複素数の素数についてのお話

花巻北高等学校　下町壽男

Ⅰ　ガウスの整数とは

1　ガウスの整数

Z を整数の集合とします。つまり

$Z=\{\cdots\cdots -2,-1,0,1,2,\cdots\cdots\}$　ですね。

ガウスの整数とは、集合 $\{m+ni \mid m,n\in Z\}$ で表されるような複素数のことです。

簡単に言うと、複素数　$a+bi$ について、a も b も整数であるような数のことです。

この集合に名前をつけて

$Z[i]=\{m+ni \mid m,n\in Z\}$　と表すことにしましょう。

例 1.1　$2+3i$, $-1-2i$, $5i$, 7 などがガウスの整数である。

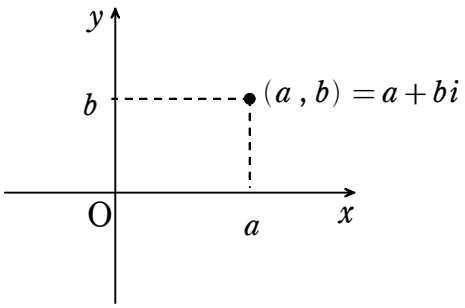
注　ガウスの整数は２つの整数の組を表しています。

そこで、$m+ni=(m,n)$ とベクトルで表現してもいいですね。

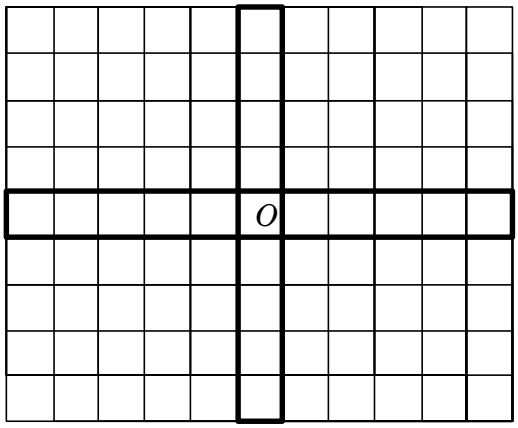
2　複素格子平面

一般に複素数 $a+bi$ （a , b は実数）は、２つの実数の組 (a,b) と考えられるので、これを下図のような平面上の点として表現することができます。

図において、横軸を実軸、縦軸を虚軸といいます。そして、この平面を複素数平面またはガウス平面といいます。



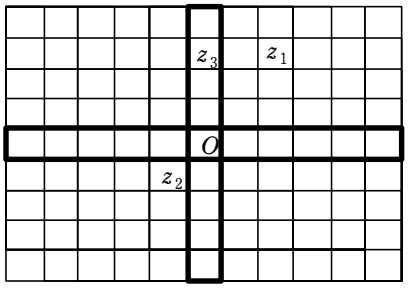
さて、これから考えるのは一般の複素数ではなく、ガウスの整数なので、図のような格子平面上で考えたほうがいいですね。



では、ガウスの整数を格子平面上に図示する練習をしてみましょう。

例 1.2

$z_1=2+3i$, $z_2=-1-i$, $z_3=3i$



3　加法・減法・乗法

複素数の加法減法は、実部は実部どうし、虚部は虚部どうし計算すればよかったですね。つまり、

① 加法　　$(m+ni)+(m'+n'i)=(m+m')+(n+n')i$

② 減法　　$(m+ni)-(m'+n'i)=(m-m')+(n-n')i$

注 $m+ni=(m\,,\,n)$ とベクトルで表現すると、加法は、

$(m\,,n)+(m'\,,\,n')=(m+m'\,,\,n+n')$　というようにベクトルの演算になります。

複素数の加法を定義するときに、$m+ni$ でもう＋ がでてきているではないかと文句をつける人がいますので、そういう意味では、ベクトルで表したほうが便利かもしれません。

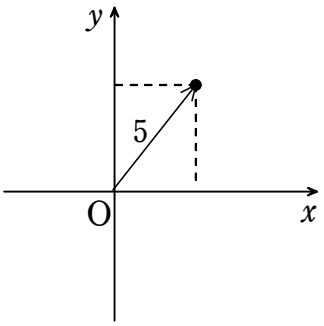
4　ノルム

ガウスの整数　$z=m+ni$ において、m^2+n^2 を z のノルムといいます。$N(z)$ で表します。

例 1.4.1

$z=3+4i$ のとき、$N(z)=3^2+4^2=25$

これは、図形的には複素数平面上の点 $(3\,,4)$ の原点からの距離の２乗を表しています。



つまり、ノルムとは、ガウスの整数（複素数）から正の実数への一つの対応ということがいえます。

ガウスの整数　→　正の整数

例 1.4.2

次のガウスの整数のノルムを求めよ。

(1)　$1+i$　　(2)　$-1+i$　　(3)　$-5i$　　(4)　6

答　(1)　2　(2)　2　(3)　25　　(4)　36

ノルムの性質についてまとめておきます。

① ガウスの整数に対してノルムは１つだけ決まる。
② ノルムは必ず０以上の整数である。
③ $z=a+bi\,,\,z'=c+di$ とすると、$N(zz')=N(z)N(z')$ が成り立つ。

①②の性質はあたりまえですが、③については証明が必要ですね。

③の証明

$$\begin{aligned}N(zz')&=N((a+bi)(c+di))=N((ac-bd)+(ad+bc)i)\\&=(ac-bd)^2+(ad+bc)^2\\&=a^2c^2+b^2d^2+a^2d^2+b^2c^2\\&=a^2(c^2+d^2)+b^2(c^2+d^2)\\&=(a^2+b^2)(c^2+d^2)=N(z)N(z')\end{aligned}$$ 終

