$Z[\sqrt{-5}]$の要素の間に「倍数・約数」の関係があることを踏まえて$Z[\sqrt{-5}]$自身が一つのイデアルであることを証明する.

【定理 6.1】$Z[\sqrt{-5}]$の整数全体は一つのイデアルである.

【証明】$Z[\sqrt{-5}]$の任意の要素αの倍数全体の集合を(α)で表す．(α)がイデアルの性質[1][2]を満たすことは明らかである．$\alpha=1$のとき，集合**(1)**は 1 と$Z[\sqrt{-5}]$の要素との積の集合なので明らかに$Z[\sqrt{-5}]$に等しい．ゆえに$Z[\sqrt{-5}]$はイデアル**(1)**である．‖

定理 6.1 内で用いたイデアル**(α)**，**(1)**を「**単項イデアル**」という．単項イデアルは倍数の集合に他ならない．ここでも有理整数の単項イデアルは強調されたゴシック体の括弧で表すことにする.

$Z[\sqrt{-5}]$の任意の要素$\alpha=x+y\sqrt{-5}$に対して，$\overline{\alpha}=x-y\sqrt{-5}$を互いに「共役数」ということや,

$$\alpha\overline{\alpha}=(x+y\sqrt{-5})(x-y\sqrt{-5})=x^2+5y^2$$

をαのノルムといい，$N\alpha$，$N(x+y\sqrt{-5})$，$|\alpha|^2$と表すことも複素整数にならうこととする．また，有理整数aを$Z[\sqrt{-5}]$に属する数と見るときには，$a=a+0\cdot\sqrt{-5}$の共役数$\bar{a}$は$a-0\cdot\sqrt{-5}=a$であり，aのノルムは$a\bar{a}=|a|^2=a^2$である．

【定理 6.2】$Z[\sqrt{-5}]$の要素α, βに対して，αの任意の整数倍とβの任意の整数倍の和からなる集合を$(\alpha,\ \beta)$で表すとき,

$$(\alpha,\ \beta)=\left\{\eta\alpha+\mu\beta \mid \eta,\mu\in Z[\sqrt{-5}]\right\}$$

は一つのイデアルである.

【証明】イデアルの性質[1][2]を満たすことを示す.

[1] $(\eta_1\alpha+\mu_1\beta)\pm(\eta_2\alpha+\mu_2\beta)=(\eta_1\pm\eta_2)\alpha+(\mu_1\pm\mu_2)\beta\in(\alpha,\ \beta)$　（複号同順）

[2] $\theta\in Z[\sqrt{-5}]$のとき，$\theta(\eta\alpha+\mu\beta)=(\theta\eta)\alpha+(\theta\mu)\beta\in(\alpha,\ \beta)$．‖

定理 6.2 を繰り返し用いて，一般に$Z[\sqrt{-5}]$の要素α_1, α_2, …,α_nから成るイデアルを,

$$(\alpha_1,\ \alpha_1,\ \cdots,\ \alpha_n)$$

で表す．$(\alpha_1,\ \alpha_1,\ \cdots,\ \alpha_n)$のようなイデアルを「$\alpha_1$, α_2, …,α_n**を生成元とするイデアル**」という．

これまで倍数の集合以外のイデアルとしては前章で紹介した

$$\mathbf{A}=\left\{x+y\sqrt{-5} \mid x\equiv y\ (\mathrm{mod}.2);\ x\in Z,\ y\in Z\right\}$$

のみであった．これに倣って他にも倍数の集合以外のイデアルを構成してみよう．**A**が条件にしたのは$x+y\sqrt{-5}$において$x\equiv y\ (\mathrm{mod}.2)$であることだったので，同じように$x\equiv y\ (\mathrm{mod}.n)$を条件にしたとき.

$$\mathbf{B}=\left\{x+y\sqrt{-5} \mid x\equiv y\ (\mathrm{mod}.n);\ x\in Z,\ y\in Z\right\}$$

はイデアルになるだろうか．これには次の定理が成り立つ.

【定理 6.3】$Z[\sqrt{-5}]$の部分集合,

$$\mathbf{B}=\left\{x+y\sqrt{-5} \mid x\equiv y\ (\mathrm{mod}.n);\ x\in Z,\ y\in Z\right\}$$

では，$n=1,\ 2,\ 3,\ 6$のとき，**B**はイデアルとなる.

【証明】$\alpha,\beta\in\mathbf{B}$で，$\alpha=x+y\sqrt{-5}$，$\beta=x'+y'\sqrt{-5}$とする．$\alpha,\beta$の和および差は,

$$\alpha\pm\beta=(x+y\sqrt{-5})\pm(x'+y'\sqrt{-5})=(x\pm x')+(y\pm y')\sqrt{-5}\quad\text{（複号同順）．}$$

このとき，$x \equiv y,\ x' \equiv y'\ (\mathrm{mod}.\ n)$より，$x \pm x' \equiv y \pm y'\ (\mathrm{mod}.\ n)$となるので$\alpha \pm \beta \in \mathbf{B}$．よって性質[1]は任意の有理正整数$n$において満たされる．

しかし，$\theta = p + q\sqrt{-5} \in Z[\sqrt{-5}]$のとき，

$$\alpha \cdot \theta = (x + y\sqrt{-5})(p + q\sqrt{-5}) = (px - 5qy) + (qx + py)\sqrt{-5}$$

であるが，$(px - 5qy) - (qx + py) = p(x - y) - q(x - y) - 6qy$となるので，ここで$n$が$-6qy$の約数であれば性質[2]も満たすが，$q$が任意の有理整数でなければならないのでそれは不可能である．
従って**B**がイデアルになるのはnが6の約数，1，2，3，6の場合だけである．‖

上の証明中，$n = 1$の場合とは「$x \equiv y\ (\mathrm{mod}.1)$」（この表現は普通使用しない）のことになるが，これはx, yは任意の有理整数であればいいということなので，結局 **B**$= Z[\sqrt{-5}]$となる．よってイデアルである．

もちろんイデアルは定理 6.3 の形のものだけではない．しかしここではあまりこだわらずに先に進むことにしよう．次にはイデアルの要素の性質を調べる．

【１】イデアルに属する有理整数について

【定理 6.4】$Z[\sqrt{-5}]$のイデアル**A**に属する全ての有理整数は，或る最小の有理正整数の有理整数倍である．

【証明】イデアル**A**が整数αを含むとすれば，αの共役数$\overline{\alpha}$が$Z[\sqrt{-5}]$に存在するから，$\alpha\overline{\alpha}$は**A**の要素である（性質[2]）．そして$\alpha\overline{\alpha}$はαのノルムであるから有理正整数である．よって**A**には有理正整数が存在する．その中の最小の有理正整数をaとする．$a + a = 2a,\ a + 2a = 3a$，…等々，aの有理整数倍は**A**の要素である（性質[1]）．このとき**A**に属する任意の有理整数nをaで割れば，

$$n = aq + r\ (0 \le r < a)$$

となる有理整数q, rが存在するが，aqはaの倍数なので$aq \in \mathbf{A}$．すると$r = n - aq \in \mathbf{A}$（性質[1]）となって$a$より小さい正の有理整数$r$が**A**の要素とならねばならない．よって$r = 0$でなければならない．すなわち$n = aq$．よって**A**に属する任意の有理整数は$a$の倍数である．‖

【２】イデアルの底，特に標準的な底について

【定理 6.5】$Z[\sqrt{-5}]$のイデアル**A**に属する整数のうち，$\sqrt{-5}$ の係数が最小の正の有理整数cであるような整数を$b + c\sqrt{-5}$とする．このとき，**A**の任意の整数$x + y\sqrt{-5}$の有理係数yはcの有理整数倍である．

【証明】**A**の任意の整数$x + y\sqrt{-5}$のyをcで割った時の商をq，余りをrとすれば，

$$y = cq + r \ (0 \le r < c)$$

となる有理整数q, rが存在する．このとき，$(x+y\sqrt{-5})-q(b+c\sqrt{-5})$という計算の結果はもちろん**A**に属するから（性質[1]），

$$\begin{aligned}(x+y\sqrt{-5})-q(b+c\sqrt{-5}) &= (x-bq)+(y-cq)\sqrt{-5} \\ &= (x-bq)+r\sqrt{-5}\end{aligned}$$

という整数が**A**に属する．ここで$r \neq 0$ならば，これはcが$\sqrt{-5}$の最小の有理正係数であることに反する．よって$r = 0$でなければならない．すなわち$y = cq$．ゆえにyはcの有理整数倍である．‖

ついでながら，**A**に属する最小の正の有理整数aに対して$a\sqrt{-5}$という数も当然**A**に属するので，cが$\sqrt{-5}$の最小の有理正係数であることから，aもcの倍数である．さらにまた，$(b+c\sqrt{-5})\sqrt{-5} = -5c+b\sqrt{-5}$も**A**に属するので$b$も$c$の倍数である．

定理 6.2によって，$Z[\sqrt{-5}]$の任意個の要素$\alpha,\beta,\gamma,\cdots$の整数倍の和からなる集合$(\alpha,\beta,\gamma,\cdots)$がイデアルになることが示されたが，ここではイデアル**A**の任意の要素が，有理正整数aと$b+c\sqrt{-5}$のそれぞれの有理整数倍で表されることになった．

一般に，イデアルに属するすべての整数が二つの整数α, βの有理整数倍の和で表されるとき，α, βをイデアル**A**の「**底**」といい，定理 6.2 の(α, β)とは異なる記号で，

$$(6\text{–}1) \quad \mathbf{A}=[\alpha, \beta]$$

と表す．さらに，特に二つの整数が定理 6.4 で求められたaと，定理 6.5 で求められた$b+c\sqrt{-5}$の有理整数倍の和で表されるとき，これをイデアルの「**標準的な底**」といい，

$$(6\text{–}2) \quad \mathbf{A}=[a, b+c\sqrt{-5}]$$

と表す（「標準的」とは，一方は（最小の）有理正整数，他方は（最小の有理正係数の）$\sqrt{-5}$という整数の二つから成る底という意味である）．

なお，定理 6.1 で，$Z[\sqrt{-5}]$がイデアル**(1)**であることを述べたが，$Z[\sqrt{-5}]$に属する任意の整数が 1 と$\sqrt{-5}$の有理整数倍の和からなっていることから，その標準的な底が$[1,\sqrt{-5}]$であることは上の議論からいって当然である．ゆえに次の等式が成り立つ．

$$Z[\sqrt{-5}]=\mathbf{(1)}=[1, \sqrt{-5}].$$

【3】原始イデアル

標準的な底で表されたイデアル，

$$\mathbf{A}=[a, b+c\sqrt{-5}]$$

では，aもbもcの倍数である．ということはcはa, bの公約数であるから，

$$a = a_0 c, \ b = b_0 c$$

となる有理整数a_0, b_0がある．ゆえに**A**は，

$$\mathbf{A}=[a_0 c, b_0 c + c\sqrt{-5}]$$

と表される．こういう時にはcを「取り出して」，

$$\mathbf{A}=c\ [a_0,\ b_0+\sqrt{-5}\,]$$

と表す．この手続きをイデアル**A**の「**原始化**[23]」といい，

$$\mathbf{A}_0=[a_0,\ b_0+\sqrt{-5}\,]$$

を**A**の「**原始イデアル**」という．よってすべてのイデアルは原始イデアルに有理整数を「掛けた」ものといえる．**(1)**はすべての単項イデアルの原始イデアルである．

イデアルの原始化はイデアルの「因数分解」ではない．例えば(6)は6の倍数の集合であるからこれを(6)=6(1)と原始化することができるが，これは(6)を「分解」したことにはならない．6(1)の 6 はイデアルではないからである．同様に(6)=2(3)とすることもできるが，これはイデアルの「分解」でもないし，原始化でもない．

【４】イデアル$\mathbf{A}=(\alpha,\beta)$を標準的な底$[a,\ b+c\sqrt{-5}\,]$で表すこと

$Z[\sqrt{-5}\,]$のイデアル**A**が (α,β) で表されている時に，これを標準的な底に変換するという問題が生ずる．その前に，この$\alpha,\ \beta$は$Z[\sqrt{-5}\,]$のどんな整数でもいいわけではなく，一定の条件が必要である．それを先に片付けよう．以下，x_1,y_1,x_2,y_2 ； p,q,r,s は有理整数とする．

【定理 6.6】$Z[\sqrt{-5}\,]$の任意の整数$\alpha,\ \beta$がイデアルの底となるための必要十分条件は，式 $\sqrt{-5}\alpha,\ \sqrt{-5}\beta$が，$\sqrt{-5}\alpha=x_1\alpha+y_1\beta,\ \sqrt{-5}\beta=x_2\alpha+y_2\beta$ の形に表されることである．

【証明】（必要条件）$\alpha,\ \beta$を標準的な底とするイデアルは$[\alpha,\ \beta]$である．定理 6.2によって $\alpha,\ \beta$を生成元とするイデアル$(\alpha,\ \beta)$が構成されれば $(\alpha,\ \beta)=[\alpha,\ \beta]$ となる．このとき$\sqrt{-5}$ は $Z[\sqrt{-5}\,]$の要素であるから，$\sqrt{-5}\alpha\in(\alpha,\ \beta)$．同様に$\sqrt{-5}\beta\in(\alpha,\ \beta)$．$(\alpha,\ \beta)=[\alpha,\ \beta]$ であるから，どちらも有理整数倍の和として$\sqrt{-5}\alpha=x_1\alpha+y_1\beta$，$\sqrt{-5}\beta=x_2\alpha+y_2\beta$と表すことができる．

（十分条件）逆に，$\alpha,\ \beta$に対して，$\sqrt{-5}\alpha=x_1\alpha+y_1\beta$，$\sqrt{-5}\beta=x_2\alpha+y_2\beta$と表されるならば，イデアル$(\alpha,\ \beta)$の要素は，$Z[\sqrt{-5}\,]$の任意の整数を$\eta,\ \mu$として$\eta\alpha+\mu\beta$の形に表されるから，$\eta=p+q\sqrt{-5}$，$\mu=r+s\sqrt{-5}$ として，

$$\begin{aligned}\eta\alpha+\mu\beta&=(p+q\sqrt{-5})\alpha+(r+s\sqrt{-5})\beta\\&=p\alpha+q\cdot\sqrt{-5}\alpha+r\beta+s\cdot\sqrt{-5}\beta\\&=p\alpha+q(x_1\alpha+y_1\beta)+r\beta+s(x_2\alpha+y_2\beta)\\&=(p+qx_1+sx_2)\alpha+(qy_1+r+sy_2)\beta\end{aligned}$$

となって，イデアル$(\alpha,\ \beta)$の任意の要素 $\eta\alpha+\mu\beta$が$\alpha,\ \beta$の有理整数倍の和の形に表された．すなわち$\alpha,\ \beta$がイデアルの底となったのである．ゆえに$(\alpha,\ \beta)=[\alpha,\ \beta]$．‖

---

23) この用語は「**講義**」にはない．筆者の造語である．

定理 6.6 は，α, β に対して$\sqrt{-5}\alpha$, $\sqrt{-5}\beta$ という要素がイデアル**A**に存在しなければ，**A**の要素を $a\alpha+b\beta$ のように有理整数倍の和として表せないということを示している．

例えば，$\alpha=7+3\sqrt{-5}$, $\beta=3+5\sqrt{-5}$ のとき，α, β が**A**の底になれるかを確かめてみよう．

$\sqrt{-5}\alpha=\sqrt{-5}(7+3\sqrt{-5})=-15+7\sqrt{-5}$ であるから $\sqrt{-5}\alpha=x\alpha+y\beta$ と置いて，α, β を代入すると，

$$\begin{aligned} x\alpha+y\beta &= x(7+3\sqrt{-5})+y(3+5\sqrt{-5}) \\ &= (7x+3y)+(3x+5y)\sqrt{-5} \end{aligned}$$

これが$-15+7\sqrt{-5}$ に等しくなければならないから，係数比較により次の連立方程式ができる．

$$\begin{cases} 7x+3y=-15 \\ 3x+5y=7 \end{cases}$$

これを解くと $x=-\dfrac{48}{13}$, $y=\dfrac{47}{13}$ となって有理整数解が得られない．ゆえに$\alpha=7+3\sqrt{-5}$，$\beta=3+5\sqrt{-5}$ は**A**の標準的な底にはなれない．

以下に例として，$\mathbf{A}=(7+3\sqrt{-5},\ 3+5\sqrt{-5})$ を標準的な底で表す手順を示す[24]．$7+3\sqrt{-5}$，$3+5\sqrt{-5}$ は上記の確かめによりそのまま標準的な底とすることはできない．

求める**A**の標準的な底を $\mathbf{A}=[a,\ b+c\sqrt{-5}]$ としよう．ここから先，x_1,y_1,x_2,y_2 は有理整数とする．

Aに属する数は，$\eta\alpha+\mu\beta$ である．ゆえに $\eta=x_1+y_1\sqrt{-5}$, $\mu=x_2+y_2\sqrt{-5}$ と置くと，それらの数は，$\alpha=7+3\sqrt{-5}$, $\beta=3+5\sqrt{-5}$ および $\alpha'=\sqrt{-5}\alpha=-15+7\sqrt{-5}$，$\beta'=\sqrt{-5}\beta=-25+3\sqrt{-5}$ と置いたとき，$\eta\alpha+\mu\beta$ は次の通りこの α, β, α', β' の有理整数倍の和で表される．

$$\begin{aligned} \eta\alpha+\mu\beta &= (x_1+y_1\sqrt{-5})\alpha+(x_2+y_2\sqrt{-5})\beta \\ &= x_1\alpha+y_1\cdot\sqrt{-5}\alpha+x_2\beta+y_2\cdot\sqrt{-5}\beta \\ &= x_1\alpha+x_2\beta+y_1\alpha'+y_2\beta' \end{aligned}$$

ここで有理整数 x_1,x_2,y_1,y_2 を適当に決めることで$b+c\sqrt{-5}$ が求められる．いま，α, β, α', β' それぞれの$\sqrt{-5}$ の係数は 3,5,7,3 で，その最大公約数は 1 （これがc）である．そこで次のような方程式から x_1,x_2,y_1,y_2 を求めることができる．

$$(6-1)\quad 3x_1+5x_2+7y_1+3y_2=1$$

一般的な解法に依るよりも有理整数を適当に当てはめて求める方が簡単である．(6−1)の例解として，$(x_1,\ x_2,\ y_1,\ y_2)=(-1,\ 0,\ 1,\ -1)$ があげられる（解は無数にある）．これによって，

$$\begin{aligned} x_1\alpha+x_2\beta+y_1\alpha'+y_2\beta' &= -(7+3\sqrt{-5})+0\cdot(3+5\sqrt{-5})+(-15+7\sqrt{-6})-(-25+3\sqrt{-5}) \\ &= (-7+0-15+25)+\underline{(-3+0+7-3)}\sqrt{-5} \\ &= 3+\sqrt{-5} \end{aligned}$$

---

24) 「講義」§ 42. の末尾の[例]を参照した．

となって$\sqrt{-5}$の係数が最も小さい整数が作られる．これが「$b+c\sqrt{-5}$」である．

もう一つのaは，α, β, α', β'各々から$\sqrt{-5}$の係数が0になるように$b+c\sqrt{-5}=3+\sqrt{-5}$の有理整数倍を引いてa_1,a_2,a_1',a_2'を求め，それらの最大公約数を求めるのである．すなわち，

$$a_1=(7+3\sqrt{-5})-3(3+\sqrt{-5})=-2$$
$$a_2=(3+5\sqrt{-5})-5(3+\sqrt{-5})=-12$$
$$a_1'=(-15+7\sqrt{-5})-7(3+\sqrt{-5})=6$$
$$a_2'=(-25+3\sqrt{-5})-3(3+\sqrt{-5})=-16$$

