因数分解と素因数分解からみる数学

肇

2022 年 5 月 11 日

概要

因数分解と素因数分解は似ていますが、何処まで同じで何処に違いがあるのかを深く考えることで大学数学（特に韓論）に自然とつながる様をみていきます。大学数学を知らない人向けに、大学数学の面白さや有用さを伝えることに主眼を置いています。大雑把に書いているので正確性に欠くところがありますがご了承ください。

1 諸々の定義

予め必要になる数学概念の定義をまとめておく。

定義 1. 群、環、整域、単項イデアル整域、ユークリッド環、体

1. 可換群
   乗、除法ができる集合（例えば $\mathbb{R} \setminus 0$）
2. 環
   和、差、乗法ができる集合（例えば 2×2 行列）
3. 整域
   $ab = 0 \Rightarrow a = 0 \ or \ ab = 0$ となる環（例えば整数係数の多項式全体）
4. 単項イデアル整域
   全てのイデアルがひとつの元で生成できる環（例えば整数全体や実数係数の多項式全体）
5. ユークリッド環
   割り算の余りが定義出来るような環（例えば整数全体や実数係数の多項式全体）

注意
これらは体 $\Rightarrow$ ユークリッド環 $\Rightarrow$ 単項イデアル整域 $\Rightarrow$ 整域 $\Rightarrow$ 環 $\Rightarrow$ 群の関係を満たしている。

定義 2. イデアル

A を環とする。

1. イデアル
   A の部分集合 I が A のイデアルとは、$I \subset A$ かつ足し算で閉じていて A 倍ができることを言う。（例：$6\mathbb{Z} \subset \mathbb{Z}$）

2. 素イデアル

$\mathfrak{p} \subset A$ がイデアルで $^{\forall}a, b \in A : ab = 0 \Rightarrow a = 0\ or\ b = 0$ を満たすとき $\mathfrak{p}$ を素イデアルと言う。
（例：$3\mathbb{Z} \subset \mathbb{Z}$）

3. 極大イデアル
$\mathfrak{m} \subset A$ がイデアルで $\mathfrak{m} \subset I \subsetneq A$ となる I が存在しないとき $\mathfrak{m}$ を極大イデアルという。

定義 3. イデアルの生成

$a \in A$ に対し、$(a) := \{ab \mid b \in A\}$ と定めるとこれは A のイデアルになる。
また I, J が A のイデアルのとき、$I + J := \{a + B \mid a \in I,\ b \in J\}$ と定めるとこれも A のイデアルとなる。

2 因数分解と素因数分解の特徴

因数分解と素因数分解の特徴付けを行う。

2.1 素因数分解

因数分解とは整数を素数の積に分解することであった。では素数とは何だろうか。例えば素数 7 については $(\mathrm{mod}\ 7)$ の世界（これを改めて $\mathbb{Z}/7\mathbb{Z}$ と書く）は体になっていて、特に整域である。そこで以下のように定義する。

定義 4. 素元（素数）

$a \in A$ に対し、(a) は A のイデアルであり $A/(a)$ が整域となるとき、a を素元という。

命題 5.

素数の生成するイデアルは極大イデアルである。特に素イデアルである。すなわち素数は素元。
注意
整数の因数分解のときは整域よりも強く体になっている。

2.2 多項式の因数分解（準備）

素因数分解のときと同じ結果を得るがそのために準備が必要なのでそこから始める。

定義 6. 全射、単射、全単射

$f : A \longrightarrow B$ が B 全ての値をとるとき f を全射、$a \neq b \in A \Rightarrow f(a) \neq f(b)$ となるとき f を単射、全射かつ単射のとき全単射という。

定義 7. 準同型、同型

$f : A \longrightarrow B$ が $a, b \in A$ に対し $f(a + b) = f(a) + f(b)$ や $fab = f(a)f(b)$ などを満たすとき f を準同型という。準同型かつ全単射のとき同型という。

例 8. 同型の例

$$\begin{array}{rccc} f\colon & \mathbb{Z} & \longrightarrow & 2\mathbb{Z} \\ & x & \longmapsto & 2x \end{array}$$

この写像は準同型かつ全単射なので、同型写像である。

定義 9. 核（*kernel*）

準同型 $f : A \longrightarrow B$ に対して、$\ker f := \{a \in A \mid f(a) = 0\}$ と定める。これは A のイデアルである。

補題 10. 自然な全射準同型

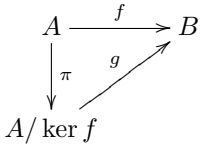
$f : A \longrightarrow B$ に対し、

$$\begin{array}{rccc} \pi\colon & A & \longrightarrow & A/\ker f \\ & a & \longmapsto & \overline{a} \end{array}$$

が定まる。これは全射準同型写像である。

定理 11. 準同型定理

準同型 $f : A \longrightarrow B$ と自然な全射準同型 $\pi\colon A \longrightarrow A/\ker f$ に対し、$f = \pi \circ g$ を満たす単射準同型 $g\colon A/\ker f \longrightarrow B$ が存在する。



特に f が全射なら g は同型である。

命題 12. 素イデアルの特徴付け

$\mathfrak{p} \subset A$ が素イデアル $\Longleftrightarrow$ $A/\mathfrak{p}$ が整域

命題 13. 極大イデアルの特徴付け

$\mathfrak{m} \subset A$ が極大イデアル $\Longleftrightarrow$ $A/\mathfrak{m}$ が体

命題 14.