上で述べたノルムの性質は後でまた使いますので気にとめておいて下さい。

5　共役

複素数 $a+bi$ に対して、$a-bi$ を共役な複素数といいましたね。これらは、同じ2次方程式から生まれてくるものでした。（同じ2次方程式が産みの親なので、兄弟複素数と呼んでもよさそうですね）

ガウスの整数についても、$m+ni$ に対して、$m-ni$ を共役なガウスの整数と呼ぶことにします。

6　単元

一般に環 R の元 x に対して、$xy=yx=1$ となるような R の元 y が存在するとき、x を環 R の単元という。

これは、普通の本に書いてある単元の定義です。環については後で述べるとして、この定義だけではちょっと解りにくいので、ガウスの整数で具体的に調べてみることにしましょう。

まず、ガウスの整数 $Z[i]$ において、上記の単元の定義を満たすものがあるか調べてみましょう。

まず、$1\cdot1=1$ で、もちろん $1\in Z[i]$ なので、1 は単元です。

$-1\cdot(-1)=1$　$-1\in Z[i]$ なので、-1も単元です。

また、　$i\cdot(-i)=(-i)\cdot i=1$　$i\,,-i\in Z[i]$ なので、$i\,,-i$ も単元です。

以上で、$1\,,-1\,,i\,,-i$ の４つの単元が見つかりました。

さて、単元はそれ以外にはないのでしょうか。実はこの４つ以外に単元がないことが、ノルムを用いて証明することができます。

証明

$x \in \mathbb{Z}[i]$, $y \in \mathbb{Z}[i]$ で、$xy=1$ となるものがあるとする。

このとき、両辺のノルムを考えて、

$N(xy)=N(1)$

$N(x)N(y)=1$　（ノルムの性質③より）

ノルムは必ず0以上の整数なので、$N(x)=1$, $N(y)=1$

よって、x , y は ± 1 , $\pm i$ 以外はありえない。終

7　同伴

$\mathbb{Z}[i]$ の元 $m+ni$ に対して、それに単元をかけたものを同伴元といいます。単元は ± 1 , $\pm i$ でしたから、同伴元は

$(m+ni)\cdot 1=m+ni$

$(m+ni)\cdot(-1)=-m-ni$

$(m+ni)\cdot i=-n+mi$

$(m+ni)\cdot(-i)=n-mi$

となりますね。

例 1.7

$3+2i$ の同伴元とそれらの共役元を求め、図示せよ。

答

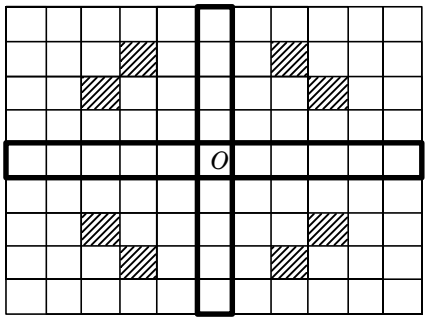
$(3+2i)\cdot 1=3+2i$　共役元は　$3-2i$

$(3+2i)\cdot(-1)=-3-2i$　共役元は　$-3+2i$

$(3+2i)\cdot i=-2+3i$　共役元は　$-2-3i$

$(3+2i)\cdot(-i)=2-3i$　共役元は　$2+3i$

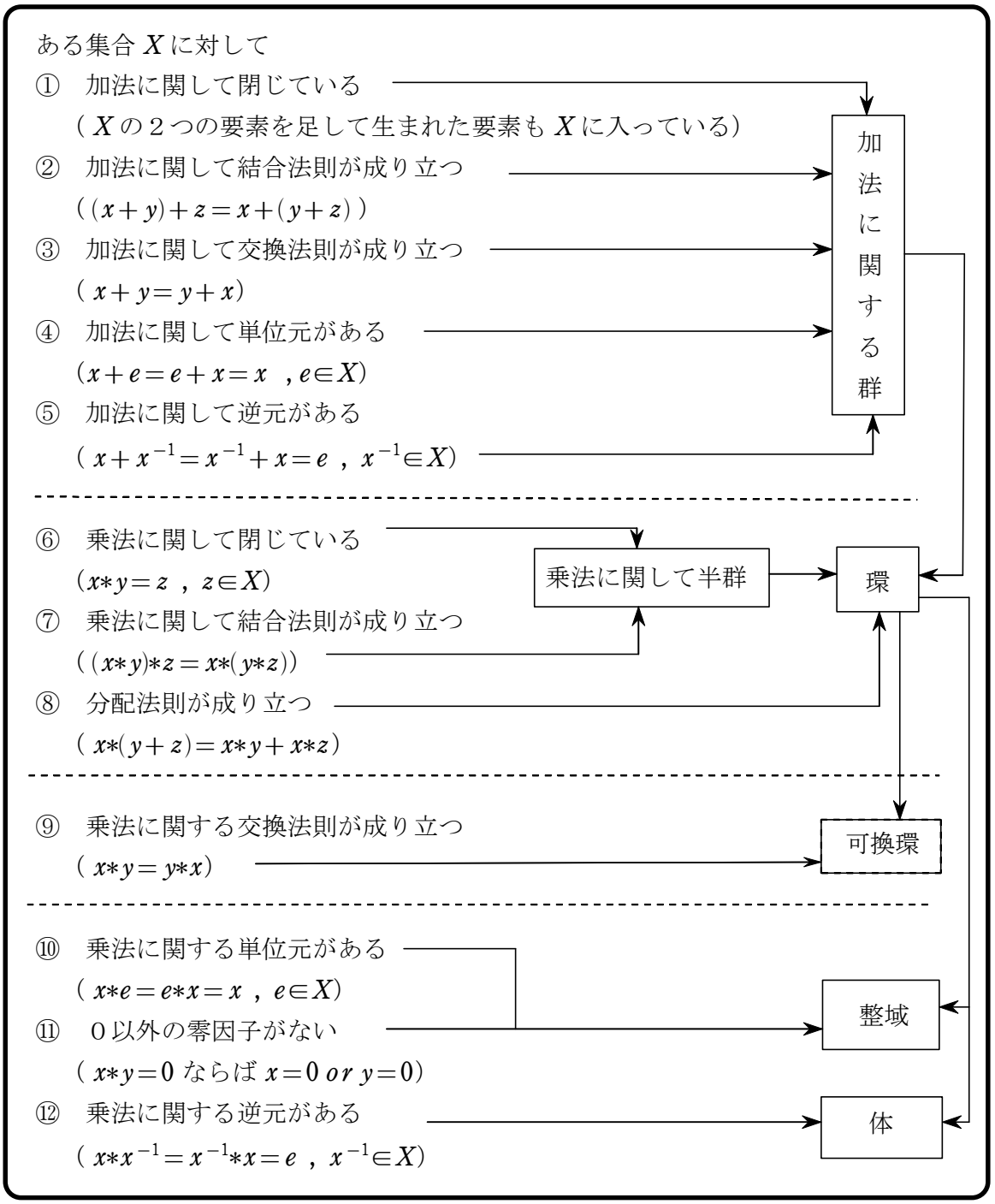
よって、図の網掛け部分である。



Ⅱ　複素数の素数を調べる前に

1　群･環･整域･体

複素数の素数について調べる前に、基礎として、群･環･整域･体などについて簡単にまとめておきましょう。



イメージはつかめましたか。環とは、加群で、更に乗法というもう一つの演算が定義され、それを分配法則がとり結ぶという感じです。整域は０以外の零因子を持たないような環です。数学Ｃで習う行列は、零行列以外にも零因子の存在がありますので整域ではない環です。体とは大雑把にいうと、四則演算が定義される世界ということです。