これらa_1,a_2,a_1',a_2'の最大公約数は2で，これがaである．よって求める**A**の標準的な底（の一つ）は，

$$\mathbf{A}=[a,\ b+c\sqrt{-5}]=[2,\ 3+\sqrt{-5}]$$

である．これはさらに簡単になる．**A**では要素間の和・差はまた**A**に属するから，$(3+\sqrt{-5})-2=1+\sqrt{-5}$も**A**の要素である．底としてはこちらの方が簡単である．よって，

$$\mathbf{A}=[2,\ 1+\sqrt{-5}]$$

これが$\mathbf{A}=(7+3\sqrt{-5},\ 3+5\sqrt{-5})$の標準的な底による表現である．この**A**は$c$が1であるからこのまま原始イデアルでもある．

上の手順のうち，x_1,x_2,y_1,y_2を求める不定方程式の解は無数にあるが，別の解で$b+c\sqrt{-5}$を求めると，例えば$(x_1,x_2,y_1,y_2)=(1,1,-1,0)$となったなら，$b+c\sqrt{-5}=25+\sqrt{-5}$となるが，次の$a$を求めるときの$a_1,a_2,a_1',a_2'$は，

$$a_1=(7+3\sqrt{-5})-3(25+\sqrt{-5})=-68$$
$$a_2=(3+5\sqrt{-5})-5(25+\sqrt{-5})=-122$$

$$a_1'=(-15+7\sqrt{-5})-7(25+\sqrt{-5})=-190$$
$$a_2'=(-25+3\sqrt{-5})-3(25+\sqrt{-5})=-100$$

となって，これらa_1,a_2,a_1',a_2'の最大公約数はやはり2で，$a=2$となる．よって$\mathbf{A}=[2,\ 25+\sqrt{-5}]$であるが，これも，$(25+\sqrt{-5})-2\times12=1+\sqrt{-5}$が**A**の要素であるから結局，$\mathbf{A}=[2,\ 1+\sqrt{-5}]$．

定理 6.6 では，$Z[\sqrt{-5}]$の任意の整数α, βがイデアルの底となるための条件を求めたが，次に$Z[\sqrt{-5}]$の整数a，$b+\sqrt{-5}$が原始イデアル $[a$，$b+\sqrt{-5}]$ の標準的な底であるための条件を求めよう．

【定理 6.8】$Z[\sqrt{-5}]$の整数a，$b+\sqrt{-5}$が，原始イデアル $[a,\ b+\sqrt{-5}]$ の標準的な底であるための必要十分条件は，$\mathrm{N}(b+\sqrt{-5})$がaで割り切れることである．（「**講義**」§42.[問題 2]）

【証明】（必要条件）原始イデアル$\mathbf{A_0}=[a,\ b+\sqrt{-5}\,]$において，$\mathrm{N}(b+\sqrt{-5}\,)=(b+\sqrt{-5})(b-\sqrt{-5})=r^2+5$ は当然有理整数であるが，$\mathbf{A_0}$に含まれる有理整数はすべてaの倍数であるから（定理 6.4）b^2+5 もaの倍数である．すなわち，$\mathrm{N}(b+\sqrt{-5}\,)$は$a$で割り切れる．

（十分条件）イデアル$(a,\ b+\sqrt{-5}\,)$が標準的な底のイデアル$[a,\ b+\sqrt{-5}\,]$であるためには，定理 6.6 により，$a\sqrt{-5}$，$(b+\sqrt{-5})\sqrt{-5}$ がそれぞれa，$b+\sqrt{-5}$ の有理整数倍の和で表されることであるが，まず，$a\sqrt{-5}$ については，a の$-b$ 倍と$b+\sqrt{-5}$ のa 倍の和：$a\sqrt{-5}=-ab+a(b+\sqrt{-5})$ で表されるから可能．

$(b+\sqrt{-5})\sqrt{-5}$ については，十分条件より$\mathrm{N}(b+\sqrt{-5}\,)$が$a$で割り切れるとして，$\mathrm{N}(b+\sqrt{-5}\,)=ac$ とおく（cは有理整数）．$\mathrm{N}(b+\sqrt{-5}\,)=b^2+5=ac$ であるから，$b^2-ac=-5$ を用いて，

$$\begin{aligned}(b+\sqrt{-5})\sqrt{-5}&=-5+b\sqrt{-5}\\&=(b^2-ac)+b\sqrt{-5}\\&=-ac+b^2+b\sqrt{-5}\\&=-ac+b(b+\sqrt{-5})\end{aligned}$$

となって$(b+\sqrt{-5})\sqrt{-5}$ がa の$-c$ 倍と$b+\sqrt{-5}$ のb 倍の和で表された．

以上の結果，定理 6.6 の条件が満たされたから，イデアル$(a,\ b+\sqrt{-5})$ は標準的な底の原始イデアル $[a,\ b+\sqrt{-5}]$ である．‖

7. イデアル論の基本定理

本章ではイデアル**A**，**B**の「積」や，イデアル**A**がイデアル**B**で「割り切れる」といった概念を定義し，ついにはイデアルが一意的に「素因数分解」されるという**イデアル論の基本定理**までを述べることを目指す．前章で述べたようにイデアルは数ではなく集合なので，素「因数」分解という表現は正しくない．それに変わる用語等も説明しなくてはならない．

【1】イデアルの積

A，**B**をそれぞれ$\alpha_1,\alpha_2,\cdots,\alpha_m$ ； $\beta_1,\beta_2,\cdots,\beta_n$ を生成元とする$Z[\sqrt{-5}]$のイデアルとする．

【定義 7.1】イデアル$\mathbf{A}=(\alpha_1,\alpha_2,\cdots,\alpha_m)$，$\mathbf{B}=(\beta_1,\beta_2,\cdots,\beta_n)$に対して，積$\alpha_i\beta_j$ $(i:1\sim m\,,\,j:1\sim n)$のすべてを生成元とするイデアルを**A**，**B**の「積」と言い，**AB**で表す．

$$\mathbf{AB}=\left(\alpha_1\beta_1,\alpha_1\beta_2,\cdots,\alpha_1\beta_n,\ \alpha_2\beta_1,\alpha_2\beta_2,\cdots,\alpha_2\beta_n,\ \cdots,\ \alpha_m\beta_1,\alpha_m\beta_2,\cdots,\alpha_m\beta_n\right).$$

イデアルの積について，交換・結合法則が成り立つことは，定義から明らかである．すなわち，イデアル**A**，**B**，**C**について，

$$\mathbf{AB}=\mathbf{BA},\quad \mathbf{A}(\mathbf{BC})=(\mathbf{AB})\mathbf{C}$$

が成り立つ．

例：単項イデアルの場合は，**(2)**，**(3)**の積は，**(2)(3)=(2×3)=(6)**．（p.30参照）

また，$\mathbf{A}=(2,\ 1+\sqrt{-5})$，$\mathbf{B}=(3,\ 1+\sqrt{-5})$ なら，

$$\begin{aligned}\mathbf{AB}&=(2,\ 1+\sqrt{-5})(3,\ 1+\sqrt{-5})\\&=(6,\ 2(1+\sqrt{-5}),\ 3(1+\sqrt{-5}),\ (1+\sqrt{-5})^2)\end{aligned}$$

であるが，$2(1+\sqrt{-5}),\ 3(1+\sqrt{-5}),\ (1+\sqrt{-5})^2$ はすべて$1+\sqrt{-5}$ の倍数であるから，

$$\mathbf{AB}=(6,\ 1+\sqrt{-5})$$

である．さらに$6=(1+\sqrt{-5})(1-\sqrt{-5})$ であるから，6も$1+\sqrt{-5}$ の倍数である．ゆえに結局，

$$【2】\ \mathbf{AB}=(1+\sqrt{-5})\,.$$

すなわち，$\mathbf{A}=(2,\ 1+\sqrt{-5})$，$\mathbf{B}=(3,\ 1+\sqrt{-5})$ の積**AB**は単項イデアル$(1+\sqrt{-5})$である．

この例からわかるように，イデアルの積**AB**のすべての要素は必ず**A**にも**B**にも属しているものである．しかしイデアルの積を集合**AB**の「共通部分」と定義することはできない．それではイデアルの性質[1][2]が保証されない．

【2】共役イデアル

【定理 7.1】イデアル$\mathbf{A}=(\alpha_1,\alpha_2,\cdots,\alpha_n)$のすべての要素の共役数からなる集合はイデアルである．

【証明】（説明を簡単にするため，要素の個数を二個に限定して議論を進めるが，n個でも同様である．）

α,β を生成元とするイデアル**A**$=(\alpha,\beta)$ の任意の要素を $\eta\alpha+\mu\beta$ とし，$\alpha=a+b\sqrt{-5}$，$\beta=c+d\sqrt{-5}$，$\eta=p+q\sqrt{-5}$，$\mu=r+s\sqrt{-5}$ とすれば，各々の共役数は，$\overline{\alpha}=a-b\sqrt{-5}$，$\overline{\beta}=c-d\sqrt{-5}$，$\overline{\eta}=p-q\sqrt{-5}$，$\overline{\mu}=r-s\sqrt{-5}$ である．このとき，

$$\begin{aligned}\eta\alpha+\mu\beta&=(p+q\sqrt{-5})(a+b\sqrt{-5})+(r+s\sqrt{-5})(c+d\sqrt{-5})\\&=(pa-5qb+rc-5sd)+(pb+qa+rd+sc)\sqrt{-5}\end{aligned}$$

一方，$\overline{\eta}\overline{\alpha}+\overline{\mu}\overline{\beta}$ は，

$$\begin{aligned}\overline{\eta}\overline{\alpha}+\overline{\mu}\overline{\beta}&=(p-q\sqrt{-5})(a-b\sqrt{-5})+(r-s\sqrt{-5})(c-d\sqrt{-5})\\&=(pa-5qb+rc-5sd)-(pb+qa+rd+sc)\sqrt{-5}\end{aligned}$$

すなわち，$\eta\alpha+\mu\beta$ の共役数は，$\overline{\eta}\overline{\alpha}+\overline{\mu}\overline{\beta}$ である．よって，$\overline{\alpha},\overline{\beta}$ を生成元とするイデアル $(\overline{\alpha},\overline{\beta})$ は**A**のすべての要素の共役数からなるイデアルである．‖

イデアル**A**のすべての要素の共役数からなるイデアルを**A**の**共役イデアル**といい，**A'**で表す．共役イデアルは一般には **A**≠**A'** であるが，**A**=**A'** と成ることもある．例えば **A**$=(2,\ 1+\sqrt{-5})$ のとき，**A'**$=(2,\ 1-\sqrt{-5})$ であるが，$2-(1+\sqrt{-5})=1-\sqrt{-5}\in$ **A** であるから **A**=**A'**．

共役イデアルについては直ちに次の定理が成り立つ．やや明快さを欠く証明内容で，これに勝る「初等的」な解答が見つけられなかったことを遺憾とする．

【定理 7.2】$Z[\sqrt{-5}]$ のイデアル**A**とその共役イデアル**A'**の積は一つの有理整数を生成元とする単項イデアルである．すなわち，**AA'**=**(**n**)**となる有理正整数 n が存在する．

【証明】イデアル**A**が有理整数 b を生成元とする単項イデアル**(**b**)**の場合は簡単である．b の共役数は $\overline{b}=b$ であるから，**A'**＝**(**b**)**．よって**AA'**=**(**b**)(**b**)=(**b^2**)**．b^2 は明らかに有理整数であるから $b^2=n>0$ が存在する．

次に，任意のイデアル**A**は $a,\ b+c\sqrt{-5}$ を標準的な底として $[a,\ b+c\sqrt{-5}]$ と表される（p.40参照）から，**A'**$=[\overline{a},\ \overline{b+c\sqrt{-5}}]=[a,\ b-c\sqrt{-5}]$ である．よって定義 7.1 により，

$$\mathbf{AA'}=(a,\ b+c\sqrt{-5})(a,\ b-c\sqrt{-5})=(a^2,\ a(b-c\sqrt{-5}),\ a(b+c\sqrt{-5}),\ b^2+5c^2)$$

となる．この四つの数のうち左端 a^2 を p，右端 b^2+5c^2 を r とし，中の二つの数の和，$a(b-c\sqrt{-5})+a(b+c\sqrt{-5})=2ab$ を r とすると，p ,q ,r は有理整数である．これら p ,q ,r の最大公約数を $n\ (>0)$ とする．言い変えれば p ,q ,r は n の倍数である．**AA'** は p ,q ,r の有理整数倍の数をすべて含んでいるから，$px+qy+rz=n$ となるような有理整数 x,y,z も存在する（付録４）．すなわち n は**AA'** の要素である．あとは**AA'** のすべての要素が n の倍数であることが示されれば **AA'**=**(**n**)**となる．

AA' を生成する四つの要素のうち，$r=b^2+5c^2$ はもちろん n の倍数である．そして $p=a^2$ も n の倍数であるから a も n の倍数である．a が n の倍数なら $a(b-c\sqrt{-5})$ および $a(b+c\sqrt{-5})$ も n の倍数である．四つの要素がすべて n の倍数であれば**AA'** の要素はすべて n の倍数である．したがって **AA'**=**(**n**)** となる．‖

定理 7.2 の証明は Z[√−5] に限ったものである．「**講義**」にはすべての二次体の整数に適合する証明が載せられているが，それをここで取り上げるには二次体の整数の定義を厳密に行わなければ不可能である．例えば，Z[√−3] の場合には上記の方法では **AA'**=(n) が証明できない．二次体の多様性に驚くばかりである．

【定義 7.2】$Z[\sqrt{-5}]$ のイデアル の積 **AA'**=**(**n**)** における有理正整数 n を，**A**(または**A'**)の**ノルム**といい，N(**A**)で表す．すなわちN(**A**)=n である．

これは定理 7.2 を根拠として，イデアルの「ノルム」を定義したのである．すなわち **AA'**=**(**n**)** と表した場合，**(**n**)** は単項イデアルであるが，このときの有理正整数 n を **A**または**A'**のノルムと称するのである．複素整数におけるノルムをイデアルに拡張したのである．

イデアルは数ではなくある構造を持った数の集合体なのであるが，以後，有理整数，複素整数に類似した様々な性質が確立されていき，ついにはイデアル論の基本定理として「素因数分解の一意性」にまで到達する．その手始めとして，ノルムについて複素数の場合に類似した次の定理が成り立つ．

【定理 7.3】N(**AB**)=N(**A**)N(**B**)

【証明】N(**AB**)とは**AB**のノルムのことだから，イデアル**J**を**J**=**AB**とすれば，**J'**=**A'B'** である．よって，

JJ'=(**AB**)(**A'B'**)=**A**(**BA'**)**B'**=(**AA'**)(**BB'**)．（イデアルでは交換法則が成り立つ．p.42）

このとき，(**AB**)(**A'B'**)=N(**AB**)，(**AA'**)(**BB'**)=N(**A**)・N(**B**)．ゆえに N(**AB**)=N(**A**)N(**B**).‖

次の定理は標準的な底で表されたイデアルのノルムの求め方を示す．

【定理 7.4】イデアル**A**=$[a,\ b+c\sqrt{-5}]$ のノルムは，N(**A**)=ac である．

【証明】**A**を原始化すれば **A**o=$c[a_0,\ b_0+\sqrt{-5}]$ である．まず，N(**A**o)を求める．

Aoの共役イデアルは **A**o'=$[a_0,\ b_0-\sqrt{-5}]$ であるから，**A**o**A**o'=**(**n**)** とおけば，

$$\mathbf{A_oA_o'}=(n)=(a_0,\ b_0+\sqrt{-5})(a_0,\ b_0-\sqrt{-5})$$

$$=(a_0^2\ ,a_0(b_0-\sqrt{-5}),\ a_0(b_0+\sqrt{-5}),\ b_0^2+5)$$

ここで，b_0^2+5 は**A**₀に属する有理整数であるから a_0 の倍数である（定理 6.4）．よって，$b_0^2+5=a_0q$ とおけば，N(**A**₀)を生成する四つの要素すべてに a_0 が共通するから，原始化によって，

$$(n)=(a_0^2\ ,a_0(b_0-\sqrt{-5}),\ a_0(b_0+\sqrt{-5}),\ a_0q)$$
$$=a_0(a_0\ ,b_0-\sqrt{-5},\ b_0+\sqrt{-5},\ q).$$

ここで，$(a_0\ ,b_0-\sqrt{-5},\ b_0+\sqrt{-5},\ q)$ はある単項イデアルになるのであるが，その生成元になる四つの要素 a_0，$b_0-\sqrt{-5}$，$b_0+\sqrt{-5}$，q は明らかに互いに素であるから，そのイデアルは(1)である．よって$(n)=a_0\ (1)=(a_0)$．すなわち，**A**₀**A**₀'=(a_0)．ゆえに，N(**A**₀)=a_0．

Aのノルム N(**A**) は原始イデアル**A**₀のノルムの c 倍となるから，

N(**A**)=ac．‖

次は，イデアルの「除法」を定義しよう．

【定義 7.3】　イデアル**A**，**B**，**C**について，**A**=**BC**が成り立つとき，「**A**は**B**で割り切れる」という．

もちろん，**A**=**BC**が成り立つとき，「**A**は**C**で割り切れる」も同様である．

イデアルの積を定義したときに述べたように，**A**=**BC**とは，**A**が**B**にも**C**にも含まれているということ，集合の包含関係でいえば，「**A**⊂**B**かつ**A**⊂**C**」ということである．

AがBで割り切れるというとAの方が「大きい」イメージがあるが，A⊂BであるからBの方が（集合としては）「大きい」のである．

イデアルの包含関係をもって「除法」というのはもちろん有理整数の整除をなぞらえているのであるが，単なる集合の包含関係A⊂Bだけでは「割り切れる」とは言わないのは当然である．あくまでA,B,Cはイデアルでなくてはならない．ただ，イデアルの除法には「剰余（余り）」の概念はない．

次は，イデアルの「除法の一意性」の証明である．

【定理 7.5】イデアル**A**，**B**，**C**について，**AB**=**AC** ならば **B**=**C** が成り立つ．

【証明】**A**が単項イデアル**A**=(α)ならば，(α)**B**=(α)**C**すなわち α**B**=α**C**であるから**B**=**C**が成り立つ．

Aが一般のイデアルならば，**AB**=**AC** の両辺に左から**A'** をかけると，

A'(AB)=**A'(AC)**　∴　**(A'A)B**=**(A'A)C**

AA'=n であるから，n**B**=n**C**．ゆえに，**B**=**C**．‖

有理整数でいう除法の一意性とは，「ab=ac ならば b=c 」のことである．すなわち「積の等しいものを同じ数で割ったときの商は等しい」というものである．これにはa≠0 という条件がある（a=0 では成り立たない）．すなわち，ab=ac <=> a(b−c)=0．ここで有理整数（一般には複素数）の重要な性質に「二数の積が 0 ならどちらかが 0 」というのがあって，これにより b−c=0 ∴ b=c となるのである．

イデアルに除法の一意性が成り立つと，任意のイデアル**A**がイデアル**B**で割り切れるための条件が求められる．それが次の定理である．

【定理 7.6】イデアル**A**がイデアル**B**で割り切れるための必要十分条件は，**A**⊂**B** となることである．

【証明】（必要条件）**A**が**B**で割り切れるとすると，**A**=**BC** であるから，定義 7.1 により**A**は**B**に含まれる．ゆえに**A**⊂**B**.

（十分条件）**A**⊂**B** とする．**A**，**B**に**B'**（**B**の共役イデアル）を右からかけると，**AB'**，**BB'** となるが，**AB'** の要素は，**A**の要素（**B**の要素でもある）に**B'**の要素をかけたものであるから明らかに **BB'** の要素でもある．ゆえに**AB'**⊂**BB'** ．このとき **BB'**=**(**n**)**となる有理整数nが存在する（定理 7.2）から，**AB'**⊂**(**n**)**.