極大イデアルは素イデアル

証明. $\mathfrak{m} \subset A$ を極大イデアルとすると、$A/\mathfrak{m}$ は体、特に整域。よって $\mathfrak{m}$ は素イデアル。

2.3 実数係数の多項式の因数分解

因数分解したときの素数に相当しそうなのも（例えば $x - 6$）は素元であることを示す。

命題 15.

$a \in \mathbb{R}$ として、$(x - a) \subset \mathbb{R}[x]$ は極大イデアルである。特に $x - a$ は素元である。

証明.

$$\begin{array}{rccc} f\colon & \mathbb{R}[x] & \longrightarrow & \mathbb{R} \\ & f(x) & \longmapsto & f(a) \end{array}$$

は全射準同型である。また $\ker f = (x-a)$ なので準同型定理（定理 11）より、$\mathbb{R}[x]/(x-a) \cong \mathbb{R}$。$\mathbb{R}$ は体なので $\mathbb{R}[x]/(x-a)$ も体。よって $(x-a)$ は極大イデアル。

以上より因数分解した構成要素はすべて極大イデアルを生成するとわかる。すなわち整数の素因数分解と全く同じ構造をしているとわかる。

2.4 整数係数の多項式の因数分解

こんどは素数に相当しそうなもの（例えば $x-6$）は先程までと同様に素元であるが、$x-6$ の生成するイデアルは極大イデアルとまでは言えないことを示す。

命題 16.

$a \in \mathbb{Z}$ として、$(x-a) \subset \mathbb{Z}[x]$ は素イデアルであるが極大イデアルでは無い。特に $x-a$ は素元である。

証明.

$$\begin{array}{rccc} f\colon & \mathbb{Z}[x] & \longrightarrow & \mathbb{Z} \\ & f(x) & \longmapsto & f(a) \end{array}$$

は全射準同型である。また $\ker f = (x-a)$ なので準同型定理より、$\mathbb{Z}[x]/(x-a) \cong \mathbb{Z}$。$\mathbb{Z}$ は整域なので $\mathbb{Z}[x]/(x-a)$ も整域。よって $(x-a)$ は素イデアル。

このように係数を整数に制限したときは素因数分解とは少し異なる構造を持つことがわかる。素数で $\mod$ をとったときは必ず逆元を持ったが（体だから）、整数係数の多項式環を $(x-a)$ で $\mod$ をとったときは逆元を持つとは限らない（整域でしかないから）。

3 RSA 暗号への応用

3.1 RSA 暗号の仕組み

2 つの素数を $p=5,\ q=7$ とし $r=pq$、$L=(p-1)(q-1)$ とおく。$e=5$（ただし $\gcd(e,(p-1)(q-1))=1$ となるように e をとる）とする。e と r は公開する。
ユークリッドの互助法を用いると $^{\exists}d,k \in \mathbb{Z}$ s.t. $ed-kL=1$ がとれ、d は復号するための秘密鍵となる。
具体的にみてみる。 $\mod r=35$ とする。2 を暗号にするときは、$2^e \equiv 2^5 \equiv 32$ とする。
復号するときは、$p=5$、$q=7$ より $L=24$。ユークリッドの互助法を使って $d=5$、$k=1$ が作れる。
$32^d \equiv (-3)^5 \equiv 2$ となり確かに上手くいっている。

3.2 必要な定理たち

上では以下の 3 つの定理を使った。

定理 17. ユークリッドの互助法

$a, b \in \mathbb{Z}$ が $\gcd(a, b) = 1$ なら、$^{\exists}s, t \in \mathbb{Z}$ s.t. $sa + tb = 1$

証明. $\mathbb{Z}$ はユークリッド環より単項イデアル整域。$(a) + (b)$ は $\mathbb{Z}$ のイデアルなので、$^{\exists}c \in \mathbb{Z}$: $(a) + (b) = (c)$。$a \in (c)$、$b \in (c)$ より、c は a, b を共に割り切り $\gcd(a, b) = 1$ より $c = 1$。

定理 18.

p は素数とする。$a \in \mathbb{Z}/p\mathbb{Z}$ なら、$a^{p-1} = 1$。

定理 19.

$\mathbb{Z}/pq\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$

証明. 定理 11 を使う。

$$\begin{array}{rccc} f\colon & \mathbb{Z} & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \\ & a & \longmapsto & (\overline{a},\ \overline{a}) \end{array}$$

は全射準同型である。また $\ker f = pq\mathbb{Z}$ なので準同型定理より従う。

4 終わりに

因数分解と素因数分解から環論を自然に考えてみた。それらの同一点や違いが明確になっただけでなく、RSA 暗号の仕組みに必要な定理の証明までもできてしまう。このように代数はとても面白いので興味があれば、雪江-[1] を読んでみて欲しい。

参考文献

[1] 雪江明彦「群論入門」(日本評論社)
[2] 雪江明彦「環と体とガロア理論」(日本評論社)
[3] 雪江明彦「初等整数論からｐ進数へ」(日本評論社)