2　イデアル

ガウスの整数は環の構造になっています（後で調べましょう）。そこで、一般に「ガウスの整数環」と呼ばれます。

さて、次にイデアルについて説明しましょう。

定義は次のようなものです。

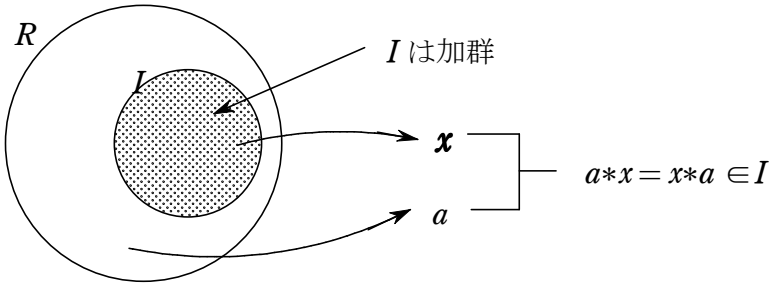
【定義】

環 R の部分集合 I が次の条件を満たすとき、I を R のイデアルという。

（ｉ）　I は加法に関して群になる。

（ii）　$x \in I$ ならば、任意の $a \in R$ に対して　$a*x = x*a \in I$

図で説明すると以下のようになります。



雑にイメージすると、例えば R を整数全体とすると、「3の倍数全体」なんていうのが R のイデアルになるわけですね。

このように見ると、イデアルは単なる「何かの倍数全体の集合」というような感じがしますが、それは「主イデアル」（単項イデアル）と呼ばれるもののイメージです。

一般には次の定理が成り立ちます。

定理2.2

R の有限個の元 $x_1, x_2, x_3, \cdots, x_n$ の一次結合

$a_1x_1 + a_2x_2 + a_3x_3 + \cdots + a_nx_n$　　$(a_k \in R)$　　の全体は R のイデアルになる。

$\alpha, \beta \in I$　として、

$\alpha = a_1x_1 + a_2x_2 + a_3x_3 + \cdots + a_nx_n$　　$\beta = b_1x_1 + b_2x_2 + b_3x_3 + \cdots + b_nx_n$

とおくと、

$\alpha + \beta = (a_1 + b_1)x_1 + (a_2 + b_2)x_2 + \cdots + (a_n + b_n)x_n \in I$

$\forall p \in R$ に対して、$p\alpha = pa_1x_1 + pa_2x_2 + \cdots + pa_nx_n \in I$

となるので、$a_1x_1 + a_2x_2 + a_3x_3 + \cdots + a_nx_n$　の全体はイデアルになることがわかります。このイデアルを、

$I = (x_1, x_2, x_3, \cdots, x_n)$　と表し、I を $x_1, x_2, x_3, \cdots, x_n$ によって生成されるイデアルといいます。

特に、１つの元によって生成されるイデアル $I = (x_1)$ を主イデアル（単項イデアル）というのです。

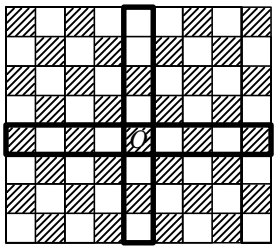
3　ガウスの整数環のイデアル

２で説明したイデアルをガウスの整数環を例にとって示したいと思います。

今、$Z[i]$の１つの元$1+i$で生成されるイデアル$I=(1+i)$を複素格子平面上に図示してみましょう。

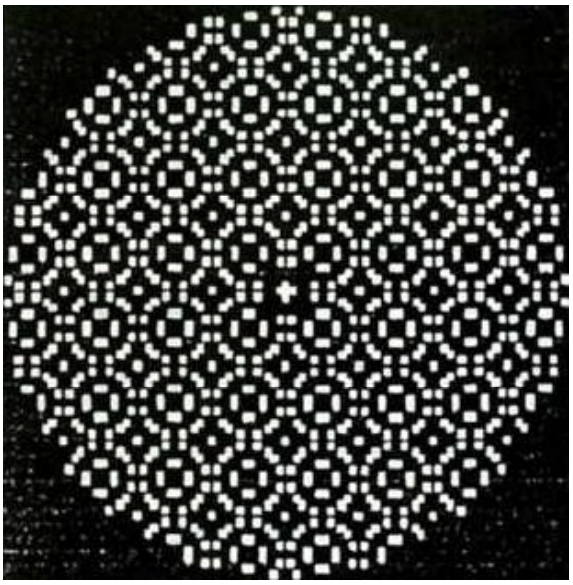
	$Z[i]$の元	Iの元
$(1+i)$	$\cdot\quad 1$	$=1+i$
$(1+i)$	$\cdot\,(-1)$	$=-1-i$
$(1+i)$	$\cdot\quad i$	$=-1+i$
$(1+i)$	$\cdot\,(-i)$	$=1-i$
$(1+i)$	$\cdot\,(1+i)$	$=2i$
……		
……		