(n**)**は有理整数nの（$Z[\sqrt{-5}]$における）倍数の集合であるから**AB'**の要素は全てnの倍数である．すなわち **AB'**=n**C** となるイデアル **C** が存在する．この両辺に右からイデアル**B**をかけると，

$$(\mathbf{AB'})\mathbf{B}=(n\,\mathbf{C})\mathbf{B} \quad \therefore\ \mathbf{A}(\mathbf{B'B})=n\,(\mathbf{CB})$$

B'B=**(**n**)**であるから，**A**(**B'B**)=**A(**n**)**=**A**n．よって，**A**n=n(**CB**)．この両辺をnで割って，**A**=**CB**．すなわち，**A**は**B**で割り切れる．‖

上記の証明で必要条件は定義 7.1から即座に出てくるが，十分条件としてイデアルの包含関係から A=CB を引き出すには，BB'=(n) が必須である．定理 7.6によって今後はA⊂Bであれば「AはBで割り切れる」または「BはAを割り切る」という言い方ができる．イデアルA,B,CでA=BCの時，Aを「倍イデアル」，B,CをAの「約イデアル」ということもある．これはもちろん「約数・倍数」になぞらえている．

Aはイデアル**(**1**)**で割り切れる，また**A**が**A**で割り切れることは当然であるが，その他のどのイデアルでも割り切れないとき，すなわち**(**1**)**と**A**以外のどのイデアルも**A**を部分集合として含まないとき，**A**を**素イデアル**という[25].

また，イデアル**A**，**B**がどちらもイデアル**C**で割り切れるとき，**C**を**A**，**B**の「**公約イデアル**」という．イデアル**(**1**)**は全てのイデアルの公約イデアルである．そして　**A**，**B**の公約イデアルが**(**1**)**以外にないとき，**A**，**B**は「**互いに素**」であるという．

以上の用語はいずれも有理整数における「素数」「公約数」や「互いに素」という用語をイデアル論に「襲用」（「**講義**」）したものである．注意すべきはイデアルは「数」ではなく，集合体であることである．イデアルが「割り切れる」とは「集合として含まれる」という意味であるから，上記の意味は以下の文章と同じ意味である．

「A⊂(1)，またA⊂Aは当然であるが，その他のどのイデアルにも含まれないとき，Aを素イデアルという．また，A,Bがどちらも**C**の部分集合であるとき，CをA,Bの公約イデアルという．すべてのイデアルはイデアル(1)に含まれている．A,Bがイデアル(1)以外のイデアルに一緒には含まれないとき，A,Bは互いに素であるという．」

以下，続いて有理整数の「最大公約数，公倍数，最小公倍数」などがイデアルにも適用される．

イデアル**A**，**B**がそれぞれ整数$\alpha_i\ (i:1\sim m)$，$\beta_j\ (j:1\sim n)$を生成元とする．

---

25) 「**講義**」では「素のイデアル」となっている．また「公約イデアル」は「公因子」となっている．

$$\mathbf{A}=(\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_m),\quad \mathbf{B}=(\beta_1,\ \beta_2,\ \cdots,\ \beta_n).$$

このとき**A**の要素α_iと**B**の要素β_jによって生成されるイデアル**M**；

$$\mathbf{M}=(\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_m,\ \beta_1,\ \beta_2,\ \cdots,\ \beta_n)$$

は，もちろん**A**，**B**の要素を全て含んでいる．すなわち**A**，**B**は**M**で割り切れる．任意のイデアル**C**がイデアル**A**，**B**の公約イデアルであるとき，**C**は必ず**M**に含まれる．つまり**C**は**M**で割り切れる．この**M**を**A**，**B**の**最大公約イデアル**という．

三つ以上のイデアルについても同様である．

A,Bの最大公約イデアルは，複素整数のときの最大公約数のようにノルムによって定義するのではない．最大公約イデアルの「最大」は有理整数の「最大公約数」の用語を「襲用」（「**講義**」）したもので，イデアルを形容する用語ではない．A,Bを含む集合体としてはいくらでも「大きい」ものを考えることができるが，最大公約イデアルMはその中で最も「小さい」ものである．

例：有理整数の単項イデアルで示せば，

(12)と(8)の最大公約イデアルは(12,8)で表される．(12,8)とは12a+8bで表される数のすべてであるが，12a+8b=4(3a+2b)でカッコの中は任意の有理整数になるので結局4の倍数．すなわち(12)と(8)の最大公約イデアルは(4).

一般のイデアルにおける例は【付録５】を参照.

次に，イデアル**C**がイデアル**A**でも**B**でも割り切れるとき，**C**を**A**，**B**の**公倍イデアル**という．「割り切れる」は「含まれる」だから，**C**⊂**A**かつ**C**⊂**B**，すなわち**C**は**A**,**B**の共通部分である．

【定理 7.7】イデアル**A**，**B**に共通する**すべての**要素からなる集合はイデアルである．またこのイデアルは**A**，**B**で割り切れる.

【証明】**A**，**B**に共通するすべての要素からなる集合を**L**とする．**L**の任意の要素をα,βとすれば，α,βはイデアル**A**，**B**共通の要素であるから$\alpha+\beta$，$\alpha-\beta$も**A**，**B**共通の要素である．よって$\alpha\pm\beta$は**L**の要素である（イデアルの性質[1]）．同様に**L**の任意の要素αの整数倍$\eta\alpha$ ($\eta\in Z[\sqrt{-5}]$)も**A**，**B**共通の要素であるから$\eta\alpha$も**L**の要素である（イデアルの性質[2]）．ゆえに**L**はイデアルである．また，上記の議論により明らかに**L**⊂**A**，**L**⊂**B**であるから，**L**は**A**，**B**で割り切れる．‖

イデアル**A**，**B**に共通する**すべての**要素からなるイデアルを**A**，**B**の**最小公倍イデアル**という．最小公倍イデアルは**A**，**B**に共通するイデアル（公倍イデアル）のうち，集合としては最も「大きい」ものとなるのだが，ここでも有理整数の用語を襲用して「最小」という.

次は基本定理に直結する重要な定理で，複素整数における定理 3.3 と同じものであるが，イデアルは数ではないので証明法は全く異なる.

【定理 7.8】$Z[\sqrt{-5}]$のイデアル**A**，**B**が互いに素で，イデアルの積**AC**が**B**で割り切れるなら，**C**が**B**で割り切れる.

【証明】**C**が**B**で割り切れるためには**C**⊂**B**であることを示せばよい．**C**の任意の要素をγとするとき，γが**B**の要素で表されることを示そう．**A**，**B**が互いに素なので**A**，**B**の最大公約イデアルは**(1)**である．つまり**A**の要素も**B**の要素もすべて**(1)**に含まれている．

$$\mathbf{(1)}=(1, \cdots, \alpha, \cdots, \beta, \cdots).$$

よって**A**の要素αと**B**の要素βで，$1=\alpha+\beta$となるものがある（イデアルの性質[1]）．

ここで**C**の要素γを$1=\alpha+\beta$の両辺に掛ければ，

$$\gamma=\alpha\gamma+\beta\gamma$$

となる．この式で，$\alpha\gamma$は**A**の要素αと**C**の要素γの積であるからイデアル**AC**の要素である．仮定により**AC**が**B**で割り切れるので**AC**⊂**B**，すなわち$\alpha\gamma$は**B**の要素である．また$\beta\gamma$は当然**B**の要素であるから和$\gamma=\alpha\gamma+\beta\gamma$も**B**の要素である．すなわち**C**⊂**B**．よって**C**は**B**で割り切れる．‖

続いて直ちに次の定理が証明される．この証明には定理 7.8が必須である．

【定理 7.9】$Z[\sqrt{-5}]$のイデアル**A**，**B**の積**AB**が素イデアル**P**で割り切れるならば，**A**または**B**が**P**で割り切れる．

【証明】**P**が素イデアルなので**A**と**P**の最大公約イデアルは**P**または**(1)**である．

もし最大公約イデアルが**P**ならば，直ちに**A**が**P**で割り切れる．

もし最大公約イデアルが**(1)**ならば，**A**，**P**は互いに素であるから定理 7.8 によって**AB**が**P**で割り切れるならば**B**が**P**で割り切れる．‖

定理 7.9 の拡張として「任意個のイデアルの積 **ABC**… が素イデアル**P**で割り切れるなら**A, B, C**，…の少なくとも 1 つが**P**で割り切れる」が成り立つことは自明である．

定理 7.9 を用いて次の「イデアル論の基本定理」が証明される．この証明は有理整数や複素整数の場合と全く同じ論法である．

【定理 7.10】（イデアル論の基本定理）**(1)**を除く$Z[\sqrt{-5}]$のイデアルは素イデアルの積に（順序を無視して）一意的に分解される．

【証明】（分解の可能性）**(1)**以外の任意のイデアルを**J**とする．**(1)**を含めれば**J**は必ず複数のイデアルの積に分解される．

$$\mathbf{J}=\mathbf{ABC}\cdots.$$

両辺のノルムを取れば，

$$\mathrm{N}(\mathbf{J})=\mathrm{N}(\mathbf{A})\cdot\mathrm{N}(\mathbf{B})\cdot\mathrm{N}(\mathbf{C})\cdot\cdots.$$

もしノルムが1となるものがあればここから取り除いておく．左辺のN(**J**)は有理整数なので右辺も有理整数の有限個の積である．**A**，**B**，**C**，…の中に素イデアルでないものがあればそれらも素イデアルの積に分解していけば，**J**は最終的に素イデアルだけの積に分解される．

（分解の一意性）仮に，**J**が次のように二通りに素イデアルの積に分解されたとする．**A,B,C,**…；**D,E,F,**…は素イデアルである．

$$\mathfrak{J}=\mathfrak{ABC}\cdots=\mathfrak{DEF}\cdots.$$

$\mathfrak{J}=\mathfrak{ABC}\cdots$より，$\mathfrak{J}$は素イデアル$\mathfrak{A}$で割り切れる．したがって$\mathfrak{J}=\mathfrak{DEF}\cdots$も$\mathfrak{A}$で割り切れるから定理 7.9 により $\mathfrak{D},\mathfrak{E},\mathfrak{F},\cdots$のいずれかは$\mathfrak{A}$で割り切れる．仮に$\mathfrak{D}$が$\mathfrak{A}$で割り切れるとすれば$\mathfrak{D}$も素イデアルであるから$\mathfrak{D}=\mathfrak{A}$となる．そこで$\mathfrak{D}$を$\mathfrak{A}$に置き換えれば，

$$\mathfrak{J}=\mathfrak{ABC}\cdots=\mathfrak{AEF}\cdots.$$

これを繰り返すことで最後には$\mathfrak{D},\mathfrak{E},\mathfrak{F},\cdots$はすべて$\mathfrak{A},\mathfrak{B},\mathfrak{C},\cdots$に置き換えられて同じものになる．よって分解は一意的である．‖

定理 7.10 が証明されて，「**イデヤル論の基礎**が成就したのである．」（「**講義**」）

8. 整数 Z[√–5]の素イデアル

前章において「イデアル論の基本定理」が証明された．それはイデアルが一意的に素イデアルの積に分解されるというものである．これを踏まえて５章の冒頭に述べた$Z[\sqrt{-5}]$の要素としての６が二通りに素因数分解されるという問題を解決する．だがその前に$Z[\sqrt{-5}]$における**素イデアル**について詳しく説明する必要がある．

【１】二種類の素イデアル

【定理 8.1】$Z[\sqrt{-5}]$における素イデアル**P**に含まれる最小の正の有理整数は素数である．

【証明】定理 6.4 により素イデアル**P**に最小の有理正整数が存在する．それをpとする．**P**はpの倍数をすべて含むから$(p)\subset$**P**．よって(p)は**P**で割り切れる．もし$p=ab$となる**P**の有理正整数$a, b\ (1<a<p, 1<b<p)$があればpは合成数で$(p)=(a)(b)$であるから，$(a)(b)\subset$**P**．すなわち$(a)(b)$が**P**で割り切れることになり，定理 7.8 により(a)または(b)が**P**で割り切れることになって**P**が素イデアルであることに反する．ゆえにpは素数である．‖

まず，$Z[\sqrt{-5}]$の素イデアルが次のように二種類に分かれることを明らかにしておこう．

上記の証明中でも述べたように，素イデアル**P**の最小の有理素数pに対して，単項イデアル(p)が**P**で割り切れるから，

$$(p)=\mathbf{PQ}$$

となるイデアル**Q**が存在する．ノルムで表せば，$N(p)=p^2$より[26]，

$$N(p)=N(\mathbf{P})\cdot N(\mathbf{Q})=p^2. \quad (8\text{–}1)$$

N(**P**)とN(**Q**)の積がp^2になるということは N(**P**)＝p または N(**P**)＝p^2 であるから，素イデアルには次の二種類がある（ **P**は素イデアルなので N(**P**)≠１）．

① **一次の素イデアル**：N(**P**)＝pの場合．定理 7.2 により**PP'**=(p)であるから，単項イデアル(p)が二つの共役イデアルの積に分解される．この場合はさらに**P**=**P'** と**P**≠**P'** に分けられる．

② **二次の素イデアル**：N(**P**)＝p^2 の場合．(8–1)式で N(**Q**)= 1 であるから，$N(p)=N(\mathbf{P})$．よって(p)=**P**．すなわち，(p)は素イデアルで，これ以上分解されない．

このように素イデアル**P**は，そのノルムが自身に含まれる最小の有理素数pに等しいときに限り単項イデアル(p)を**P**およびその共役素イデアル **P'** の積に分解する．以下，一次の素イデアルについて詳述する．

---

[26] p=p+0·√-5であるからN(p)=(p+0·√-5)(p-0·√-5)=p×p=p². N(p)とN(**P**)を混同しないこと．

【定理 8.2】$Z[\sqrt{-5}]$ におけるイデアル **P**=$[a,\ b+c\sqrt{-5}]$ が一次の素イデアルであるための必要十分条件は $b^2 \equiv -5 \pmod{p}$ である.

【証明】**P**=$[a,\ b+c\sqrt{-5}]$ を一次の素イデアルとする．定理 8.1 により p は有理素数である．定理 7.4 により N(**P**)=ac であるが **P**は一次の素イデアルであるからN(**P**)=p．よって $c=1, a=p$．ゆえに **P**=$[p,\ b+\sqrt{-5}]$．このとき，定理 6.8 により N($b+\sqrt{-5}$) は p で割り切れるから，N($b+\sqrt{-5}$) =b^2+5 より，

$$(8\text{–}2)\quad b^2+5\equiv 0 \quad \therefore\ b^2\equiv -5 \pmod{p}.$$

逆に (8–2) が成り立つとする．**P'**=$[p,\ b-\sqrt{-5}]$ であるから，

$$\begin{aligned}\mathbf{PP'} &= (p,\ b+\sqrt{-5})(p,\ b-\sqrt{-5})\\ &= (p^2,\ p(b-\sqrt{-5}),\ p(b+\sqrt{-5}),\ b^2+5).\end{aligned}$$

ここで，(8–2) より b^2+5 は p の倍数であるから結局四つの生成元はすべて p の倍数である．ゆえに **PP'**=**(** p **)**．よって，N(**P**)= p となり，**P**は一次の素イデアルである．‖

p の値をいくつか採って見よう．なお，(8–2) での b の解は複数個存在することもあるが，代表として最小の正整数をとる（臨機応変に他の値も取るものとする）．

(1) $p=2$ の場合：$b^2\equiv -5\equiv 1 \pmod{2}$ であるから，解は $b\equiv 1 \pmod{2}$．つまり b は奇数．b として最小の奇数 1 を取れば，**P**=$[2,\ 1+\sqrt{-5}]$，N(**P**)= 2．このとき，**P'**=$[2,\ 1-\sqrt{-5}]$ であるが，$2-(1+\sqrt{-5})=1-\sqrt{-5}\in$**P** であるから**P**=**P'**．よって**(** 2 **)**=**PP**=**P**^{2}と表す.

(2) $p=3$ の場合：$b^2\equiv -5\equiv 1 \pmod{3}$ であるが，このとき b は 3 の倍数以外の有理整数である．この場合の最小の有理整数 b は 1 なので，**P**=$[3,\ 1+\sqrt{-5}]$，N(**P**)= 3．よって**P'**=$[3,\ 1-\sqrt{-5}]$．この場合，**P'**の生成元の$1-\sqrt{-5}$ は**P**の要素では表せないので **P**≠**P'** である[27)].

(3) $p=5$ の場合：$b^2\equiv -5\equiv 0 \pmod{5}$ より，解は $b\equiv 0 \pmod{5}$．つまり b は 5 の倍数．この場合の最小の有理整数 b は 0 なので，**P**=$[5,\ \sqrt{-5}]=[\sqrt{-5}]$，N(**P**)= 5．よって**P'**=$[-\sqrt{-5}]$ であるが，もちろん**P**=**P'**である．よって**(** 5 **)**=**P**^{2}.

(4) $p=7$ の場合：$b^2\equiv -5\equiv 2 \pmod{7}$ より，解は $b\equiv 3,4 \pmod{7}$．この場合の最小の有理整数 b は 3 なので，**P**=$[7,\ 3+\sqrt{-5}]$，N(**P**)= 7．よって**P'**=$[7,\ 3-\sqrt{-5}]$ であるが，**P**≠**P'** である.

27) 1-√-5=3a+b(1+√-5)とおいてa,bの連立方程式を解いても整数解が得られない.

（注意：$[2,\ 1+\sqrt{-5}]$はイデアルの計算で特に重要な役割をなすことから $\mathbf{L}=[2,\ 1+\sqrt{-5}]$で表わされる．$\mathbf{L}^2=2$，$\mathbf{L}=[2,\ 1\pm\sqrt{-5}]=[2,\ -1\pm\sqrt{-5}]=[2,\ 3\pm\sqrt{-5}]$…などが成り立つ．）

【２】素イデアル分解

$p=2,3,5,7$の場合を取り上げたが，注意すべきは$p=2$のときと$p=5$のときである．これらの場合のみ **P=P'**．それ以外では **P≠P'** ．それぞれの素数によって素イデアルの振る舞いが異なる．それを説明するにはやはり「二次体の整数」を根本から論議する必要があるので，ここでは触れないことにする．詳細はもちろん「**講義**」を参照していただきたい．ともかくこれによって各有理素数（の単項イデアル）が次のように素イデアルの積に分解される．

(1) $(2)=(2,\ 1+\sqrt{-5})^2$．　$(2,\ 1+\sqrt{-5})=(2,\ 1-\sqrt{-5})$であるから$(2,\ 1-\sqrt{-5})^2$ でも可．

$$(2,1+\sqrt{-5})^2=(2,1+\sqrt{-5})(2,1+\sqrt{-5})=(4,2(1+\sqrt{-5}),2(1+\sqrt{-5}),2(-2+\sqrt{-5}))=(2).$$

(2) $(3)=(3,\ 1+\sqrt{-5})(3,\ 1-\sqrt{-5})$．

$$(3,\ 1+\sqrt{-5})(3,\ 1-\sqrt{-5})=(9,3(1-\sqrt{-5}),3(1+\sqrt{-5}),6)=(3)$$

(3) $(5)=(\sqrt{-5})^2$．明白．

(4) $(7)=(7,\ 3+\sqrt{-5})(7,\ 3-\sqrt{-5})$，または　$(7)=(7,\ 4+\sqrt{-5})(7,\ 4-\sqrt{-5})$．

$$(7,\ 3+\sqrt{-5})(7,\ 3-\sqrt{-5})=(49,\ 7(3-\sqrt{-5}),\ 7(3+\sqrt{-5}),\ 14)=(7),\ \text{または}$$

$$(7,\ 4+\sqrt{-5})(7,\ 4-\sqrt{-5})=(49,\ 7(4-\sqrt{-5}),\ 7(4+\sqrt{-5}),\ 21)=(7).$$

この結果を利用して p.29 に掲出した$Z[\sqrt{-5}]$における次の（一意的でない）「素因数分解」を振り返って見よう．

$$(8\text{–}2)\quad 6=2\times 3=(1+\sqrt{-5})(1-\sqrt{-5})$$

$$(8\text{–}3)\quad 21=3\times 7=(1+2\sqrt{-5})(1-2\sqrt{-5})=(4+\sqrt{-5})(4-\sqrt{-5})$$

$Z[\sqrt{-5}]$の整数としてはこの結果は変えられないが，イデアルについてここまで議論を進めてきた立場からは，６および 21 は整数としてよりも単項イデアル(6)，(21)と見るべきである．すなわち (8–2) の２，３および$(1+\sqrt{-5})$, $(1-\sqrt{-5})$ などはすべて（単項）イデアルである．(8–3) の３，７および$(1+2\sqrt{-5})$, $(1-2\sqrt{-5})$,$(4+\sqrt{-5})$,´ $(4-\sqrt{-5})$ などもすべてイデアルと見るのである．

まず(6)の方は，$(2)=(2,\ 1+\sqrt{-5})^2$，$(3)=(3,\ 1+\sqrt{-5})(3,\ 1-\sqrt{-5})$ であるから，

$$(8\text{–}4)\quad (6)=(2)(3)=(2,\ 1+\sqrt{-5})^2(3,\ 1+\sqrt{-5})(3,\ 1-\sqrt{-5})$$

となる．結果としてはこれが単項イデアル(6)の「**素イデアル分解**」なのであるが，これが$(1+\sqrt{-5})(1-\sqrt{-5})$ と同じものであることを示さなくてはならない．まず (8–4) 中の $(2,\ 1+\sqrt{-5})$ と $(3,\ 1+\sqrt{-5})$ を組み合わせて掛ければ，

$$(2,\ 1+\sqrt{-5})(3,\ 1+\sqrt{-5})=(6,\ 2(1+\sqrt{-5}),\ 3(1+\sqrt{-5}),\ (1+\sqrt{-5})^2).$$

であるが，$6=(1+\sqrt{-5})(1-\sqrt{-5})$ であるから，四つの要素はすべて$1+\sqrt{-5}$ の倍数である．よって，$(1+\sqrt{-5})$ となる．つまり単項イデアル $(1+\sqrt{-5})$ は

$$(1+\sqrt{-5})=(2,\ 1+\sqrt{-5})(3,\ 1+\sqrt{-5})$$

と素イデアル分解される．一方，(8–4)で残っている二つの素イデアルは $(2,\ 1+\sqrt{-5})$ と $(3,\ 1-\sqrt{-5})$ であるが，$(2,\ 1+\sqrt{-5})$ は $(2,\ 1-\sqrt{-5})$ と同じイデアルであるから，これと $(3,\ 1-\sqrt{-5})$ を組み合わせて掛ければ，6 は$1-\sqrt{-5}$ の倍数でもあるので，

$$(2,\ 1-\sqrt{-5})(3,\ 1-\sqrt{-5})=(6,\ 2(1-\sqrt{-5}),\ 3(1-\sqrt{-5}),\ (1-\sqrt{-5})^2)=(1-\sqrt{-5}).$$

よって単項イデアル $(1-\sqrt{-5})$ は

$$(1-\sqrt{-5})=\ (2,\ 1-\sqrt{-5})(3,\ 1-\sqrt{-5})$$

と素イデアル分解される．

以上から，

$$\begin{aligned}(6)=(2)(3)&=(2,\ 1+\sqrt{-5})^2(3,\ 1+\sqrt{-5})(3,\ 1-\sqrt{-5})\\&=\left\{(2,\ 1+\sqrt{-5})(3,\ 1+\sqrt{-5})\right\}\left\{(2,\ 1-\sqrt{-5})(3,\ 1-\sqrt{-5})\right\}\\&=(1+\sqrt{-5})(1-\sqrt{-5})\end{aligned}$$

となって，$(2,\ 1+\sqrt{-5})^2\cdot(3,\ 1+\sqrt{-5})(3,\ 1-\sqrt{-5})$ が**(6)**の素イデアル分解であることが示された．見通しよくするために，$(2,\ 1+\sqrt{-5})=\mathbf{P}$，$(3,\ 1+\sqrt{-5})=\mathbf{Q}$，$(3,\ 1-\sqrt{-5})=\mathbf{Q'}$とすれば，

$$(2)=(2,\ 1+\sqrt{-5})^2=\mathbf{P}^2,$$

$$(3)=(3,\ 1+\sqrt{-5})(3,\ 1-\sqrt{-5})=\mathbf{QQ'}.$$

よって，

$$(6)=(2)(3)=\mathbf{P}^2\mathbf{QQ'}$$

$$(1+\sqrt{-5})=\mathbf{PQ},\ \ (1-\sqrt{-5})=\mathbf{PQ'}\ .$$

同様の手順で (8–3) の「21」の三通りの「因数分解」が単項イデアル**(21)**の素イデアル分解によって解決される．

$$(8\text{–}5)\quad (21)=(3)(7)=(1+2\sqrt{-5})(1-2\sqrt{-5})=(4+\sqrt{-5})(4-\sqrt{-5})$$

$(3)=(3,\ 1+\sqrt{-5})(3,\ 1-\sqrt{-5})$，$(7)=(7,\ 3+\sqrt{-5})(7,\ 3-\sqrt{-5})$ であるが，$b\pm\sqrt{-5}$ のb が揃っていないと計算が煩雑になるので，$(3,\ 1\pm\sqrt{-5})$ は$(3,\ 4\pm\sqrt{-5})$ に，$(7,\ 3\pm\sqrt{-5})$ は$(7,\ 4\pm\sqrt{-5})$ に変えておく[28]（この変更が可能なのもイデアルならではである）．よって (8–5) は，

$$(8\text{–}5)'\quad (21)=(3)(7)=(3,\ 4+\sqrt{-5})(3,\ 4-\sqrt{-5})\ (7,\ 4+\sqrt{-5})(7,\ 4-\sqrt{-5})$$

になる．結果としてこれが**(21)**の素イデアル分解である．

まず，(8–5) の$(4+\sqrt{-5})$ は$(3,\ 4+\sqrt{-5})$ と$(7,\ 4+\sqrt{-5})$ の積から作られる．

---

28) 4±√-5は3と1±√-5から，あるいは7と3±√-5から作られるのでそれぞれ同じイデアルである．

$$(3,\ 4+\sqrt{-5})(7,\ 4+\sqrt{-5})=(21,3(4+\sqrt{-5}),7(4+\sqrt{-5}),(4+\sqrt{-5})^2)$$

で，$21=(4+\sqrt{-5})(4-\sqrt{-5})$ なので四つの生成元はすべて $4+\sqrt{-5}$ の倍数である．よって，

$$(4+\sqrt{-5})=(3,\ 4+\sqrt{-5})(7,\ 4+\sqrt{-5}).$$

これが単項イデアル $(4+\sqrt{-5})$ の素イデアル分解である．

同様に単項イデアル $(4-\sqrt{-5})$ は=$(3,\ 4-\sqrt{-5})$ $(7,\ 4-\sqrt{-5})$ と分解される．

ちょっとわかりにくいのは $(1+2\sqrt{-5})$ および $(1-2\sqrt{-5})$ である．しかし**(21)**の素イデアルは(8–5)'の右辺の四つしかないので手がかりはこの中にある．実は整数 $1+2\sqrt{-5}$ はイデアル $(3,\ 4-\sqrt{-5})$ の要素である．$1+2\sqrt{-5}=3x+y(4-\sqrt{-5})$ と置いて $x,\ y$ を求めれば，$x=3,\ y=-2$ の有理整数解が得られる．すなわちイデアル $(1+2\sqrt{-5})$ は $(3,\ 4-\sqrt{-5})$ に含まれる．言い換えれば，$(1+2\sqrt{-5})$ は $(3,\ 4-\sqrt{-5})$ で割り切れるのである．では，

$$(1+2\sqrt{-5})=(3,\ 4-\sqrt{-5})\mathbf{Q}$$

と置いたときの**Q**は何か．(8–5)'の右辺の四つのうちではあとは $(7,\ 4+\sqrt{-5})$ しかない（素イデアル分解の一意性による）．実際に計算すると，

$$(3,\ 4-\sqrt{-5})(7,\ 4+\sqrt{-5})=(21,3(4+\sqrt{-5}),7(4-\sqrt{-5},21)$$

であるが，この 四つの生成元はすべて $1+2\sqrt{-5}$ の倍数である．

$$21=(1+2\sqrt{-5})(1-2\sqrt{-5})$$

$$\frac{3(4+\sqrt{-5})}{1+2\sqrt{-5}}=\frac{3}{21}\left\{(4+\sqrt{-5})(1-2\sqrt{-5})\right\}=\frac{1}{7}(14-7\sqrt{-5})=2-\sqrt{-5}$$

$$\frac{7(4-\sqrt{-5})}{1+2\sqrt{-5}}=\frac{7}{21}\left\{(4-\sqrt{-5})(1-2\sqrt{-5})\right\}=\frac{1}{3}(-6-9\sqrt{-5})=-2-3\sqrt{-5}$$

よって $(3,\ 4-\sqrt{-5})(7,\ 4+\sqrt{-5})=(1+2\sqrt{-5})$ である．

同様に $(1-2\sqrt{-5})=(3,\ 4+\sqrt{-5})$ $(7,\ 4-\sqrt{-5})$ が得られる．こうして (8–5) から (8–5)' が導かれた．イデアル **(21)** が素イデアルの積に分解されたのである．

$$\mathbf{(21)}=(3,\ 4+\sqrt{-5})(3,\ 4-\sqrt{-5})\ (7,\ 4+\sqrt{-5})(7,\ 4-\sqrt{-5}).$$

これも **P**=$(3,\ 1+\sqrt{-5})$，**P'=**$(3,\ 1-\sqrt{-5})$，**Q**=$(7,\ 3+\sqrt{-5})$，**Q'**=$(7,\ 3-\sqrt{-5})$ で表せば，

(3**)**=$(3,\ 1+\sqrt{-5})(3,\ 1-\sqrt{-5})$=**PP'**，**(**7**)**=$(7,\ 3+\sqrt{-5})(7,\ 3-\sqrt{-5})$=**QQ'** より，

$$\therefore\quad \mathbf{(21)}=\mathbf{(}3\mathbf{)}=\mathbf{(}7\mathbf{)}=\mathbf{PP'QQ'}$$

一方，$(4+\sqrt{-5})$=**PQ**，$(4-\sqrt{-5})$=**P'Q'** より，

$$\mathbf{(21)}=(4+\sqrt{-5})\ (4-\sqrt{-5})=\mathbf{PQP'Q'}=\mathbf{PP'QQ'}$$

最後に，$(1+2\sqrt{-5})$=**P'Q**，$(1-2\sqrt{-5})$=**PQ'** より，

$$\mathbf{(21)}=(1+2\sqrt{-5})\ (1-2\sqrt{-5})=\mathbf{P'QPQ'}=\mathbf{PP'QQ'}$$

こうして$Z[\sqrt{-5}]$における「素因数分解の一意性」不可の問題をイデアル論によって「解決」したのだが，このことはどう考えたらいいのだろうか．

まず，Zから$Z[\sqrt{-5}]$に整数の範囲を広げたことで，Zでは可能であった素因数分解の一意性が成り立たないことになったのは，明らかに整数の次数が１から２になったことに原因がある．一意性が整数の「倍数」という外延的な性質に頼っていたからである．その性質が二次体では維持されなくなるのだ．それが「イデアル」によって復活する．イデアルは倍数という自明な外観によって隠されていた整数の本来の属性（イデアルの性質[1][2]）を開示し，自身も二次的な様相を持って「素因数分解」の一意性を復活する．もちろんイデアルの本体は「整数の集合」であるからそれは素因数による分解ではない．しかし集合によって表現されたところの，整数の内包的な性質そのものである[29]．

このようにイデアルの性質がすべての（$Z[\sqrt{-5}]$の）整数に内包されているものであるならば，あえて整数とイデアルを区別する必要はなくなってくる．いわば，整数がイデアルによって止揚（アウフヘーベン）されるのである．すなわち，**イデアルとは「整数」そのものである**．

これまで整数と単項イデアルを区別してきたが，ここまでくればその必要は無くなる．整数として表記すること自体がイデアルを表していると考えるのである．ただ，二つの整数を底とするイデアルはこれまで通り（α, β）で表すこととする．従って上記の有理整数の単項イデアルの素イデアル分解なども次のように表記することにする．

$$6=(2,\ 1+\sqrt{-5})^2(3,\ 1+\sqrt{-5})(3,\ 1-\sqrt{-5})$$

$$21=(3,\ 4+\sqrt{-5})(3,\ 4-\sqrt{-5})(7,\ 4+\sqrt{-5})(7,\ 4-\sqrt{-5})$$

ただし，２が数なのかイデアルなのか紛らわしい場合にはイデアルの方を**(２)**と表す．

さらに「**講義**」に倣って，イデアルでは「割り切れる」は「含まれる」であったから，「イデアル$(1+2\sqrt{-5})$がイデアル$(7,\ 4+\sqrt{-5})$で割り切れる」ことを「整数$1+2\sqrt{-5}$はイデアル$(7,\ 4+\sqrt{-5})$で割り切れる」，または$1+2\sqrt{-5}\subset(7,\ 4+\sqrt{-5})$と表すことがある．

---

[29] あえて例えればデデキントの「切断」のようなものである．切断も数の集合であるが，それによって実数の本質的な性質（＝連続性）を目に見えるものにする．

9. 不定方程式 $x^2+5y^2=a$ とイデアル

この小論３章で扱った $x^2+y^2=a$ では，複素整数 $Z[\sqrt{-1}]$ による解法を紹介したが，ここで扱う二元二次不定方程式は，

$$(9-1)\quad x^2+5y^2=a \qquad (a \text{ は有理正整数の定数})$$

というもので，もちろん x, y の有理整数解を求めるのである．この左辺を「因数分解」すれば，

$$(9-2)\quad (x+y\sqrt{-5})(x-y\sqrt{-5})=a$$

となり，整数 $Z[\sqrt{-5}]$ に強く関係することがうかがえる．

まず，小手調べとして x, y に適当に有理整数を代入してみよう．$(x, y)=(1, 0)$ なら $a=1$，$(x, y)=(0, 1)$ なら $a=5$，$(1, 1)$ なら $a=6$，…となる．これら a の値をいくつか集めてみれば，

$$(9-3)\quad a=0, 1, 4, 5, 6, 9, 14, 20, 21, 24, 29, 41, \cdots$$

となるが，これらの値から帰納的に (x, y) の一般解に至ることは不可能である．そこで a について場合分けしてできるだけ初等的なアプローチを試みることにする．

なお，右辺の有理整数 a は素因数に m^2 のような有理整数を含まないものとする．有理整数 k, l が互いに素でなくて (9−1)の解であれば，$k^2+5l^2=a$．このとき，k, l の最大公約数を m とすれば $k=mk'$, $l=ml'$ と置くことで k', l' は互いに素になる．このときには

$$(mk')^2+5(ml')^2=m^2(k'^2+5l'^2)=a.$$

すなわち a は m^2 で割り切れるのである．ゆえに k, l と k', l' は (9−1) の解としては同類とみなし，以下では x, y が互いに素である解だけを求めることとする（このような解を「**原始解**」という）．

逆に言えば，原始解 (x, y) が見つかれば (mx, my) も(9−1) の解になるわけである．

まず a を有理素数に限って考えてみる．

【１】$a=p$（有理素数）の場合

(9−1) で $a=p$ として，

$$(9-1-1)\quad x^2+5y^2=p \qquad (p \text{ は有理素数})$$

とする．すぐにわかることは，x^2-p が５の有理整数倍，すなわち，

$$(9-2)\quad x^2\equiv p \pmod{5}$$

ということである．p は法５の平方剰余でなければならないから，

$$(9-3)\quad p\equiv 0,1,4 \pmod{5}.$$

なお，$p=2$ および $p=5$ は方程式 (9−1−1) でそれぞれ $(x, y)=(\pm1, 0), (0, \pm1)$ という解を持つが，これは特別とし，以下では $p\neq 2, 5$ とする．よって，

$$(9\text{–}3)' \quad p \equiv 1,4 \pmod{5}.$$

(9–3)' は方程式 (9–1–1) に解があるための p の第一条件である.

ここで, 方程式 (9–1–1) をイデアルのノルムの式と考えてみよう. この問題はノルムが p となる $Z[\sqrt{-5}]$ の**イデアル**を求めることである. 左辺はあるイデアル **J** のノルムの計算式で, 右辺はその値である. 求めるイデアル **J** はノルムが x^2+5y^2 となるのであるから単項イデアルである. よって **J**$=x+y\sqrt{-5}$ と置ける. ノルムは N(**J**)$=x^2+5y^2$ であるから, これが有理素数 p に等しいというのが方程式 (9–1–1) である.

$$\mathrm{N}(\mathbf{P})=x^2+5y^2=p$$

さて, **J**はノルムが有理素数であるから一次の素イデアルである（p.51参照）. ここで, **J**を標準的な底で表せば,

$$(9\text{–}4) \quad \mathbf{J}=[p,\ b+\sqrt{-5}]$$

とすることができる（定理 8.2）. 次に **J** が一次の素イデアルであるための必要十分条件は,

$$(9\text{–}5) \quad b^2 \equiv -5 \pmod{p}$$

に解が存在すること, 言い換えれば−5が法 p の平方剰余であることであった（定理 8.2）.

(9–3)' および (9–5) の二つの条件に当てはまる有理素数を羅列してみると,

(9–3)'より : p =11,19,29,31,41,59,61,71,79,89,91,…

(9–5)より : p =3,7,23,29,41,43,47,56,61,67,83,89,…　（2は特別扱いで除外）

注意：(9–5)を求める計算は, 例えば p =23のとき, $b^2 \equiv -5 \equiv 18 \pmod{23}$ であるから,

b : 1, 2, 3, 4, 5, 6, 7, **8**, 9, 10, 11, 12, 13, 14, **15**,…
b²: 1, 4, 9, 16, 25, 36, 49, 84, 81,100,121,144, 169,196, 225,…

法23の剰余: 1, 4, 9, 16, 2, 13, 3, **18**, 12, 8, 6, 6, 8, 12, **18**,…

よって, b=8,15が平方剰余である. すなわち $8^2 \equiv -5$, (mod.23), $15^2 \equiv -5$, (mod.23). ゆえに p =23は(9–5)に該当する. 他の素数も同様に計算して判定する. p =11,19等は(9–5)に該当する平方剰余がない.

(9–3)' および (9–5) の両方に含まれる有理素数は,

$$(9\text{–}6) : \ p=29,41,61,89,\cdots$$

となる. こうして労を厭わず計算することで方程式 (9–1–1) に解が存在する有理素数を見つけることができる. 解は (9–6) の素数の順に $(x,y)=(3,2),(6,1),(4,3),(3,4),\cdots$　（複号±略）

(9–6)の値から帰納的に方程式 (9–1–1) で解の存在する素数 p は「**20で割ると1または9余る素数**」ではないかと推測できる. これが実は正解である.

さりげなく「**20**」という数字が出てきたが, これは $Z[\sqrt{-5}]$ における「判別式」と呼ばれる重要な数で, 通常 d で表される. $d=20$ **を** $Z[\sqrt{-5}]$ **の判別式**という.