左のように計算を行い、Iの元を作ると下のような市松模様ができますね。



$1+i$で生成されるイデアル

下図は、以前コンピュータを使って、$2+3i$から生成されるイデアルを図示したものです。なかなか美しい模様になりますね。



4　整域いろいろ

ガウスの整数の構造を調べる前に、イデアルについて補足しておきましょう。

①　主イデアル整域（P.I.D）

整域の任意のイデアルが主イデアルのとき、その整域を主イデアル整域といいます。つまりどんなイデアルも必ずある元の倍数全体の集合となっているような整域です。例えば、整数全体の集合（整数環といいます）Zにおいて、$6,8$の２つの元で生成されるイデアル（２項イデアル）を考えましょう。

$I=\{6x+8y \mid x, y\in Z\}$　ですね。このとき、$6x+8y=2(3x+4y)$　となるので、$I\subset\{2$の倍数全体$\}$　となることがいえます。

また、$3\cdot3+4\cdot(-2)=1$ とできるので、$\{3x+4y\}$はすべての自然数を生成できます。
このことから、I は２の倍数すべてを生成できることがわかります。
つまり、$I\supset\{2$の倍数全体$\}$ なので、$I=\{2x \mid x\in Z\}$ と２項イデアルは２だけで生成される主イデアルになります。

② ユークリッド整域

整域の任意の元 x（ただし０以外）に対して、整数 $n(x)$ が対応していて、以下の条件を満たすとき、この整域はユークリッド整域であるといいます。

（ｉ） 整域の元 x, y に対して $n(x*y)\geqq n(x)$

（ii） $n=yq+r$ $(n(y)>n(r))$（q, r は整域の元）とできる

例えば、x の整式全体の集合を考えます。任意の整式 $f(x)$ に対して、
$n(f)=dim(f)$ を対応させてみましょう。これは整式の次数を示す値ですね。
整式 f を整式 g で割ったとき、商が q で余りが r のとき、
$f=gq+r$ $(dim(g)>dim(r))$ とできますから、整式はユークリッド整域をなすことがわかります。

ここで、整域に関する大切な定理をまとめておきたいと思います。

【定理】2.4.1

ユークリッド整域は主イデアル整域である。

証明

R をユークリッド整域とし、I を R の任意のイデアルとします。
今、I の最小元を d とします。ここでいう最小元とは、$n(d)$ が最小である元のことです。
さて、I の任意の元を a とすると、R はユークリッド整域だから、
$a=bq+r$ $(n(d)>n(r))$ となるような $q, r\in R$ をとることができます。
もし、$r\neq0$ とすると、$r=a-dq$ この式の前項 a はもちろん I の元です。また後項は d の倍元であり、$d\in I$ だから、やはり I の元です。
ということは、r は、I の元どうしを引いたものなので、r も I の元になるわけですが、そうすると、d の最小性に反します。
従って、$r=0, a=dq$
つまり、a は必ず d の倍元であることがわかります。
a は I の任意の元だったから、$I\subset(d)$（右辺は d で生成される主イデアルですね）
一方、d は I の元だから、d で生成されるイデアルは当然 I に含まれます。
つまり、$I\supset(d)$
以上より $I=(d)$ つまり、I は主イデアルであることがわかります。

【定理】2.4.2

主イデアル整域では任意の元（ただし０と単元を除く）は既約元の積に 一意に分解できる。

整数や整式は一意に因数分解できることはご存知の通りですね。このような整域を一意分解整域（U.F.D）といいます。ガウスの整数も一意分解整域なのですが、このことは後でまた述べましょう。

㊟ 一意に因数分解できるといっても、もちろん単元の因数の違いはあります。
例えば、整数環において、$6=2\cdot3=(-2)\cdot(-3)$ というように同伴元が対応していてもいいのです。

尚、定理2.4.2の証明は省略します。$x=p_1p_2\cdots p_l$、$x=q_1q_2\cdots q_m$ としておいて、任意の i,j に対して、$p_i \neq q_j$ としたとき矛盾を導く方法である i に対し $p_i=q_j$ となることを示せば、以下数学的帰納法により証明できますので興味のある人はやってみてください。

さて、ここまで述べたことをまとめると、以下のようになります。

ユークリッド整域
↓
主イデアル整域
↓
一意分解整域

つまり、ガウスの整数がユークリッド整域であれば、自動的に一意分解整域であることがいえるわけですね。

では、そろそろ本題の「複素数の素数」の話に入っていきましょう。
例えば、５は整数環の世界では素数ですが、考える世界をガウスの整数環にすると、
$5=(2+i)(2-i)$ と因数分解することができます。つまり５はガウスの整数の世界では素数ではないことになります。
$-2+9i$ も$(2+i)(1+4i)$ というように因数分解できますね。しかし、３や７や $2+i$ などはガウスの整数の世界に拡張しても因数分解することはできません。
ではどのような場合に因数分解可能なのか、ガウスの整数で素数であるものはガウス平面上でどのように分布しているのか、などいろいろな疑問が起こってきます。

次の章ではガウスの整数の構造を調べることで、徐々に複素数の素数の実体にせまってみたいと思います。

Ⅲ　ガウスの整数の構造を調べよう

Ⅱの「複素数の素数を調べる前に」のところの表に照らし合わせていけば、ガウスの整数 $Z[i]$ が可換環であることがすぐわかります。

では、更に $Z[i]$ が整域であることを示してみます。

（ⅰ） 乗法に関する単位元　$1 \in Z[i]$ は明らか。

（ⅱ） 零因子について

$a=m+ni$, $b=m'+n'i$　（a , $b \in Z[i]$）　において、

$ab=0$ とすると

$$\begin{cases} mm'-nn'=0 \cdots ① \\ mn'+m'n=0 \cdots ② \end{cases}$$

①より $mm'=nn'$

$m' \neq 0$ とすると

$$m=\frac{nn'}{m'}$$

②より　$\dfrac{nn'^2}{m'}+m'n=0$

よって　$nn'^2+m'^2n=0$

$n(n'^2+m'^2)=0$

$m'^2 \neq 0$ なので $n'^2+m'^2 \neq 0$

よって、$n=0$

このとき　$m=0$

$m=0$ とすると①②から

$n=0$ または $n'=m'=0$ となるので

$ab=0$ ならば $a=0$ または $b=0$

つまり０以外の零因子はない。　㊮

上の(ⅰ)(ⅱ)から$Z[i]$は整域であることがいえました。

次に $Z[i]$ がユークリッド整域になることをいいましょう。

a , $b \in Z[i]$ のとき　$a=bq+r$ とする。

このとき、$\dfrac{a}{b}=q+\dfrac{r}{b}=x+yi$　とおく　（x , $y \in R$）

今、 x , y に最も近い整数を m , n とすると

$$|x-m| \leqq \frac{1}{2} , |y-n| \leqq \frac{1}{2}$$

$q=m+ni \in Z[i]$ とおくと、

$r=a-bq \in Z[i]$

これで、$N(b)>N(r)$ がいえればよい。

$$N(r)=N(a-bq)=N\left(b\left(\frac{a}{b}-q\right)\right)=N(b)N\left(\frac{a}{b}-q\right)$$

$$N\left(\frac{a}{b}-q\right)=N((x-m)+(y-n)i)=(x-m)^2+(y-m)^2\leqq\frac{1}{2}<1$$

よって、$N(r)<N(b)$

以上より $Z[i]$ がユークリッド整域であることが示されました。

今述べたことを実感するために、具体例で説明しましょう。

例えば、$a=5+7i$, $b=1+2i$ としたとき、次のように q , r を決定します。

$$\frac{a}{b}=\frac{5+7i}{1+2i}=\frac{19-3i}{5}=\frac{19}{5}-\frac{3}{5}i$$

ここで、$\frac{19}{5}$, $-\frac{3}{5}$ に最も近い整数 m , n を選ぶと、$m=4$, $n=-1$　となります。

よって、$q=4-i$

$r=5+7i-(1+2i)(4-i)=-1$

つまり、$5+7i=(1+2i)(4-i)-1$　　$(N(1+2i)>N(-1))$ となりました。

例 3.1

$a=8+3i$, $b=1+2i$ のとき、上の方法で

$a=bq+r$　$(N(b)>N(r))$ の形にしてみよ。

答　$\frac{8+3i}{1+2i}=\frac{(8+3i)(1-2i)}{(1+2i)(1-2i)}=\frac{14-13i}{5}$ より、$m=3$, $n=-3$ として

$8+3i=(1+2i)(3-3i)+(-1)$

Ⅳ　複素数の素数を図示するための諸定理

長い準備が完了し、いよいよ「複素数の素数」の話題に入りましょう。「複素数の素数」とは、「ガウスの整数で因数分解できないもの」ということです。このようなガウスの整数を「既約なガウスの整数」と呼ぶことにします。また、因数分解できる場合は可約ということにしましょう。