判別式は一般の二次体の整数 Z[√m] において規定されるが, その値 d はmの値によってd=m, またはd=4mの二種類がある. Z[√−5]の場合はd=−20 である. 整数 Z に対する Z[√−5]の生成元である√−5は, 二次方程式 $x^2+5=0$の解である. この方程式の判別式dは $d=0^2-4\cdot1\cdot5=-20$ で, これがZ[√−5]の判別式にな

るのである（この小論ではd=20（絶対値）を使用）．その起源をたどるには二次体の整数の厳密な定義に及ぶため，本論では天下り的にしか述べることができない（「**講義**」での判別式 d の初出は p.291）．

有理整数 Z において，$d=20$ を法とする剰余類（0 を除く 1 ～19）の中で，d と互いに素であるものだけを特に d の**既約剰余類**（既約類）という．d の既約剰余類は 1,3,7,9,11,13,17,19 の八個である．正確には，

$$d\text{の既約剰余類：}\ x\equiv 1,3,7,9,11,13,17,19\ (\mathrm{mod}.\ d)$$

としなければならない．これらは法20とは互いに素であるが，素数とは限らない（例えば $x=21$）．d の約数である 2 と 5 は含まれていない．

さて，$d=20$ を法とする既約剰余類 $x\equiv 1,3,7,9,11,13,17,19\ (\mathrm{mod}.\ d)$ の中で，条件 (9–5) $b^2\equiv -5\ (\mathrm{mod}.\ p)$ に解をもつ素数 p は $p\equiv 1,3,7,9\ (\mathrm{mod}.\ d)$ であることを計算で確かめよう．例えば，$p\equiv 1\ (\mathrm{mod}.\ 20)$ とすれば，p は $20t+1$ の形の素数：$p=41,61,\cdots$ であるが，

$$p=41\text{ならば }b^2\equiv -5\ (\mathrm{mod}.\ 41)\quad\therefore\ b\equiv 6,35\ (\mathrm{mod}.\ 41)$$

$$p=61\text{ならば }b^2\equiv -5\ (\mathrm{mod}.\ 61)\quad\therefore\ b\equiv 19,56\ (\mathrm{mod}.\ 61)$$

$$\vdots$$

同様に $p\equiv 3,7,9\ (\mathrm{mod}.\ 20)$ も $b^2\equiv -5\ (\mathrm{mod}.\ p)$ に解を持つ（ぜひ確かめてください）．

しかし $p\equiv 11,13,17,19\ (\mathrm{mod}.\ d)$ の場合には $b^2\equiv -5\ (\mathrm{mod}.\ p)$ に解が存在しない．例えば，$p\equiv 11\ (\mathrm{mod}.\ 20)$ を採れば p は $20t+11$ の形の素数：$p=11,31,\cdots$ で，$p=11$ とすれば，$b^2\equiv -5\equiv 6\ (\mathrm{mod}.\ 11)$ となるが，法11における－5の平方剰余は 1,3,4,5,9 で，6 は存在しない．以下同様にして $p\equiv 11,13,17,19\ (\mathrm{mod}.\ d)$ のいずれの素数も $b^2\equiv -5\ (\mathrm{mod}.\ p)$ に解を持たない．

結局，20の既約剰余類八つのうち，半分の $p\equiv 1,3,7,9\ (\mathrm{mod}.\ d)$ が $b^2\equiv -5\ (\mathrm{mod}.\ p)$ を満たし，残りの $p\equiv 11,13,17,19\ (\mathrm{mod}.\ d)$ は $b^2\equiv -5\ (\mathrm{mod}.\ p)$ を満たさないのである．

さて，$p\equiv 1,3,7,9\ (\mathrm{mod}.\ d)$ に該当する有理素数は，

$$(9\text{–}7)\quad p=3,7,23,29,41,43,47,61,67,83,89,101,103,107,109\cdots$$

であるが，最初の条件，

$$(9\text{–}3)'\quad p\equiv 1,4\ (\mathrm{mod}.\ 5)$$

を満たさなくてはならない．これによって $p\equiv 1,3,7,9\ (\mathrm{mod}.\ d)$ のうち，$p\equiv 3,7\ (\mathrm{mod}.\ d)$ が当てはまらなくなることは明らかである．なぜなら「d (=20) で割って 3 または 7 が余る数」を 5 で割れば 3 または 2 が余るのだから，$p\equiv 1,4\ (\mathrm{mod}.\ 5)$ を満たすことはない．ゆえに，

$$(9\text{–}8)\quad p\equiv 1,9\ (\mathrm{mod}.\ d)$$

だけになる．羅列すれば，

$$(9\text{–}8)'\quad p=29,41,61,89,101,109\cdots$$

これが方程式 (9–1–1) $x^2+5y^2=p$ に解をもつ素数たちである．

以上をまとめていえば，方程式 (9−1−1) $x^2+5y^2=p$， $p>5$ で，この方程式が有理整数解を持つための p の条件は次の三つである．

① $p\equiv 1,3,7,9,11,13,17,19 \pmod{d}$ （d は $Z[\sqrt{-5}]$ の判別式）

② $p\equiv 1,4 \pmod{5}$ （p は法 5 の平方剰余）

③ 合同式 $x^2\equiv -5 \pmod{p}$ に解を持つ（-5 が p の平方剰余）

これを一つにしていえば $p\equiv 1,9 \pmod{d}$ である．

また言い訳であるが， p≡1,3,7,9 (mod.20) だけが $b^2\equiv -5$ (mod. p)の解を持つことの証明がなされず，計算例だけを上げている（それも一部のみ）のは，証明に「**平方剰余の相互法則**」が必須だからである．次章でこれに触れるが，ここではしばらくこれを承認することで先に進めたい．

例：$x^2+5y^2=109$

109は $p\equiv 1,9 \pmod{d}$ に属する有理素数であるからこの方程式は有理整数解を持つ．

109 をノルムとするイデアルを **J**= $x+y\sqrt{-5}$ とする．**J**を一次の素イデアルとして **J**= $[109,\ b+\sqrt{-5}]$ とすれば， $b^2\equiv -5\equiv 104 \pmod{109}$ から $b=39$ を選ぶと，**J**= $[109,\ 39+\sqrt{-5}]$．ここで，N($39+\sqrt{-5}$)=1526 を利用した次のような解法を紹介する．

N($39+\sqrt{-5}$)=1526=109×2×7．109は**J**の，2は**L=** $[2,\ 1+\sqrt{-5}]$ の，そして 7 は**Q**= $[7,\ 3+\sqrt{-5}]$ のノルムである．よって，N($39+\sqrt{-5}$)=N(**J**)・N(**L**)・N(**Q**)．ゆえに，

$$39+\sqrt{-5}=\mathbf{JLQ}.$$

ここで，**LQ**= $(2,\ 1+\sqrt{-5})\ (7,\ 3+\sqrt{-5})$ であるが，**L=** $[2,\ 3+\sqrt{-5}]$ でもあるので，**LQ**= $3+\sqrt{-5}$ となる．よって， $39+\sqrt{-5}=\mathbf{J}(3+\sqrt{-5})$．ここから，

$$\mathbf{J}=\frac{39+\sqrt{-5}}{3-\sqrt{-5}}=\frac{1}{14}(39+\sqrt{-5})(3+\sqrt{-5})=8+3\sqrt{-5}.$$

J= $8+3\sqrt{-5}$ から $(x,\ y)=(8,\ 3)$ が解である（複号略）．**J'**を計算しても同じ結果になるのでこれ以外の解はない．

(**L**=[2,1+√−5]の柔軟性を利用したかなり技巧的な計算であるが，これらを習得することでイデアルの理解につながる．「講義」p.343 参照)

方程式 (9−1−1) に解があるための有理素数 p の条件が， $p\equiv\pm 1 \pmod{5}$ と $x^2\equiv -5 \pmod{p}$ だけでなく $Z[\sqrt{-5}]$ の判別式 d (= 20) を必要とすることが，まさに「判別式」の所以である．もう一つ重要なことは， $p\equiv 1,9 \pmod{d}$ に入っていない有理素数 $p=5$ も(9−1−1)に解を持つ．

「**講義**」p.292 には「判別式 d の約数である有理素数 p は二次体に関して特異な性質（$p=\mathbf{P}^2$）を有するものである」と述べられている．

（念のため「解法」を紹介すれば，$x^2+5y^2=5$ より，$x+y\sqrt{-5}=\sqrt{-5}$ ∴ (x,y)=(0,1)．）

【2】$a=2p$ のとき

Jを単項イデアルとして **J**$=x+y\sqrt{-5}$ とおけば，N(**J**)$=x^2+5y^2$ であるから，

$$(9\text{–}1\text{–}2)\quad x^2+5y^2=2p$$

となって所定の方程式が得られる．よって $x^2\equiv 2p\ (\mathrm{mod}.5)$ を満たすことが必要となる．

ここで，法が5のとき $2p$ が平方剰余ならば p は平方非剰余であることを示そう．

$x^2\equiv 2p\ (\mathrm{mod}.5)$ より，$2p\equiv\pm 1\ (\mathrm{mod}.5)$ であるから，$2p\equiv\pm\equiv\mp 4\ (\mathrm{mod}.5)$，よって，

$$(9\text{–}10)\quad p\equiv\pm 2\ (\mathrm{mod}.5)\ \text{または}\ p\equiv 2,\ 3\ (\mathrm{mod}.5).$$

$p\equiv 1,4\ (\mathrm{mod}.5)$ が5の平方剰余であるから $p\equiv 2,3\ (\mathrm{mod}.5)$ は平方非剰余である．これが p の最初の条件である．

方程式 (9–1–2) $x^2+5y^2=2p$ では，**J**を単項イデアルとして **J**$=x+y\sqrt{-5}$ と置いたのであるが，右辺の $2p$ が合成数なので，**J** は素イデアルではない．そこで **P**をノルム p のイデアルとすれば，**P**は一次の素イデアルであるから，**P**$=[p,\ b+\sqrt{-5}]$ と置ける．N(**P**)$=p$ である．そして，**L**$=[2,\ 1+\sqrt{-5}]$ とすれば N(**L**)$=$**L**$^2=2$ であるから（p.52 参照），$x^2+5y^2=2p$ は，

$$\mathrm{N}(\mathbf{J})=\mathrm{N}(\mathbf{L})\cdot\mathrm{N}(\mathbf{P})=\mathrm{N}(\mathbf{LP})$$

すなわち，**J**$=$**LP** である．こうして **J** が素イデアル分解された．要するに，右辺が $2p$ という有理素数の積なので，それに対応する左辺も素イデアルの積に分解されるということである．

Lは確定しているため，**P**を求めることで **J** を決定できる．素イデアル **P**$=[p,\ b+\sqrt{-5}]$ では，$\mathrm{N}(b+\sqrt{-5})=b^2+5$ が p で割り切れるため，

$$(9\text{–}5)\quad b^2\equiv -5\ (\mathrm{mod}.\ p)$$

が p の条件である．さらに $d=20$ を法とする既約剰余類の中で，条件 (9–5) $b^2\equiv -5\ (\mathrm{mod}.\ p)$ に解をもつ素数は $p\equiv 1,3,7,9\ (\mathrm{mod}.\ d)$ であることはすでに述べている（p.59）が，今度はこの中で条件 (9–10)の $p\equiv 2,3\ (\mathrm{mod}.5)$ を満たすことが必要になる．これは $p\equiv 3,7\ (\mathrm{mod}.\ d)$ である（なぜなら，20で割って3余るものは5で割っても3余り，20で割って7余るものは5で割れば2余るから）．

すなわち，**P**$=[p,\ b+\sqrt{-5}]$ の p の条件は，$p\equiv 3,7\ (\mathrm{mod}.\ d)$ ということになる．p が決まれば自動的に b も決まる．つまり **P** が決定する．

実際に $p\equiv 3,7\ (\mathrm{mod}.\ d)$ から p を選んで**P**を決定し，**J**を求めてみよう．

例 1 : $x^2+5y^2=6$，$p=3$

$p=3$ のとき **P**$=[3,\ b+\sqrt{-5}]$ で，$b^2\equiv -5\ (\mathrm{mod}.3)$ から $b=1$ を選べば **P**$=[3,\ 1+\sqrt{-5}]$．

$$\mathbf{J}=\mathbf{LP}=(2,1+\sqrt{-5})(3,\ 1+\sqrt{-5})=\left(6,2(1+\sqrt{-5}),3(1+\sqrt{-5}),(1+\sqrt{-5})^2\right)=1+\sqrt{-5}$$

$\therefore$ N(**P**)$=1^2+5\cdot 1^2=6$ （$=2\cdot 3$）．これは直感でも解ける．

例 2 : $x^2+5y^2=94$，$p=47$

$p=47$ のとき **P**=[47, $b+\sqrt{-5}$] と置いて，$b^2\equiv -5\equiv 42$ (mod. 47) から $b=18$ を選べば，**P**=[47, $18+\sqrt{-5}$]．これもN($18+\sqrt{-5}$)を利用する（「**講義**」p.343参照）．

N($18+\sqrt{-5}$)=329=47×7（整数 $a+b\sqrt{-5}$ のノルムは a^2+5b^2），N(**P**)=47，またイデアル**Q**＝[7, $3-\sqrt{-5}$] と置けば，N(**Q**)= 7．ゆえに，N($18+\sqrt{-5}$)=N(**P**)・N(**Q**)と変形できる．よって，$18+\sqrt{-5}$ =**PQ**.

この両辺に$\mathbf{L}^2$=2をかければ，2($18+\sqrt{-5}$)=**LLPQ**となる．**QL**=(7, $3-\sqrt{-5}$)(2, $1+\sqrt{-5}$) $=3+\sqrt{-5}$ である（なぜなら，**L**=[2, $3-\sqrt{-5}$] でもある）から，

$$2(18+\sqrt{-5}\,)=\mathbf{LP}(3-\sqrt{-5}\,)$$

ここから，

$$\mathbf{LP}=\frac{2(18+\sqrt{-5}\,)}{3-\sqrt{-5}}=\frac{2}{14}(18+\sqrt{-5})(3+\sqrt{-5})=7+3\sqrt{-5}$$

よって，**J**=**LP**= $7+3\sqrt{-5}$ より，$(x,\ y)=(7,\ 3)$ となる（複号略）．**LP**に対して**LP'**を計算しても同じ結果になるのでこれ以外の解はない.

以上をまとめていえば，方程式 (9–1–2) $x^2+5y^2=2p$，$p>5$ で，この方程式が有理整数解を持つための p の条件は次の三つである.

① $p\equiv 1,3,7,9,11,13,17,19$ (mod. d) （d は $Z[\sqrt{-5}]$ の判別式）

② $p\equiv 2,3$ (mod. 5) （p は法5の平方剰余）

③ 合同式 $x^2\equiv -5$ (mod. p) に解を持たない（-5 が p の平方非剰余）

①～③を満たす p は，$p\equiv 3,7$ (mod. d) である．具体的には，$p=3,7,23,43,47,\cdots$.

したがって，$2p$ の値は，

$$(9\text{–}14)'\qquad 2p=6,14,46,86,94,\cdots$$

この順に，$(x,y)=(1,1),(3,1),(1,3),(9,1),(7,3),\cdots$ が (9–1–2) の有理整数解である（複号±略）．このほかに $p=2$（$2p=4$）のときも解を持つが，これは【1】ので述べたように d の約数として特別である.

念のため「解法」を述べれば，$x^2+5y^2=4$より，N(4)となるイデアルはx+√−5=２である．よって x=±2,y=0.

【3】$a=5p$ のとき

Jを単項イデアルとして **J**=$x+y\sqrt{-5}$ とおけば，N(**J**)=x^2+5y^2 であるから，

$$(9\text{–}1\text{–}3)\quad x^2+5y^2=5p$$

となる．よって $x^2\equiv 0$ (mod. 5) を満たすことが必要となる．これは $x\equiv 0$ (mod. 5)，すなわち x は5の倍数でしかあり得ない．よって，$x=5m$ とおいて (9–1–2) に代入すると，

$$(9\text{–}15)\quad y^2+5m^2=p$$

これは【１】の場合と文字が変わっただけで同じである．よって p の要件は，

$$(9\text{–}8)\quad p\equiv 1,9\ (\mathrm{mod}.\ d)$$

となる．例題として(9–8)から $p=41$ とすると，(9–15) の解は $(y,m)=(6,1)$．よって，$(x,y)=(5,6)$．$a=5p$ は，５が判別式 d の約数であることから特別な場合になる．

【４】$a=pq$ のとき

方程式 (9–1) $x^2+5y^2=a$ で，$a=pq$ のとき，

$$(9\text{–}1\text{–}4)\quad x^2+5y^2=pq\ （p,q\text{ は有理素数で }p>5,\ q>5）$$

は a が二つの素因数に分解される場合となる．まず，$x^2-pq=5y^2$ より，

$$(9\text{–}15)\ x^2\equiv pq\ (\mathrm{mod}.5)$$

でなければならない．法５に対する平方剰余は $x\equiv\pm1\ (\mathrm{mod}.5)$ であるから，(9–15) より，

$$(9\text{–}16)\ pq\equiv\pm1\ (\mathrm{mod}.5)$$

となる．pq が法５の平方剰余であるとき，p,q はともに平方剰余または平方非剰余（$x\equiv\pm2\ (\mathrm{mod}.5)$）であることを示そう．

① $p,q\equiv\pm1\ (\mathrm{mod}.5)$ のとき：$p\equiv\pm1\ (\mathrm{mod}.5)$，$q\equiv\pm1\ (\mathrm{mod}.5)$ ならば $pq\equiv\pm1\ (\mathrm{mod}.5)$（複号は不同順，以下同じ）

② $p\equiv\pm1\ (\mathrm{mod}.5)$，$q\equiv\pm2\ (\mathrm{mod}.5)$ のとき：$pq\equiv\pm2\ (\mathrm{mod}.5)$（$p,q$ が逆でも同じ）

③ $p,q\equiv\pm2\ (\mathrm{mod}.5)$ のとき：$p\equiv\pm2\ (\mathrm{mod}.5)$，$q\equiv\pm2\ (\mathrm{mod}.5)$ ならば $pq\equiv\pm4\equiv\mp1\ (\mathrm{mod}.5)$

以上の結果，pq が法５の平方剰余になるのは，p,q がともに平方剰余または平方非剰余であるときである．よって，(9–16) からは，

$$(9\text{–}17)\ p,q\equiv\pm1\ (\mathrm{mod}.5)\ \text{または}\ p,q\equiv\pm2\ (\mathrm{mod}.5)$$

$$（p,q\equiv1,4\ (\mathrm{mod}.5)\ \text{または}\ p,q\equiv2,3\ (\mathrm{mod}.5)\ \text{でも同じ}）$$

となる．これが方程式 (9–1–4) に解が存在するための p,q の第一条件である．

さて，(9–1–4) の左辺を単項イデアル $\mathbf{J}=x+y\sqrt{-5}$ のノルム，右辺の pq を一次の単項素イデアル $\mathbf{P}=[p,\ k+\sqrt{-5}]$，$\mathbf{Q}=[q,\ l+\sqrt{-5}]$ のノルムの積と見れば，

$$(9\text{–}18)\quad \mathrm{N}(\mathbf{J})=\mathrm{N}(\mathbf{P})\cdot\mathrm{N}(\mathbf{Q})=\mathrm{N}(\mathbf{PQ})$$

$$(9\text{–}19)\quad \therefore\ \mathbf{J}=\mathbf{PQ}$$

よって $\mathbf{J}$ は二つの素イデアルに分解される．

$\mathbf{P}$，$\mathbf{Q}$が一次の素イデアルであるから p,q の条件は，それぞれ，

$$(9\text{–}20)\quad k^2\equiv-5\ (\mathrm{mod}.\ p),\quad l^2\equiv-5\ (\mathrm{mod}.\ q)$$

である．そして $Z[\sqrt{-5}]$ の判別式 $d=20$ における既約剰余類のうち (9–20) を満たす p,q は，

$$(9\text{–}21)\quad p,\ q\equiv1,3,7,9\ (\mathrm{mod}\ d)$$

でなければならないから，これと条件 (9–17) から，

(9–22)　$p,\ q \equiv 1,\ 9\ (\mathrm{mod}.\ d)$ または $p,\ q \equiv 3,\ 7\ (\mathrm{mod}.\ d)$

となる．いずれにしても $d=20$ における既約剰余類中の $x \equiv 11,13,17,19\ (\mathrm{mod}\ d)$ は含まれてはいない．逆に言えば p,q どちらかが $x \equiv 11,13,17,19\ (\mathrm{mod}\ d)$ に属するのであれば方程式 (9–1–4) は有理整数解を持たないということになる．

解が可能な有理素数を具体的に列記すれば，

(9–23)　$p,\ q$ =29,41,61,89,101,109…．または　(9–24)　$p,\ q$ =23,43,47,67,83,87,….