例えば、$7+6i$ は$Z[i]$ 上、既約だろうか、13はZ 上では素数だが、$Z[i]$上ではどうだろうかなどということを考えていきたいと思います。

では、$Z[i]$ 上既約であるかを判定するためのいくつかの定理を述べましょう。

1　ノルムによる基本的判定法

ノルムの性質　$N(xy)=N(x)N(y)$　を用います。次の例で判定法を示しましょう。

例 4.1

$7+6i$ は$Z[i]$ 上既約であるか。

$7+6i=(a+bi)(c+di)$　とし、両辺のノルムをとると

$49+36=(a^2+b^2)(c^2+d^2)$

$\therefore (a^2+b^2)(c^2+d^2)=85$

ここで、$85=5\cdot 17$ なので、

$a^2+b^2=5\,,\ c^2+d^2=17$ という整数を見つければよいという問題になります。

視察より、すぐに $a=2\,,\ b=1\,,\ c=4\,,\ d=1$ などが見つかるので、

$7+6i=(2+i)(4+i)$　となり、規約でないことがわかります。

注　$7+6i=(-1+2i)(1-4i)$ などとも表されるので、一意的に分解されていないと思うかもしれませんが、これは単元の因子がかかっているためです。

例 4.2

13 は$Z[i]$ 上既約であるか。

$13=(a+bi)(c+di)$ とおき、両辺のノルムを考えて

$13^2=(a^2+b^2)(c^2+d^2)$

$a^2+b^2=13\,,\ c^2+d^2=13$ とすると、$a=2\,,\ b=3\,,\ c=2\,,\ d=3$ が 1 つの解

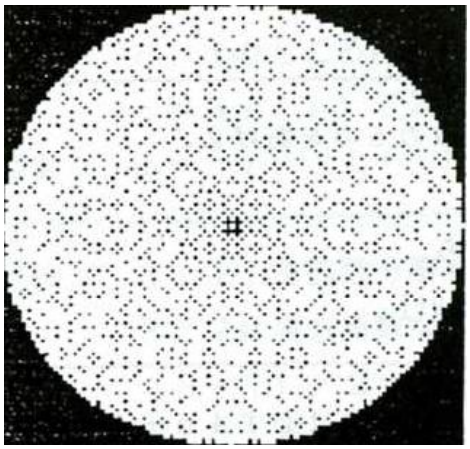
すなわち、$13=(2+3i)(2-3i)$ とできるので規約ではない。

2　複素格子平面への図示の考え方

既約なガウスの整数を図示するのに、1 で述べた判定法で一つ一つの元について調べるというのでは莫大な時間がかかります。そこで、既約元を見つけるということではなく、約数をふるっていくという方法が考えられます。これは、整数における素数を求めるときに良く行われる「エラトステネスのふるい」と同様の考え方ですね。

$Z[i]$ 上の 0 と単元を除くある元 d に対して、単元を除いた $Z[i]$ の任意の元 a との積 ad を除いていくということです。つまり、$Z[i]$ のあるイデアルを消去していくといってもいいですね。

下図は、コンピュータを使って、半径50内の領域で、$Z[i]$ の可約元をふるって、「複素数の素数」を残したものです。とても面白い図が得られます。



2　既約元を得るための諸定理

【定理】4.2.1

$m+ni$ が可約ならばその共役である $m-ni$ も可約である

証明

$m+ni=(a+bi)(c+di)$　とすると、$m+ni=(ac+bd)+(ad+bc)i$

このとき、

$(a-bi)(c-di)=(ac+bd)-(ad+bc)i=m-ni$ とできるので、

$m-ni$ は可約である。終

【定理】4.2.2

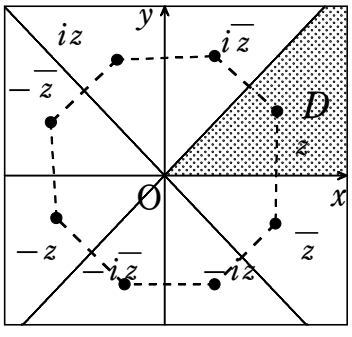
$m+ni$ が可約ならばその同伴元も可約である

証明

$m+ni$ が可約ならばその同伴元は、$m+ni$ に単元をかけたものであるから

明らかに可約である。終

上の２つの定理から、$m+ni$ が可約ならば、図の格子平面上で8個の点がそろって可約であるということがわかります。ようするに、図の領域 D のところだけ調べれば残りはそれを対称移動すればよいことがわかります。これで、図示するための労力はかなり減りますね。



定理4.2.1 と定理4.2.2 によって、

「ある元が可約⟹共役･同伴である8個すべての元が可約」がいえていますので、その対偶を考えれば、次の定理に言い換えることができます。

【定理】4.2.3

$m+ni$ が既約ならば、その共役、同伴である8個の元はすべて既約である。

次に、パソコンで図示する上で強力な定理をあげておきましょう。

【定理】4.2.4

$m+ni$ （$n\neq 0$, $m=n=1$を除く）が既約ならば m , n の一方が偶数、 もう一方が奇数である。

証明

（ｉ） m , n がともに偶数のとき

$m=2k$, $n=2k'$ $(k,k'\in Z$, $k\neq 0)$ とおくと、

$m+ni=2(k+k'i)$

$k+k'i\neq 1$ なので、$m+ni$ は可約である。

（ⅱ） m , n がともに奇数のとき

$m=2k+1$, $n=2k'+1$ $(k^2+k'^2\neq 0)$ とおくと

$m+ni=(2k+1)+(2k'+1)i$

$\therefore m^2+n^2=(2k+1)^2+(2k'+1)^2=4k^2+4k+1+4k'^2+4k'+1$

$=2(2k^2+2k'^2+2k+2k'+1)=(1^2+1^2)\{(k+k'+1)^2+(k-k')^2\}$

と変形できるので、$m+ni=(1+i)\{(k+k'+1)-(k-k')i\}$ と分解できる。

ここで、$(k+k'+1)-(k-k')i$ は単元でないので、$m+ni$ は可約である

（ｉ）（ⅱ）より、定理の対偶が証明されました。終

注 定理4.2.4 の逆は成り立たない。例えば、$-7+6i$ はm , n の一方が奇数、もう一方 が偶数であるが、$-7+6i=(1+2i)(1+4i)$ と分解できます。