例(1)：$p,\ q \equiv 1,\ 9\ (\mathrm{mod}.\ d)$ に属する二つの有理素数を $p=29,\ q=41$ とすれば，方程式(9–1–4) は，$x^2+5y^2=29\cdot 41=1189$．求める単項イデアルを **J**$=x+y\sqrt{-5}$ とおく．このとき **P**$=[29,\ k+\sqrt{-5}]$，**Q**$=[41,\ l+\sqrt{-5}]$ と置けば，

$$\mathbf{J}=\mathbf{PQ}\quad \therefore \mathrm{N}(\mathbf{J})=\mathrm{N}(\mathbf{P})\cdot\mathrm{N}(\mathbf{Q}).$$

そして $k^2 \equiv -5 \equiv 24\ (\mathrm{mod}.\ 29)$，$l^2 \equiv -5 \equiv 36\ (\mathrm{mod}.\ 41)$ の条件から $k=13,\ l=6$ が得られる．よって，**P**$=[29,\ 13+\sqrt{-5}]$，**Q**$=[41,\ 6+\sqrt{-5}]$ となる．

まず，**P**$=[29,\ 13+\sqrt{-5}]$ より，$\mathrm{N}(13+\sqrt{-5})=174=29\times 2\times 3$．N(**P**)=29．**L**$=[2,\ 1+\sqrt{-5}]$，**R**$=[3,\ 1+\sqrt{-5}]$ と置けば．N(**L**)=2，N(**R**)=3．ゆえに，$13+\sqrt{-5}=$**PLR**，そして**LR**$=1+\sqrt{-5}$．よって，$13+\sqrt{-5}=$**P**$(1+\sqrt{-5})$．ゆえに，

$$\mathbf{P}=\frac{13+\sqrt{-5}}{1+\sqrt{-5}}=3-2\sqrt{-5}$$

一方，**Q**$=[41,\ 6+\sqrt{-5}]$ は，$\mathrm{N}(6+\sqrt{-5})=41$ なので　**Q**$=6+\sqrt{-5}$．すなわち，**P**，**Q**ともに単項イデアルである（$p,\ q \equiv 1,\ 9\ (\mathrm{mod}.\ d)$ に属するので当然）．よって求めるイデアル **J** は

$$\mathbf{J}=\mathbf{PQ}=(3-2\sqrt{-5})(6+\sqrt{-5})=28-9\sqrt{-5}.$$

J$=28-9\sqrt{-5}$ から，$(x,\ y)=(28,\ 9)$ が得られる（複号略）．

一方，**P**，**Q**に対して**P'**，**Q'**（共役イデアル）を計算すれば，**P'Q'**=(**PQ**)'=**J'** $=28+9\sqrt{-5}$ であるから，同じ解しか得られないが，**P**，**Q'**からは

$$\mathbf{PQ'}=(3-2\sqrt{-5})(6-\sqrt{-5})=8-12\sqrt{-5}$$

となって，別解の $(x,\ y)=(8,\ 12)$ が得られる．ゆえに $x^2+5y^2=1189$ の解は

$(x,\ y)=(28,\ 9)$，$(8,\ 12)$ である．

上の例で，$p,\ q$ がともに $x \equiv 1,\ 9\ (\mathrm{mod}.\ d)$ に属するような有理素数は，方程式 $x^2+5y^2=p$，$x^2+5y^2=q$ がともに有理整数解を持つので，N(**P**)$=p$，N(**Q**)$=q$ となるイデアル**P**，**Q**はともに単

項イデアルである．だから最初から**P**，**Q**を単項イデアルとして扱っても良いのであるが，上の解法は，$p,\ q$ がともに $x\equiv 3,\ 7\ (\mathrm{mod}.\ d)$ に属する場合にも適用できる．

例(2)：$p,\ q\equiv 3,\ 7\ (\mathrm{mod}.\ d)$ に属する二つの有理素数を $p=23,\ q=43$ とすれば，方程式(9−1−4) は，$x^2+5y^2=23\cdot 43=989$．求める単項イデアルを **J**$=x+y\sqrt{-5}$ とおく．このとき **P**$=[23,\ k+\sqrt{-5}]$，**Q=**$[43,\ l+\sqrt{-5}]$ と置けば，

$$\mathbf{J}=\mathbf{PQ}\quad \therefore\ \mathrm{N}(\mathbf{J})=\mathrm{N}(\mathbf{P})\cdot\mathrm{N}(\mathbf{Q}).$$

そして $k^2\equiv -5\equiv 18\ (\mathrm{mod}.\ 23)$，$l^2\equiv -5\equiv 38\ (\mathrm{mod}.\ 43)$ の条件から $k=8,\ l=9$ が得られる．よって，**P**$=[23,\ 8+\sqrt{-5}]$，**Q=**$[43,\ 9+\sqrt{-5}]$ となる（これらは $p,\ q$ が $x\equiv 3,\ 7\ (\mathrm{mod}.\ d)$ に属するので単項イデアルにはなり得ない）．

まず，**P**$=[23,\ 8+\sqrt{-5}]$ より，$\mathrm{N}(8+\sqrt{-5})=69=23\times 3$．$\mathrm{N}(\mathbf{P})=23$．**R**$=[3,\ 1-\sqrt{-5}]$ と置けば $\mathrm{N}(\mathbf{R})=3$．ゆえに，$8+\sqrt{-5}=\mathbf{PR}$ …①．

一方，**Q=**$[43,\ 9+\sqrt{-5}]$ より，$\mathrm{N}(9+\sqrt{-5})=86=43\times 2$．**L**$=[2,\ 1-\sqrt{-5}]$ とおけば，$9+\sqrt{-5}=\mathbf{QL}$ …②．

①×②より，**PQRL**$=(8+\sqrt{-5})(9+\sqrt{-5})=67+17\sqrt{-5}$．また**LR**$=1-\sqrt{-5}$ だから，

$$\mathbf{PQ}=\frac{67+17\sqrt{-5}}{1-\sqrt{-5}}=3+14\sqrt{-5}.$$

他の解は，**Q'**$=[43,\ 9-\sqrt{-5}]$ として **Q'L**$=9-\sqrt{-5}$．あとは同様に，**PQ'RL**$=(8+\sqrt{-5})(9-\sqrt{-5})=77+\sqrt{-5}$．よって，

$$\mathbf{PQ'}=\frac{77+\sqrt{-5}}{1-\sqrt{-5}}=12+13\sqrt{-5}.$$

以上から，$(x,\ y)=(3,\ 14),\ (12,\ 13)$ が得られる．

上の例では，**R**$=[3,1-\sqrt{-5}]$や **L**$=[2,1-\sqrt{-5}]$を$[3,1+\sqrt{-5}]$，$[2,1+\sqrt{-5}]$としていないのは，後の方で，$67+17\sqrt{-5}$や$77+\sqrt{-5}$を$1+\sqrt{-5}$で割ったのでは単項イデアルが得られないからである．このように，非単項素イデアルの底を臨機応変に対応させることが必要である．

【5】a が一般の合成数のとき

【1】～【4】の解法からわかるように，方程式

$$(9-1)\quad x^2+5y^2=a\qquad (a\text{ は有理正整数の定数})$$

の原始解（$x,\ y$ は互いに素）を求めるためには，まず右辺の a を素因数分解し，その素因数中に，

(1) 平方因数k^2があればx, yは互いに素ではないので，左辺のx, yを$x=kx'$, $y=ky'$と置き換えて両辺をk^2で割り，x', y'が互いに素であるようにする（x', y'を求めたのちにx, yをk倍して解を得る）．

平方因数を取り除いた後の残った素因数中に，

(2) $x\equiv 11,13,17,19 \pmod{d}$に属するものが入っていればその方程式は有理整数解を持たないと結論づけることができる．具体的に列記すれば，

$$p=11,13,17,19,31,37,59,71,73,79,97,113\cdots.$$

(3) 素因数２および５は一つしか含んではならない．

(4) $x\equiv 1,\ 9 \pmod{d}$の属する有理素数は何個含まれていても良いが，$x\equiv 3,\ 7 \pmod{d}$に属するものは必ず偶数個含まれていなければならない．ただし，素因数２は$x\equiv 3,\ 7 \pmod{d}$の仲間と考えて，偶数個の中に入れること．（$a=2p$のときに述べたようにここでのpは$x\equiv 3,\ 7 \pmod{d}$に属する）．

例：$x^2+5y^2=1314684641$

（$1314684641=541\times 1223\times 1987$．100番目，200番目，300番目の素数の積）

この例は，541が$x\equiv 1,\ 9 \pmod{d}$に，1223と1987が$x\equiv 3,\ 7 \pmod{d}$に属する有理素数なので解がある．つまり，541は単項イデアルのノルム，1223と1987は非単項イデアルであるが２個あるのでその積は単項イデアルのノルムになる．よってこれらの積である1314684641 は 541の単項イデアルと1223と1987の積の単項イデアルの積であるから左辺は単項イデアルのノルムを表す.

左辺のノルムを持つ単項イデアルを$\mathbf{J}=x+y\sqrt{-5}$とおく．$\mathbf{P}=[541,\ k+\sqrt{-5}]$，$\mathbf{Q}=[1223,\ l+\sqrt{-5}]$，$\mathbf{R}=[1987,\ m+\sqrt{-5}]$とおけば，$\mathbf{J}=\mathbf{PQR}$．よって$\mathbf{PQR}$を求める．

それぞれ，$k^2\equiv -5\equiv 536 \pmod{541}$，$l^2\equiv -5\equiv 1218 \pmod{1223}$，$m^2\equiv -5\equiv 1982 \pmod{1987}$．これらから，$k=87$，$l=799$，$m=63$を見つける（これらは表計算ソフトに依った）．

よって，$\mathbf{P}=[541,\ 87+\sqrt{-5}]$，$\mathbf{Q}=[1223,\ 799+\sqrt{-5}]$，$\mathbf{R}=[1987,\ 63+\sqrt{-5}]$となる．

$\mathbf{P}$は単項イデアルになることがわかっているから，$\mathrm{N}(87+\sqrt{-5})=7574=541\times 2\times 7$より，$87+\sqrt{-5}=\mathbf{PL}(7,\ 3+\sqrt{-5})$，ただし$\mathbf{L}=(2,\ 3+\sqrt{-5})$．ゆえに，$\mathbf{L}(7,\ 3+\sqrt{-5})=3+\sqrt{-5}$．

$$\therefore\quad \mathbf{P}=\frac{87+\sqrt{-5}}{3+\sqrt{-5}}=19-6\sqrt{-5}\ .\quad\cdots①$$

次に，$\mathbf{Q}=[1223,\ 799+\sqrt{-5}]$より，$\mathrm{N}(799+\sqrt{-5})=638406=1223\times 2\times 3^2\times 29$．29は$x\equiv 1,\ 9 \pmod{d}$に属するから単項素イデアルに分解できる．$29=\mathrm{N}(3+2\sqrt{-5})$．よって，

$$799+\sqrt{-5}=\mathbf{QL}\cdot 3(3+2\sqrt{-5})\ .\quad\cdots②$$

次に，$\mathbf{R}=[1987,\ 63+\sqrt{-5}]$より，$\mathrm{N}(63+\sqrt{-5})=3974=1987\times 2$．よって，

$$63+\sqrt{-5}=\mathbf{RL}. \quad \cdots③$$

②×③より，

$$(799+\sqrt{-5})(63+\sqrt{-5})=\mathbf{QL}\cdot 3(3+2\sqrt{-5})\cdot\mathbf{RL}=\mathbf{QR}\cdot\mathbf{L}^2\times 3\cdot(3+2\sqrt{-5})$$

ここで$\mathbf{L}^2\times 3=6=(1+\sqrt{-5})(1-\sqrt{-5})$であるのを利用して，両辺を$(1+\sqrt{-5})$で割る．

$$\frac{799+\sqrt{-5}}{1+\sqrt{-5}}\cdot(63+\sqrt{-5})=(1-\sqrt{-5})(3+2\sqrt{-5})\mathbf{QR}$$ [30)]

$$\therefore\ (134-133\sqrt{-5})(63+\sqrt{-5})=(-7+5\sqrt{-5})\mathbf{QR}$$

$$\therefore\quad \mathbf{QR}=\frac{(134-133\sqrt{-5})(63+\sqrt{-5})}{-7+\sqrt{-5}}$$

$$=1551-70\sqrt{-5}$$

そして，**J**=**PQR**は，

$$\mathbf{J}=\mathbf{PQR}=(19-6\sqrt{-5})(1551-70\sqrt{-5})$$

$$=27369-10636\sqrt{-5}$$

となる．他の解は，**J**=**P'QR**として（**P'**は**P**の共役数），

$$\mathbf{J}=\mathbf{P'QR}=(19+6\sqrt{-5})(1551-70\sqrt{-5})$$

$$=31569-7976\sqrt{-5}\ .$$

確かめてみれば，$27369^2+5\times 10636^2=31569^2+5\times 7976^2=1314684641$．

以上で方程式 $x^2+5y^2=a$（a は有理正整数の定数）の解法についての記述を終える．

30) この右辺の$1-\sqrt{-5}$は，$1+\sqrt{-5}$でないと正解にたどり着けない．原因はまだわからない．

10. 平方剰余の相互法則

前章（p.61）において，$d=20$ を法とする既約剰余類 $x\equiv 1,3,7,9,11,13,17,19 \pmod{d}$ の中で，二次合同式 $b^2\equiv -5 \pmod{p}$ に解をもつ素数 p は $p\equiv 1,3,7,9 \pmod{d}$ であることを証明なしで用いたが，これなくして方程式 $x^2+5y^2=a$ を解くことができないためやむを得なかったのである．この章ではその根拠をたずね，「平方剰余の相互法則」が『「二次整数論において基本的」な理由』（「**講義**」p.294）を探ろうとするものである．

以下，平方剰余の相互法則を記述するが，そのためにはまず「ルジャンドルの記号」というものを導入しなければならない．

【定義 10.1】 p で割り切れない整数 a （≠0）が p の平方剰余であるかどうかを表す記号として，

$$\left(\frac{a}{p}\right)=1,\ \text{または}\ -1$$

を定める．これを「**ルジャンドルの記号**」という[31]．

括弧の下が法 p を表す[32]．この記号は±1のいずれかを表すだけで，1 なら a は p の平方剰余，−1 なら平方非剰余という意味である．平方剰余であるかどうかを ±1 で示すだけである．本論では $\left(\frac{a}{p}\right)$ を (a/p) と表すこともある．

ルジャンドルの記号のいくつかの性質を示しておく．これらは実際にルジャンドルの記号を計算するときに多用される．

【定理 10.1】 $\left(\frac{1}{p}\right)=1$.

【証明】問題 2.2 参照．1 は常に平方剰余である．‖

ちなみに，0 も（あらゆる整数の）平方剰余であるが，ルジャンドルの記号には用いられない．

【定理 10.2】整数 a, b が法 p に対して合同なら，つまり，$a\equiv b \pmod{p}$ であるなら，

$$\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$$

---

31) 「**講義**」では「Legendreの記号」となっている．ルジャンドル(1752−1833)はフランスの数学者．

32) 分数とは全く異なる記号である．

【証明】まず，a が p の平方剰余なら $(a/p)=1$．このとき，$x^2\equiv a \pmod{p}$ であるが，$a\equiv b \pmod{p}$ なので，$x^2\equiv a\equiv b \pmod{p}$．ゆえに $(b/p)=1$．$\therefore (a/p)=(b/p)$．

また，$(a/p)=-1$ ならば，$x^2\not\equiv a\equiv b \pmod{p}$ より，$(b/p)=-1$．$\therefore (a/p)=(b/p)$．‖

同じ意味で，$\left(\dfrac{a}{p}\right)=\left(\dfrac{a+pc}{p}\right)$，（$c$ は整数）．

例：2は7の平方剰余なので，$(2/7)=1$．このとき，$9\equiv 2 \pmod{p}$ より $(9/7)=1$ となる．また，3は7の平方非剰余なので，$(3/7)=-1$．よって，$\left(\dfrac{3-7}{7}\right)=\left(\dfrac{-4}{7}\right)=-1$．

次の性質もよく使われる（この証明は「ガウス整数論」の第98条を参考にした）．

【定理 10.3】$\left(\dfrac{ab}{p}\right)=\left(\dfrac{a}{p}\right)\left(\dfrac{b}{p}\right)$.

【証明】(1) $(a/p)=1,\ (b/p)=1$ のとき：

$a\equiv a'^2$, $b\equiv b'^2 \pmod{p}$ となる数 a', b' が $1,2,\cdots,p-1$ の中にある．ゆえに $ab\equiv a'^2\cdot b'^2=(a'b')^2 \pmod{p}$．つまり ab は p の平方剰余である．よって，$\left(\dfrac{ab}{p}\right)=1$．

$$\therefore \left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

(2) 一方が平方剰余，他方が平方非剰余のとき：

仮に $(a/p)=1,\ (b/p)=-1$ とすれば，$a\equiv a'^2 \pmod{p}$ …①となる数 a' があるが，b は平方非剰余である．もし ab が平方剰余ならば，$ab\equiv k^2 \pmod{p}$ …②となる k が存在する．このとき c を合同式 $a'x\equiv k \pmod{p}$ の解とすれば $a'c\equiv k \pmod{p}$ となる．これを②に代入して $ab\equiv a'^2c^2 \pmod{p}$．両辺を① $a\equiv a'^2$ で割れば $b\equiv c^2 \pmod{p}$． すなわち，b が p の平方剰余となって仮定に反する．ゆえに ab は平方非剰余である．$\therefore \left(\dfrac{ab}{p}\right)=-1$．一方，$\left(\dfrac{a}{p}\right)\left(\dfrac{b}{p}\right)=-1$．

$$\therefore \left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right).\quad (\ (a/p),\ (b/p) \text{が逆でも同じ})$$

(3) $(a/p)=-1,\ (b/p)=-1$ のとき：

定理 2.1によれば，p の（0を除く）剰余類 $p-1$ 個のうち，平方剰余は $(p-1)/2$ 個あり，平方非剰余も $(p-1)/2$ 個である．仮定により a, b は平方非剰余に属する．ab もいずれかに属する．このうちの平方剰余の各数を c_i（$i=1,2\cdots,(p-1)/2$）として，これら全てに a をかけると ac_i に

なる．これら ac_i はすべて上記(2)によって平方非剰余であるが，この中には ab は存在しない．なぜなら ab は(平方非剰余)×(平方非剰余)であり，ac_i は(平方非剰余)×(平方剰余)だからである．ab が平方非剰余の中にない以上は ab は平方剰余である．ゆえに，$\left(\frac{ab}{p}\right)=1$．一方，$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)=(-1)(-1)=1$．ゆえに，$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

以上，(1)，(2)，(3) を合わせて，$\left(\frac{a}{p}\right),\left(\frac{b}{p}\right)$ の値に関わらず $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ が成り立つ．‖

定理 10.5 を繰り返し続けることで，$\left(\frac{abc\cdots}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\left(\frac{c}{p}\right)\cdots$ が成り立つ.

さて，相互法則には，その補完と実用を兼ねるような二つの「補充法則」と呼ばれるものが二つあるのでそちらを先に紹介しよう.

まず，奇素数 p に関して $x^2\equiv -1\ (\mathrm{mod}.\ p)$，つまり，法 p に対する平方剰余が− 1 になるものがあるかあるかどうかを判定する公式がある．それは，

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$$

というもので，これは相互法則の「**第一補充法則**」と呼ばれている便利な公式である．これによれば，二次合同式 $x^2\equiv -1\ (\mathrm{mod}.\ p)$ をわざわざ解かなくても解があるかどうかを判定することができる．例を挙げると，

$p=3$ なら $\left(\frac{-1}{3}\right)=(-1)^{\frac{3-1}{2}}=-1$ なので平方非剰余，$x^2\equiv -1\ (\mathrm{mod}.\ 3)$ には解はないことを示す.

$p=5$ なら $\left(\frac{-1}{5}\right)=(-1)^{\frac{5-1}{2}}=(-1)^2=1$ なので平方剰余，解は $x\equiv 2,\ 3\ (\mathrm{mod}.\ 5)$.

$p=7$ なら $\left(\frac{-1}{7}\right)=(-1)^{\frac{7-1}{2}}=(-1)^3=-1$ なので平方非剰余，$x^2\equiv -1\ (\mathrm{mod}.\ 7)$ は解なし.