ここで行った証明の（ⅱ）の考え方から、$m+ni$ において、 m , n がともに奇数であるとき、次のような方法で因数分解ができます。

$m+ni=(a+bi)(c+di)$ とできたとすると、上の定理の（ⅱ）から

$a=b=1$, $c=k+k'+1$, $d=-(k-k')$

$m=2k+1$, $n=2k'+1$ より $k=\dfrac{m-1}{2}$, $k'=\dfrac{n-1}{2}$

c , d のところに代入して $c=\dfrac{m+n}{2}$, $d=\dfrac{n-m}{2}$

よって、$m+ni=(1+i)\left(\dfrac{m+n}{2}+\dfrac{n-m}{2}i\right)$

例 4.1

$3+7i$ を因数分解せよ。

$\dfrac{3+7}{2}=5$, $\dfrac{7-3}{2}=2$ より、 $3+7i=(1+i)(5+2i)$

さて、だんだん終盤に近づいてきました。今度は、$m+ni$ において $n=0$ の場合、すなわち、整数の場合における既約性について調べておきましょう。

【定理】4.2.5

Z 上の $4n+3$ 型の素数は、$Z[i]$ 上でも素数（既約）である。

証明

Z 上の素数（奇素数）を p とおきます。p が $Z[i]$ 上で可約ならば、単元でない２つの元の積によって、

$p=(a+bi)(c+di)$ と表せます。

ここで、両辺のノルムを考えれば

$p^2=(a^2+b^2)(c^2+d^2)$　p は素数なので

$a^2+b^2=p$ ， $c^2+d^2=p$

この式が成り立つためには、$(a\,,b)\,,(c\,,d)$ の組の一方が奇数でもう一方が偶数でなければなりません。（それ以外ではpは偶数となります）

$a=2k\,,b=2k'+1$ とおくと、

$p=(2k)^2+(2k'+1)^2=4(k^2+k'^2+k')+1$　よって、p は$4n+1$ 型の素数。

奇素数は、$4n+1$ 型と $4n+3$ 型しかないので、今述べたことの対偶を考えれば定理は証明されます。終

例 4.2

Z 上100までの素数の中で、$Z[i]$ 上でも素数であるものをあげよ。

解答

$4n+3$ 型の素数を列挙すればよいから

$\{3\ ,\ 7\,,11\,,19\,,23\,,31\,,43\,,47\,,59\,,67\,,71\,,79\,,83\}$

この定理は非常に重要な定理です。$4n+3$ 型の素数であることを調べさえすれば、それが複素数の素数であることが言えるのです。

奇素数は $4n+3$ 型と $4n+1$ 型しかないのですが、それでは、$4n+1$ 型の素数は必ず可約であるといえるのでしょうか。つまり、定理4.2.5 の逆は成り立つのでしょうか。これが成り立てば、

$4n+1$ 型素数は可約　$4n+3$ 型素数は既約

とシンプルに表現できますね。

$4n+1$ 型素数を見ると、

$5=(2+i)(2-i)$ ， $13=(2+3i)(2-3i)$ ， $17=(1+4i)(1-4i)$ などと確かに因数分解できそうに見えます。

しかし、この証明は簡単ではありません。私は15年くらい前にこの証明を考えたときどうしてもできなくて、棚上げにしていました。ところが、2002年慶応大学の入試に次のような問題が出題されました。

設問(1)から(5)に答えなさい

４で割ると余りが１になるような素数 p , $p=4k+1$ を１つとる。これに対し等式

(Q)　$a^2+4bc=p$

を満たす自然数３つの組 (a,b,c) 全体を考える。両辺の絶対値を比べればわかるように、このような自然数３つの組の可能性は有限通りしかありえない。

いま等式(Q)を満たす自然数３つの組 (a,b,c) から新しく自然数３つの組を作る手続きを次の(ⅰ)(ⅱ)(ⅲ)により定める。

(ⅰ)　$a<b-c$ ならば $(a+2c,c,b-a-c)$　を作る

(ⅱ)　$b-c<a<2b$ ならば $(2b-a,b,a-b+c)$ を作る

(ⅲ)　$a>2b$ ならば $(a-2b,a-b+c,b)$ を作る

(1)　(a,b,c) が等式(Q)を満たす自然数の組でさらに(ⅰ)の条件 $a<b-c$ を満たすとする。このとき、上の(ⅰ)より得られる $(a+2c,c,b-a-c)$ もまた等式(Q)を満たすことを示しなさい。

(2)　等式(Q)を満たす自然数の組 (a,b,c) は $a=b-c$ や $a=2b$ を満たすことはないことを示しなさい。

(3)　等式(Q)を満たす自然数の組 (a,b,c) の中には、上の手続きを施しても変化しないという性質をもつものが存在する。$p=4k+1$ と表すとき、この性質を持つ (a,b,c) を k を用いて具体的に与え、かつそれがただ1組しか存在しないことを示しなさい。

(4)　等式(Q)を満たす自然数の組 (a,b,c) に対して上の手続きを2回繰り返すとどうなるか。結論を簡潔に説明しなさい。また、この観察をもとに等式(Q)を満たす自然数３つの組の全体の個数が偶数か奇数かを決定し、そう判断できる理由を述べなさい。ただし、等式(Q)を満たす自然数３つの組から上の手続きにより新しく作られた自然数３つの組は(ⅰ)(ⅱ)(ⅲ)のどの場合でも再び等式(Q)を満たすという事実についてはここでは証明なしに用いてよい。

(5)　素数 $p=4k+1$ をある２つの自然数 a , b により

$p=a^2+(2b)^2$

と表すことができることを示しなさい。　　(2002　慶応大（医）)

非常に長い問題ですが、この問題の結論は、まさに私が今までできなくて苦労していた証明。『$4n+1$ 型素数は $\mathbb{Z}[i]$ 上可約である』　そのものではありませんか！
つまり、この問題を解きさえすれば、先ほどの定理4.2.5 の逆を証明したことになるのです。

では、少し長いのですが、この問題を解いてみましょう。

解答の道筋は、等式(Q)を満たす自然数$(a\,,b\,,c\,)$の組全体の個数が奇数個であることを示し、また、(Q)は$b\,,c$に関して対称なので、$(a\,,b\,,c)$が解であるならば$(a\,,c\,,b)$も解なので、必ず$b=c$であるものが解に含まれるということです。