剰余 a が大きくなるほど普通の計算で解の有無を確かめるのは大変だが，例えば，

$p=7919$ なら $\left(\frac{-1}{7919}\right)=(-1)^{\frac{7919-1}{2}}=(-1)^{3959}=-1$ なので，$x^2\equiv -1\ (\mathrm{mod}.\ 7919)$ は解なし.

この第一補充法則は，二次合同式 $x^2\equiv a\ (\mathrm{mod}.\ p)$ で，a が -1 に限定されていることで「補充」法則と呼ばれているが，実用性からいっても重要であるので単独に証明しておこう.

【定理 10.4】（平方剰余の相互法則の「第一補充法則」） p を奇数の素数とするとき，

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}.$$

【証明】素数が $p=4n+1$ の型（n は自然数）なら，定理 2.4 より，-1 が法 p の平方剰余になる整数が存在する．すなわち，$x^2 \equiv -1 \pmod{p}$ に解がある．ゆえに，

$$\left(\frac{-1}{p}\right)=1.$$

また，p が $4n+3$ 型の素数ならば，$p-1=4n+2=2(2n+1)$ で，$2n+1$ は奇数である．このとき，フェルマーの小定理（定理 2.3）より，$x^{p-1}=x^{2(2n+1)} \equiv 1 \pmod{p}$ となるが，この $x^{2(2n+1)}$ は x^2 の奇数乗で，それが $\equiv 1$ であるから，$x^2 \equiv 1 \pmod{p}$ となり，$x^2 \equiv -1 \pmod{p}$ ではあり得ない．よって，$x^2 \not\equiv -1 \pmod{p}$．ゆえに，

$$\left(\frac{-1}{p}\right)=-1.$$

以上から，p が $4n+1$ の型なら $(p-1)/2$ が偶数に，$4n-1$ 型なら $(p-1)/2$ が奇数になるため，上の二つの等式を一つにまとめて表して，

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}. \quad \|$$

定理 10.4 からただちに言えることは，$\left(\frac{-1}{p}\right)=1$ が成り立つための必要十分条件は，素数 p が $4n+1$ 型であること，合同式でいえば，$p \equiv 1 \pmod{4}$ である．

次に，相互法則の「**第二補充法則**」と呼ばれているものは，2 が法 p の平方剰余であるかどうかを判定する公式である．p はもちろん奇素数である．

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}.$$

「**講義**」p.75 に見事な「説明」が述べられているので，それをそのまま紹介する．

「すべて奇数 m は $8n\pm1$ または $8n\pm5$ の形の数である．これらの二つの場合において，それぞれ $(m^2-1)/8$ は偶数または奇数である．

実際

$$\frac{(8n\pm1)^2-1}{8}=8n^2\pm2n \qquad \text{（偶数），}$$

$$\frac{(8n\pm5)^2-1}{8}=8n^2\pm10n+3 \qquad \text{（奇数）．}$$

故に（３）の意味は次のとおりである．（筆者注：(3)とは第二補充法則のこと）

m が $8n\pm1$ の形か，または $8n\pm5$ の形かの素数であるに従って，$\left(\dfrac{2}{p}\right)$ は＋1 または−1 である．すなわち，合同式 $x^2\equiv 2 \pmod{p}$ に解があるために必要かつ十分な条件は

$p\equiv\pm1 \pmod{8}$．」

これも例を上げておこう．

$p=3$ なら $\left(\dfrac{2}{3}\right)=(-1)^{\frac{3^2-1}{8}}=(-1)^1=-1$．平方非剰余，$x^2\equiv 2 \pmod{3}$ には解はない．

$p=7919$ なら $\left(\dfrac{2}{7919}\right)=(-1)^{\frac{7919^2-1}{2}}=(-1)^{7838820}=1$ なので，$x^2\equiv 2 \pmod{7919}$ に解がある（$x\equiv 89 \pmod{7919}$ など）．実際には $(7919^2-1)/8=(7919+1)(7919-1)/8$で約分して偶・奇だけわかればいいのである．

第二補充法則の証明も「ガウス整数論」を参考にする．これは帰納法と背理法を組み合わせたような証明法で，このあとの相互法則自身の証明にも用いられている，なかなか興味深いものである．．以下は「ガウス整数論」第112条に出ているものを筆者が勝手に解釈（換骨奪胎？）したものなので，記述についてはガウスに，というより訳者の高瀬正仁氏に責任はない．

【定理 10.5】（平方剰余の相互法則の「第二補充法則」） p を奇数の素数とするとき，

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}.$$

【証明】まず，2を平方剰余とする素数（二桁）を集めてみると，7，17，23，31，41，47，71，73，79，89，97 となる．これらの素数を $8n+a$ の型に照らしてみると，すべて $8n-1$ か $8n+1$ 型である．言い換えれば，二桁の素数で2を平方剰余とするものは $8n+3$ および $8n+5$ 型（$=8n\pm5$ 型）のものは見当たらない．これは重要な前提である．

すべての奇数が $8n\pm1$ 型または $8n\pm5$ 型のどれかに当てはまることは自明だから，奇素数も必ずこれらのうちのどれかに属する．したがって2を平方剰余とする $8n\pm5$ 型の素数は存在しないことが予想される．実際，上記のように100以下には存在しない．

そこで 101 以上の素数の中に，$8n\pm5$ 型で，2が平方剰余となるものが存在したと仮定して，その中の最も小さいものを t とする．ここで，

$$(10-1)\quad x^2\equiv 2 \pmod{t}$$

とおけば，この合同式は解を持つことになり，また，その解 x を t より小さい正の奇数とすることができる（x が解なら，$x^2\equiv(t-x)^2 \pmod{t}$ より，$t-x$ も解である．x と $t-x$ は一方が奇数，他方が偶数である．定理 2.1 参照）．このとき x^2 は $8n+1$ 型の数である．なぜなら x は奇数だから $x=2m+1$ と置き，m を偶数・奇数に場合分けしても結果はどちらも $8n+1$型になる．

$m=2m'$（偶数）の時：$x^2=(2m+1)^2=(2\cdot 2m'+1)^2=8(2m'^2+m')+1$，

$m=2m'+1$（奇数）の時：$x^2=(2m+1)^2=\{2(2m'+1)+1)\}^2=8(2m'^2+3m'+1)+1$.

すると，(10−1) から二次方程式$x^2-2=t\cdot u$が成り立つようなuがいくらでも存在するが，このuをtより小さい素数として採ることができる．すなわち$u<t$．このとき，$8n+1$型のx^2から２を引けば$8n-1$型になるから $x^2-2=t\cdot u$ は$8n-1$型の奇数である．

さて，もしtが$8n\pm5$型の素数なら，uは$8n\mp5$型の数になる（複号同順）．なぜなら，$u=8m\mp5$として，$t\cdot u$を計算すれば，

$$t\cdot u=(8n\pm5)(8m\mp5)=8(8mn\mp5n\pm5m-3)-1 \quad \text{（複号同順）}$$

と$8n-1$型になるが，それ以外の型では積$t\cdot u$が$8n-1$型にならないからである（試してください）．こうしてuはtより小さい$8n\pm5$型の素数となるのである．

一方，$x^2-2=t\cdot u$ から$x^2\equiv2 \pmod{u}$でもあるから，２はtより小さいuの平方剰余でもあることになるが，これはtが２を平方剰余とする$8n\pm5$型の最小の素数であるいう仮定に反する．つまり，２を平方剰余とする$8n\pm5$型の素数はあり得ないのである．よって，２を平方剰余とするすべての素数は$8n-1$または$8n+1$型でなければならないことが証明された．

さて，奇素数pが$8n-1$または$8n+1$型（$8n\pm1$型）であれば，２を平方剰余とするから，

$$(10-2)\quad \left(\frac{2}{p}\right)=1,\quad \frac{p^2-1}{8}=\frac{(8n\pm1)^2-1}{8}=8n^2\pm2n \text{（偶数）}\therefore (-1)^{\frac{p^2-1}{8}}=1.$$

pが$8n+3$または$8n+5$型（$8n\pm5$型）であれば，

$$(10-3)\quad \left(\frac{2}{p}\right)=-1,\quad \frac{p^2-1}{8}=\frac{(8n\pm5)^2-1}{8}=8n^2\pm10n+3 \text{（奇数）}\therefore (-1)^{\frac{p^2-1}{8}}=-1.$$

(10−2)，(10−3)を合わせて．

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}.\quad \|$$

本論は常に「**講義**」をお手本として記述してきたのであるから，定理 10.2，10.3 および 10.5 の証明も「講義」のものを採りたいのはやまやまである．しかし，「**講義**」の証明にはここで紹介していないいくつかの前提理論（指数の理論，オイラーの基準，ガウスの予備定理など）が駆使されており，そのため非常に簡潔かつ明快でありながら，ここでは紹介できなかった．筆者の独断をご容赦ください．

これまでのルジャンドルの記号の性質および補充法則を用いて，37 が 41 の平方剰余であるかを求めてみよう．つまり$\left(\frac{37}{41}\right)$の計算である．これが 1 になれば平方剰余，−1なら平方非剰余である．まず，$41\equiv4 \pmod{37}$ なので，定理 10.2 により，

$$\left(\frac{41}{37}\right)=\left(\frac{4}{37}\right).$$

次に，定理 10.3 より，

$$\left(\frac{4}{37}\right)=\left(\frac{2}{37}\right)\left(\frac{2}{37}\right)$$

で，第二補充法則より，$(2/37)=(-1)^{\frac{37^2-1}{8}}=(-1)^{171}=-1$ なので，

$$\left(\frac{4}{37}\right)=(-1)(-1)=1.$$

ゆえに，$\left(\frac{37}{41}\right)=1$．となる．すなわち，37は41の平方剰余である．実際，$x^2\equiv 37\ (\mathrm{mod}.\ 41)$ の解は $x\equiv 18,\ 23\ (\mathrm{mod}.\ 41)$ である（$18^2=41\times 7+37$，$23^2=41\times 12+37$）.

さて，ここまで来たことで，この章の目的である「$d=20$ を法とする既約剰余類 $p\equiv 1,3,7,9,11,13,17,19\ (\mathrm{mod}.\ d)$ の中で，二次合同式 $b^2\equiv -5\ (\mathrm{mod}.\ p)$ に解をもつ素数 p は $p\equiv 1,3,7,9\ (\mathrm{mod}.\ d)$ である」ことが証明される．本論では二次体の整数を $Z[\sqrt{-5}]$ に限っていることで，相互法則そのものを用いなくともその補充法則だけでこれを証明することができるのである．いずれにしても相互法則（の補充法則）による簡明な証明を先にみることで，すぐあとの相互法則の証明の困難さを克服するための動機となると確信するからである．

【定理 10.6】20を法とする既約剰余類 $p\equiv 1,3,7,9,11,13,17,19\ (\mathrm{mod}.\ 20)$ のうち，−5が平方剰余となるものは $p\equiv 1,3,7,9\ (\mathrm{mod}.\ 20)$ だけである.

【証明】 $p\equiv 1,3,7,9,11,13,17,19\ (\mathrm{mod}.\ 20)$ の中で，−5が p の平方剰余であるものを取り出せばいいのであるが，定理 10.2 と相互法則の第一補充法則により，

$$(10-4)\quad \left(\frac{-5}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{5}{p}\right)=(-1)^{(p-1)/2}\left(\frac{5}{p}\right)$$

である．この式に $p\equiv 1,3,7,9,11,13,17,19\ (\mathrm{mod}.\ 20)$ を順次当てはめていくことで $\left(\frac{-5}{p}\right)$ の値を判定する.

まず，$p\equiv 1\ (\mathrm{mod}.\ 20)$ とすると，$p=20t+1$ とおいて，$(p-1)/2$ を計算すれば，

$$(p-1)/2=(20t+1-1)/2=10t$$

は偶数だから，$(-1)^{(p-1)/2}=1$．また，$p\equiv 1\ (\mathrm{mod}.\ 5)$ である（20で割って1余る数は5で割っても1余る）から，1はすべての数の平方剰余である（定理 10.1）．よって，

$$\left(\frac{-5}{p}\right)=1\cdot 1=1.$$

次に，$p\equiv 3\ (\mathrm{mod}.\ 20)$ なら，$(p-1)/2$ は上記と同様に $p=20t+3$ とおいて，

$$(p-1)/2=(20t+3-1)/2=10t+1$$

となって奇数だから，$(-1)^{(p-1)/2}=-1$．そして $p\equiv 3\ (\mathrm{mod}.\ 5)$ であるが．3は法5の平方剰余ではない．よって $(3/p)=-1$．ゆえに (10−4) の値は，

$$\left(\frac{-5}{p}\right)=(-1)(-1)=1.$$

次に，$p\equiv 7 \pmod{20}$ なら，$(p-1)/2$ も奇数だから，$(-1)^{(p-1)/2}=-1$．そして $p\equiv 2 \pmod{5}$ である（20で割って７余る数は５で割れば２余る）が，２も法５の平方剰余ではない．よって $(2/p)=-1$．ゆえにこれも (10−4) の値は，

$$\left(\frac{-5}{p}\right)=(-1)(-1)=1.$$

次に，$p\equiv 9 \pmod{20}$ なら，$(p-1)/2$ は偶数だから，$(-1)^{(p-1)/2}=1$．そして $p\equiv 4 \pmod{5}$ である（20で割って９余る数は５で割れば４余る）．４は法５の平方剰余である．よって $(4/p)=1$．ゆえに (10−4) の値は，

$$\left(\frac{-5}{p}\right)=1\cdot 1=1.$$

さて，次に $p\equiv 11 \pmod{20}$ なら，$(p-1)/2$ は奇数だから，$(-1)^{(p-1)/2}=-1$．そして $p\equiv 1 \pmod{5}$ である（20で割って11余る数は５で割れば１余る）．１は平方剰余である．よって $(1/p)=1$．ゆえに (10−4) の値は，

$$\left(\frac{-5}{p}\right)=(-1)\cdot 1=-1.$$

次に $p\equiv 13 \pmod{20}$ なら，$(p-1)/2$ は偶数だから，$(-1)^{(p-1)/2}=1$．そして $p\equiv 3 \pmod{5}$ である（20で割って13余る数は５で割れば３余る）．３は法５の平方非剰余である．よって $(3/p)=-1$．ゆえに (10−4) の値は，

$$\left(\frac{-5}{p}\right)=1\cdot(-1)=-1.$$

次に $p\equiv 17 \pmod{20}$ なら，$(p-1)/2$ は偶数だから，$(-1)^{(p-1)/2}=1$．そして $p\equiv 2 \pmod{5}$ である（20で割って17余る数は５で割れば２余る）．２は法５の平方非剰余である．よって $(2/p)=-1$．ゆえに (10−4) の値は，

$$\left(\frac{-5}{p}\right)=1\cdot(-1)=-1.$$

最後に $p\equiv 19 \pmod{20}$ なら，$(p-1)/2$ は奇数だから，$(-1)^{(p-1)/2}=-1$．そして $p\equiv 4 \pmod{5}$ である（20で割って19余る数は５で割れば４余る）．４は法５の平方剰余である．よって $(4/p)=1$．ゆえに (10−4) の値は，

$$\left(\frac{-5}{p}\right)=(-1)\cdot 1=-1.$$

以上の結果，$p\equiv 1,3,7,9,11,13,17,19 \pmod{20}$ のうち，−５が平方剰余となるものは $p\equiv 1,3,7,9 \pmod{20}$ だけで，$p\equiv 11,13,17,19 \pmod{20}$ は−５が平方非剰余であることが証明された．‖

いよいよ本題の「平方剰余の相互法則」に入る．以下の等式がそれである．

【定理 10.7】（平方剰余の相互法則） p, q を互いに異なる奇素数とすれば,

$$(10-5)\quad \left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

これも「**講義**」p.74 にある「説明」を引用する．

「奇数 m が $4n+1$ の形かまたは $4n-1$ の形かであるに従って，$(m-1)/2$ は偶数または奇数である．実際

$$\frac{(4n+1)-1}{2}=2n,\quad \frac{(4n-1)-1}{2}=2n-1.$$

故に（1）の意味は次の通りである．（筆者注：(1)とは平方剰余の相互法則(10−5)のこと）

p, q のうち少なくとも一つが $4n+1$ の形の素数ならば，$\left(\frac{p}{q}\right)$ と $\left(\frac{q}{p}\right)$ とはともに+1または −1 で，すなわち相等しい．p も q も $4n-1$ の形の素数であるときに限って，$\left(\frac{p}{q}\right)=-\left(\frac{q}{p}\right)$．」

同じ箇所で「**講義**」は次のように語っている．平方剰余の相互法則は，

「すでにEuler（筆者注：オイラー）が帰納的に発見したもので，Legendre（筆者注：ルジャンドル）はそれを上記のような形に書き表わし，かつその証明を試みたのであるが，彼はその証明において，算術級数中に素数の存在することを証明なしに仮定したから，その証明は完全ということを得なかった．相互法則の最初の完全なる証明はGauss（同：ガウス）の功績に帰する．Gaussは相互法則を整数論の基本定理と名づけ，六つの全く趣を異にする証明を与えた．」（「**講義**」p.75）

この法則の「最初の完全なる証明」者であるガウスはその著書の中で次のように述べている．

「p が $4n+1$ という形の素数なら $+p$ は，また p が $4n+3$ という形の素数なら $-p$ は，正に取るときに p の剰余となる任意の素数の剰余であり，正に取るときに p の非剰余となる任意の素数の非剰余である．

平方剰余に関して語りうる事柄のほとんどすべてはこの定理に支えられているのであるから，我々がこれから使用する**基本定理**（筆者注：強調は原文）という呼称は決して不適切ではあるまいと思われる．」
（「ガウス整数論」 第131条　高瀬正仁訳　朝倉書店）

さて，相互法則の証明であるが，「**講義**」にある証明（p.78）は「格子を利用」した「最も簡明」なものでありながら，これも証明の中で「ガウスの予備定理」等を用いているため，ここでは「ガウス整数論」（第137条以降）の厳密な証明を筆者が要約（換骨奪胎？）したあくまで簡易的なものを紹介する．とはいえ，それでも次のような「予備定理」を準備しなければならない．これらは証明の中で使われる整数の平方剰余に関する若干の性質をあらかじめ確認しておくもので，「ガウス整数論」の第132条にあるものと全く同じものである．

【定理 10.8】 a を $4n+1$ 型の素数, b を $4n+3$ 型の素数, A を $4n+1$ 型の合成数, B を $4n+3$ 型の合成数とする．平方剰余の相互法則が成り立つとき,

(1) $(\pm a/A)=1$ ならば $(\pm A/a)=1$

(2) $(\pm b/A)=1$ ならば $(A/b)=1$ または $(-A/b)=-1$

(3) $(a/B)=1$ ならば $(\pm B/a)=1$.

(4) $(-a/B)=1$ ならば $(\pm B/a)=-1$.

(5) $(b/B)=1$ ならば $(-B/b)=1$ または $(B/b)=-1$.

(6) $(-b/B)=1$ ならば $(B/b)=1$ または $(-B/b)=-1$.

本来ルジャンドルの記号 (q/p) は「q は p で割り切れない数($q\neq 0$)で, p は奇素数」として定義されているが, p が合成数である場合（上記$(\pm a/A)$等）にも (q/p) が意味を持つための記号を改めて導入することはせず，本論ではこれまで通りルジャンドルの記号によって表すことにする．すなわち，$(\pm a/A)=1$ とは「$\pm a$ は合成数 A の平方剰余」という意味を表す（「ガウス整数論」では，$\pm aRA$ が「$\pm a$ は A の平方剰余」，$\pm aNA$ が「$\pm a$ は A の平方非剰余」という記号を用いている）．

定理 10.8 は平方剰余の相互法則が成り立つことが前提であるから，実際に小さい奇素数を素因数とする合成数を当てはめてみるならば,

(1) 13以下の奇素数で $(a/A)=1$ となるものが見つからないので，(1)の対偶を取れば「$(\pm A/a)=-1$ ならば $(a/A)=-1$」であるから，$a=13, A=3\times 7=21$のとき，$(\pm A/a)=(\pm 21/13)=(\pm 8/13)=-1$，$(a/A)=(13/21)=-1$，よってもとの命題も成り立つ.

(2) $b=11, A=5\times 5=25$のとき，$(b/A)=(11/25)=1$ なら $(A/b)=(25/11)=(3/11)=1$；$(-b/A)=(-11/25)=1$ のとき $(-A/b)=(-25/11)=1$．よって成り立つ.

(3) $a=13, B=3^3=27$ のとき，$(a/B)=(13/27)=1$，$(\pm B/a)=(\pm 27/13)=(\pm 1/13)=1$，よって成り立つ.

(4) $-a=-5, B=27$ のとき，$(-a/B)=(-5/27)=(22/27)=1$，$(\pm B/a)=(\pm 27/5)=(\pm 2/5)=-1$，よって成り立つ.

(5) $b=11, B=35$のとき，$(b/B)=(11/35)=1$，$(-B/b)=(-35/11)=(9/11)=1$，$(B/b)=(35/11)=(2/11)=-1$．よって成り立つ.

(6) $-b=-11, B=3\times 5=15$ のとき，$(-b/B)=(-11/15)=(4/15)=1$，$(B/b)=(15/11)=(4/11)=1$ または $(-B/b)=(-15/11)=(7/11)=-1$．よって成り立つ.

【証明】(1)〜(6)をすべて証明することは煩雑なだけでなくあまり意味がないことである．というのはすべて同じ論法で行われるからである．そこで例として(1)のみ以下に証明を記す.

(1)の証明：A を素因数分解して，$A=a_1a_2\cdots b_1b_2\cdots$ とする．ここで a_i は $4n+1$ 型の，b_i は $4n+3$ 型の素因数とする．このとき，$(a/A)=1$ なら，a は A の各素因数の平方剰余である（なぜなら a がどれかの素因数の平方非剰余だったら，a は素因数全体の積である A の平方剰余にはならない）．よって$(a/a_i)=1$，$(a/b_i)=1$.

次に，相互法則 (10−5) が成り立ち，a が $4n+1$ 型であるので (a/a_i) と (a_i/a)，(a/b_i) と (b_j/a) は同符号，よって $(a_i/a)=1$，$(b_j/a)=1$である．そして定理 10.3 により，

$$\left(\frac{A}{a}\right)=\left(\frac{a_1}{a}\right)\left(\frac{a_2}{a}\right)\cdots\left(\frac{b_1}{a}\right)\left(\frac{b_2}{a}\right)=1$$

これで「$(a/A)=1$ ならば $(A/a)=1$」が示された．$(-A/a)$の場合は，$(-A/a)=(-1/a))(A/a)$=であるが，aが$4n+1$型の素数なので，相互法則の第一補充法則により，$(-1/a)=(-1)^{2n}=1$．ゆえに$(-A/a)=(A/a)$である．

以上から「$(a/A)=1$ ならば $(\pm A/a)=1$」が示された．(2)〜(6)も同様に証明される．‖

これで相互法則証明のための準備は整った．

【定理 10.7】（再掲）（平方剰余の相互法則）p, q を互いに異なる奇素数とすれば,

$$(10-5)\quad \left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

【証明】初めに， 13以下の奇素数（3, 5, 7,11,13）で，相互法則 (10−5) が成り立つことを直接確かめる．「13以下」というのは，$4n+1$型と$4n+3$型の素数が少なくとも２個ずつあって相互法則の検証に漏れがないようにするためである．

① p, q のいずれかまたは両方が$4n+1$型：$(p, q)=(5, 3),(7, 5),\cdots,(13, 11)$ のとき（八通り），

(3/5)=−1，(5/3)=−1 ，∴ 左辺= 1，右辺=$(-1)^{2\times1}$= 1．ゆえに成り立つ.

(5/7)=−1，(7/5)=(2/5)=−1 ，∴ 左辺= 1，右辺=$(-1)^{3\times2}$= 1．ゆえに成り立つ.

…（途中略）

(11/13)=−1，(13/11)=−1 ，∴ 左辺= 1，右辺=$(-1)^{6\times5}$= 1．ゆえに成り立つ.

② p, q ともに$4n+3$型：$(p, q)=(7, 3),(11, 3),(11, 7)$のとき.

(3/7)=−1，(7/3)=(1/3)=1 ，∴ 左辺=− 1，右辺=$(-1)^{3\times1}$=− 1．成り立つ.

(3/11)=−1，(11/3)=(2/3)=1 ，∴ 左辺=− 1，右辺=$(-1)^{5\times1}$=− 1．成り立つ.

(7/11)=−1，(11/7)=(4/7)=1 ，∴ 左辺=− 1，右辺=$(-1)^{5\times3}$=− 1．成り立つ.

以上の結果，相互法則 (10−5) は13以下の奇素数に対しては成り立つことがわかった[33]．これを踏まえて議論を進める．

(10−5) が成り立たない素数があるとすれば，それは17以上である．そこでpを相互法則の成り立たない最初の素数と仮定する．これで矛盾が起きれば，pは相互法則の成り立たない最初の素数ではない，すなわちそういう素数はないことになり，結局すべての奇素数で相互法則が成り立つことが証明される．以下，$p>q$とする．

（1）pが$4n+1$型のとき：

① $(p-1)/2$が偶数であるから (10−5) の右辺は 1．よって，pになって (10−5) が成り立たないのであれば左辺は−1 でなければならない．すなわち (q/p) と (p/q) は異符号でなければならない．これが仮定である．

---

33) 理論上はただ二つの奇素数 5,3 において (3/5)=−1, (5/3)=−1 だけでも十分である.

仮に $(q/p)=1$ とする．q は p の平方剰余になるから $q\equiv e^2 \pmod{p}$ となる偶数の整数 e が存在して $e^2=q+pf$ ($0<f<p$) と置ける（e は偶奇性が選べる）．ここで e^2 は偶数の自乗だから４の倍数，p は $4n+1$ 型，q が $4n+1$ 型なら f は $4n+3$ 型，q が $4n+3$ 型なら f は $4n+1$ 型の奇数でなければならない．そして $e^2=q+pf$ から $q\equiv e^2 \pmod{f}$ でもあるから，q は f の平方剰余，よって，$(q/f)=1$.

ここでもし，f が $4n+1$ 型ならば 定理 10.8 の(2) により，また f が $4n+3$ 型ならば定理 10.8 の(3) により，何れにしても $(f/q)=1$ となる．また，$e^2=q+pf$ から $pf\equiv e^2 \pmod{q}$ でもあるので，$(pf/q)=1$．よって，定理 10.3 より，

$$\left(\frac{pf}{q}\right)=\left(\frac{p}{q}\right)\left(\frac{f}{q}\right) \quad \therefore\ 1=\left(\frac{p}{q}\right)\cdot 1 \quad \therefore\ \left(\frac{p}{q}\right)=1.$$

これは「(q/p)と(p/q)は異符号でならなければならない」という仮定に反する．よって p が $4n+1$ 型ならば相互法則は成り立つ.

（２）p が $4n+3$ 型のとき：q が $4n+3$ 型のときと，$4n+1$ 型のときに分けて証明する.

① q も $4n+3$ 型ならば $(p-1)/2$, $(q-1)/2$ はどちらも奇数であるから (10−5) の右辺は -1 ．よって，(10−5) が成り立たないのであれば左辺は 1 でなければならない．すなわち (q/p)と(p/q)は同符号でなければならない.

仮に $(q/p)=1$ とすれば（１）と同様に $q\equiv e^2 \pmod{p}$ となる偶数 e が存在して $e^2=q+pf$ ($0<f<p$) と置ける．すなわち e^2 は４の倍数になる．このとき p, q がともに $4n+3$ 型であるから f も $4n+3$ 型の奇数になる．$e^2=q+pf$ から q は f の平方剰余であり，$(q/f)=1$ となる．よって定理 10.8 の(5) により $(f/q)=-1$ となる．一方，$e^2=q+pf$ から $pf\equiv e^2 \pmod{q}$ でもあるので pf は q の平方剰余である．ゆえに $(pf/q)=1$．よって定理 10.3 より，

$$\left(\frac{pf}{q}\right)=\left(\frac{p}{q}\right)\left(\frac{f}{q}\right) \quad \therefore\ 1=\left(\frac{p}{q}\right)\cdot(-1) \quad \therefore\ \left(\frac{p}{q}\right)=-1$$

となって「(q/p)と(p/q)は同符号」という仮定に反する．よって，p, q がともに $4n+3$ 型の素数ならば，相互法則は成り立つ.

② q が $4n+1$ 型ならば，$(p-1)/2$ は奇数，$(q-1)/2$ は偶数であるから (10−5) の右辺は 1 ．よって，(10−5) が成り立たないのであれば左辺は -1 でなければならない．すなわち (q/p)と(p/q) は異符号でなければならない.

仮に $(q/p)=1$ とすれば $q\equiv e^2 \pmod{p}$ となる偶数 e が存在して $e^2=q+pf$ ($0<f<p$) と置ける．すなわち e^2 は４の倍数，p は $4n+3$ 型，q は $4n+1$ 型であるから f は $4n+1$ 型の奇数になる．$e^2=q+pf$ から q は f の平方剰余であり，$(q/f)=1$ となる．よって定理 10.8 の (1) より

$(q/f)=1$．一方，$e^2=q+pf$ から $pf\equiv e^2\ (\mathrm{mod}.\ q)$ でもあるので pf は q の平方剰余である．ゆえに $(pf/q)=1$．よって定理 10.3 より

$$\left(\frac{pf}{q}\right)=\left(\frac{p}{q}\right)\left(\frac{f}{q}\right)\quad\therefore\ 1=\left(\frac{p}{q}\right)\cdot 1\quad\therefore\ \left(\frac{p}{q}\right)=1.$$

これは(q/p)と(p/q)は異符号という仮定に反する．よって，pが$4n+3$型，qが$4n+1$型の素数であるとき，(q/p)と(p/q)は同符号となる．

以上，（1），（2）によってすべての奇素数 p, q に対して相互法則 (10−5) が成り立つ．‖

上記に示した「証明」は，あくまでガウスの証明の簡約化されたものである．ガウスの証明はもっと詳しく，もっと精密で，あらゆる例外を逃さず，いささかの曖昧さも残さない完璧なものである．しかしそれをそのままここに記すのは筆者の「初学的」方針に反することなのでやむを得なかった．また「**講義**」における証明も簡明なものでありながら取り上げなかったわけは既述した通りである．

相互法則の本当の意義は筆者などには想像もつかないが，平方剰余であるかないかの計算の苦労をある程度軽減する効果があるのは次の例題からもわかる．これは 365が 1847（素数）の平方剰余であるか否かを求めるものである（「**講義**」p.81 の〔例 2〕より）．

$$\left(\frac{365}{1847}\right)$$

まず，365=5×73 であるから，定理 10.3 により，

$$=\left(\frac{5}{1847}\right)\left(\frac{73}{1847}\right)$$

5 も 73 も$4n+1$型であるから相互法則により上下を入れ替えてもルジャンドルの記号の値は変わらないので,

$$=\left(\frac{1847}{5}\right)\left(\frac{1847}{73}\right)$$

1847≡2 (mod. 5)，および 1847≡22 (mod. 73) であるから定理 10.2 より，

$$=\left(\frac{2}{5}\right)\left(\frac{22}{73}\right)=\left(\frac{2}{5}\right)\cdot\left(\frac{2}{73}\right)\left(\frac{11}{73}\right)$$

第二補充法則より $(2/5)=(-1)^{(5^2-1)/8}=-1$，$(2/73)=(-1)^{(73^2-1)/8}=1$であるから，

$$=-1\cdot 1\cdot\left(\frac{11}{73}\right)=-\left(\frac{11}{73}\right)$$

73 は$4n+1$型であるから (11/73) = (73/11)，また，73≡−4 (mod.11) より，

$$=-\left(\frac{73}{11}\right)=-\left(\frac{-4}{11}\right)$$

$-4=-1\times 2^2$ であるから，

$$=-\left(\frac{-1}{11}\right)\left(\frac{2^2}{11}\right)$$

第一補充法則により，$(-1/11)=(-1)^{(11-1)/2}=-1$．よって，

$$=-(-1)\left(\frac{2^2}{11}\right)=\left(\frac{2^2}{11}\right)$$

最後に，$(2^2/11)$とは，２が平方剰余であると言っているのと同じだから当然＝１，よって結果は，

$$\left(\frac{365}{1847}\right)=1$$

すなわち， 365 は 1847 の平方剰余である．実際 $x\equiv 496, 1351 \pmod{1847}$．

以上で拙論「イデアルとは何か」を終える．読んでくださったことを感謝します．

【付録】

【付録１】 (p.3)

整数の除算では，もし割り切れない時には「余り」（剰余）を考えるのが普通である．これについては次の重要な定理が成り立つが，その証明のためガウスの記号$\left[\ \right]$を使う．

【定理 1.1】a を整数，b を自然数とするならば，

$$a = bq + r, \quad 0 \le r < b$$

が成り立つ整数q, r がただ一組ある．

実数1.2や-3.14などの整数部分を表す記号に**ガウスの記号**$\left[\ \right]$というのがある．これは，

$$[1.2]=1,\ [-3.14]=-4,\ [\pi]=3$$

のように，簡単に言えば小数部分を切り捨てて整数部分だけを取り出す関数であるが，注意しなければならないのは負の数の場合で，$[-3.14]$ は -3ではなく -4 である．数直線でいえば，与えられた実数の位置から常に左側にある直近の整数を表す（実数が整数のときはもちろんそれ自身を表す）．

【証明】a, b に対してガウスの記号$[a/b]=q$ とすると q は整数で，$a/b-q$ は 0 以上 1 より小さい．よって，

$$0 \le \frac{a}{b} - q < 1 \quad \therefore \quad 0 \le a - bq < b.$$

ここで$r = a - bq$ とおくと，$a = bq + r$，$0 \le r < b$.

q, r がただ一組であることを示すには，もし，

$$\begin{aligned} a &= bq_1 + r_1, \quad 0 \le r_1 < b \\ a &= bq_2 + r_2, \quad 0 \le r_2 < b \end{aligned} \qquad (q_1 \ne q_2,\ r_2 > r_1 \text{とする})$$

のようにふた通りの組が見つかったとすれば，$a = bq_1 + r_1 = bq_2 + r_2$ より，

$$b(q_1 - q_2) = r_2 - r_1$$

であるが，$0 \le r_1 < b$, $0 \le r_2 < b$ より，$0 \le r_2 - r_1 < b$．よって$r_2 - r_1$ はb より小さいb の倍数であるから$r_2 - r_1 = 0$．したがって$b(q_1 - q_2) = 0$ より，$q_1 - q_2 = 0$．すなわち，$q_1 = q_2$, $r_1 = r_2$．‖

例：a=20，b=5なら，a/b=4，q=[a/b]=4，20=5×4，r=20−5×4+0=0
a=21，b= 5 なら，a/b=4.2，q=[a/b]=4，4.2−4<1，21=5×4+1, r=21−5×4=1
a=−21，b=5 なら， a/b=−4.2，q=[a/b]=−5，−4.2−(−5)<1，−21=5×(−5)+4，r=−21−5×(−5)=4
（注意：除数 b が負の整数の場合は除算の一意性が問題になるので，ここでは取り上げない）

【付録２】 (p.21)

互いに素である $x,\ y$ で　$p=x^2+y^2$ が成り立つならば，$x+y,\ x-y$ も互いに素である．

【証明】仮に $x+y,\ x-y$ が互いに素でないとすると，1 より大きい共通因数 m がある．ゆえに，$x+y=ma,\ x-y=mb$（$a>1,\ b>1$）とおける．このとき，$x=(ma+mb)/2,\ y=m(a-b)/2$ であるから．

$$p=x^2+y^2=\left(\frac{m(a+b)}{2}\right)^2+\left(\frac{m(a-b)}{2}\right)^2=\frac{m^2}{2}\left(a^2+b^2\right)$$

となるが，右辺は整数にならなければならない．$m>1$ であるから $m^2>2$．よって m^2 が 2 で割り切れても 1 より大きい整数 m' が残って $p=m'(a^2+b^2)$ となって p が素数であることに反する．また，m^2 が割り切れなければ a^2+b^2 が 2 で割り切れなければならない．これも $a>1,\ b>1$ であるから $a^2+b^2>2$．ゆえに割り切れたとしても 1 より大きい整数 m'' が残り，$p=m^2m''$ となる．何れにしても p が素数であることに反する．よって $x+y,\ x-y$ は互いに素でなければならない．‖

【付録3】 (p.24)

$4n+1$ 型の有理素数 k 個の積 $p_1p_2\cdots p_k$ があるとき，それらの積を有理整数の二乗の和に分解すると，2^{k-1}通りの解があることの証明（数学的帰納法）．

【証明】まず二個の場合は本論 p.24 において実際に示されている．また k 個の有理素数は $4n+1$ 型で全てが互いに素でかつ共役数である複素整数に分解できるので，それらを $p_1=A\overline{A}$，$p_2=B\overline{B}$，…，$p_k=P\overline{P}$ とする（$\overline{A},\overline{B},\cdots,\overline{P}$ は $A,B,\cdots,P$ の共役数）．

さて，有理素数が k 個までは2^{k-1}通りあることが示されたと仮定し，実際にそれらの分解を以下に示したとすれば，

$$p_1p_2\cdots p_k=(A\overline{A})(B\overline{B})\cdots(P\overline{P})$$

(1)　$=(AB\cdots P)(\overline{A}\overline{B}\cdots\overline{P})$，$(\overline{A}B\cdots P)(A\overline{B}\cdots\overline{P}),\cdots,(AB\cdots P)(\overline{A}\overline{B}\cdots\overline{P})$

1，　2，　…，2^{k-1}通り

となる．ここで左辺の $p_1p_2\cdots p_k$ に新たな $4n+1$ 型の有理素数 $q=Q\overline{Q}$ を掛ければ，右辺には $Q\overline{Q}$ が新たに増えるので，これまでの2^{k-1}個のそれぞれの組み合わせに対し，$Q,\ \overline{Q}$ とその入れ替えの $\overline{Q},\ Q$ 分の二個ずつが追加される．ゆえに全体の個数は$2\times2^{k-1}=2^k=2^{(k+1)-1}$個である．よって有理素数の個数が $k+1$ 個の場合にも成り立つ．

（上記 (1) の$(AB\cdots P)(\overline{A}\overline{B}\cdots\overline{P})$ に対し，$(AB\cdots PQ)(\overline{A}\overline{B}\cdots\overline{P}\overline{Q})$ と $(AB\cdots P\overline{Q})(\overline{A}\overline{B}\cdots\overline{P}Q)$ が追加される．以下同様に2^{k-1}通りに対して二個ずつ増えるので全体として二倍になる．）‖

あとがき

「2017年2月9日」付けで「はじめに」を書いているから，約半年で書き終えたことになる．とても勉強になった期間であった．誰のためでもない自分のために書いたことがよく理解できた．

「**講義**」の魅力に導かれながら次々に新しい出来事に出会い，小さな感動を積み重ねながら何とか書き続けることができた．一番苦しかったのはやはり「平方剰余の相互法則」である．イデアル論を書いたつもりが，最後の２か月はこの法則の証明をどう記すかに費やした．結局「ガウス整数論」（135条以下）の手法に落ち着いたのは，「**講義**」の証明には，指数の理論，オイラーの基準，ガウスの予備定理，そして最後に「格子の幾何学」を用いていることが，初学者としてはハードルが高過ぎるのではないかと思ったからである．ガウスの方法は複雑ではあるが，代数的計算だけで結論を出していると即断したのがその理由であった．しかし，２か月費やして，いささかの曖昧さもない完璧な証明のために整数のあらゆる性質を理解していることが要求され，決して「初学的」ではないことを思い知らされた．今では妙なこだわりを捨てて「**講義**」の証明に徹することにすればよかったと，反省している．

とはいえ，本論は初等整数論からイデアル論への飛躍を目指した筆者にとって目的の一端を果たしたものにはなった，そういう感慨のある労作である（自画自賛）．

2017年7月29日

【索引】