なかなかカッコイイ考え方ですね。

解答

(1)　$a'=a+2c\,,b'=c\,,c'=b-a-c$とする。

このとき、$a'^2+4b'c'=(a+2c)^2+4c(b-a-c)$

$$=a^2+4ac+4c^2+4bc-4ac-4c^2$$

$$=a^2+4bc=p$$

よって、$(a'\,,b'\,,c')$は等式(Q)を満たすことがわかりました。

注ついでに、(ⅱ)(ⅲ)についても示しておきましょう。

(ⅱ)　$a'=2b-a\,,b'=b\,,c'=a-b+c$とする。

$a'^2+4b'c'=(2b-a)^2+4b(a-b+c)=a^2-4ab+4b^2+4ab-4b^2+4bc=a^2+4bc=p$

(ⅲ)　(ⅱ)を$(a\,,b\,,c)$としたとき、(ⅲ)は$(-a\,,c\,,b)$なので、明らかに(Q)を満たす。

(2)　$a=b-c$のとき、(Q)の左辺は

$(b-c)^2+4bc=(b+c)^2$　これは素数ではない。

$a=2b$　のとき、(Q)の左辺は

$4b^2+4bc=4b(b+c)$　これは4の倍数であり素数でない。

以上より、$a=b-c$や$a=2b$のとき、等式(Q)を満たすことはない。

(3)　(ⅰ)のとき、

$$\begin{cases} a+2c=a \\ c=b \\ b-a-c=c \end{cases}$$ とおくと

$c=0$となり不適

(ⅱ)のとき

$$\begin{cases} 2b-a=a \\ b=b \\ a-b+c=c \end{cases}$$ とおくと

$a=b$

このとき、(Q)より

$a^2+4ac=4k+1$

$a(a+4c)=4k+1$

右辺が素数であるためには$a=1$でなければならない。

よって、$(a\,,b\,,c)=(1\,,1\,,k)$

(iii)のとき

$$\begin{cases} a-2b=a \\ a-b+c=b \\ b=c \end{cases}$$ とおくと

$b=0$ となり不適。

以上より、$(a,b,c)=(1,1,k)$　のただ1組である。　㊒

(4)　(ⅰ)のとき、$(a',b',c')=(a+2c,c,b-a-c)$

ここで、$a'-2b'=(a+2c)-2c=a>0$ より $a'>2b'$

よって、(ⅰ)の手続きの後は、手続き(iii)を行うことになる。

すると、$(a,b,c)\to(a+2c,c,b-a-c)\to(a+2c-2c,a+2c-c+b-a-c,c)=(a,b,c)$

となり、最初の状態に戻る。

(ⅱ)のとき、$(a',b',c')=(2b-a,b,a-b+c)$

ここで、$b'-c'=2b-a-c$　$,a'=2b-a$ ，$2b'=2b$

よって、$b'-c'<a'<2b'$

(ⅱ)の手続きの後は、再び手続き(ⅱ)を行うことになる。

すると、$(a,b,c)\to(2b-a,b,a-b+c)\to(2b-2b+a,b,2b-a-b+a-b+c)=(a,b,c)$

となり、最初の状態に戻る。

(iii)のとき、$(a',b',c')=(a-2b,a-b+c,b)$

ここで、$a'=a-2b$ ，$b'-c'=a-2b+c$

よって、$a'<b'-c'$

(iii)の手続きの後は、手続き(ⅰ)を行うことになる。

すると、$(a,b,c)\to(a-2b,a-b+c,b)\to(a-2b+2b,b,a-b+c-a+2b-b)=(a,b,c)$

となり、最初の状態に戻る。

(ⅰ)(ⅱ)(iii)から生み出される (a,b,c) はすべて異なり、その総数は偶数個である。

また、(3)より $(1,1,k)$ がただ1組あるので、自然数の組 (a,b,c) 全体の個数は偶数個である。

(5)　等式　$a^2+4bc=p$ は b,c に関して対称式なので、(a,b,c) が解のとき、(a,c,b) も解である。

(4)で解の総数が奇数個だったので、解の中には、$b=c$ のものが必ず存在する。

このとき等式(Q)は　$p=a^2+(2b)^2$　と表すことができる。㊓

上のことから、p が $4n+1$ 型の素数であるときは、必ず

$p=(a+2bi)(a-2bi)$

と因数分解できることがわかります。

以上によって、とてもありがたい定理が示されました。

【定理】4.2.6

（Z 上の）$4n+1$ 型の素数は可約である。

定理4.2.6と定理4.2.7によって、整数の場合の既約性は、それが $4n+1$ 型素数か、$4n+3$ 型素数かを調べるだけでよいことがわかりました。

最後に、皆さんに一つの問題を提示したいと思います。

【定理】4.2.7

z が整数及び純虚数でないとき、ノルムが素数であれば既約である。

証明

$z=m+ni$ $(mn\neq 0)$ が可約であるとき、

$m+ni=(a+bi)(c+di)$ （右辺の因数はどちらも単元でない）

と表せる。両辺のノルムをとって

$m^2+n^2=(a^2+b^2)(c^2+d^2)$

よって、m^2+n^2 は素数でない。

今述べたことの対偶により定理は証明された。終

これはある意味最強な考えで、複素数の素数の判定の基本になります。

問題はこの定理の逆が真かどうかです。もし、真であれば、

「複素数の素数⇔ノルムが素数」

と単純化されて、格子平面上から可約元を「ふるって」いく考え方を用いずに、ノルムが素数かどうかだけで判定することができますね。

さて、ノルムが素数でない、すなわち、ノルムが合成数であるとき、可約でしょうか。m , n がともに奇数、またはともに偶数のときは、ノルムは２の倍数になり、このときは確かに可約でしたので、m , n が奇数と偶数の場合を考えればよいことになります。

このとき、ノルムは$4n+1$ 型の数なので、これが合成数であるとは、

① $(4k+1)(4l+1)$ 型

② $(4k+3)(4k+3)$ 型

の２つの場合が考えられます。①の場合は可約になります。例をあげると、

$z=9+2i$ のとき、$N(z)=9^2+4^2=85=5\cdot 17$ なので

$z=9+2i=(2+i)(4-i)$ と因数分解できます。

では、②の場合は、どうでしょう。この場合は可約にはならないのですが、しかしそもそも、②の形になるような z はあるのでしょうか。

つまり

$m^2+n^2=(4k+3)(4l+3)$ となるような m ,n は存在しない

これが成り立てば、複素数の素数の図示はとても楽になるのです。

是非皆さん考えてみてくださいね！　　（しもまっち）