代数学 II 要約 NO.1

今日のテーマ:

環と体の定義の復習。記号の約束 環 $\mathbb{Z}$、 $\mathbb{Z}/n\mathbb{Z}$

本題に入る前に、この講義の大まかなあらすじについて書いておく。

この講義の主題は有限体 (要素の数が有限個であるような体) である。

まず、環と体の定義の復習から始めて、有限体の定義、その例と諸性質を調べる。環と体の定義については諸君は 2 回生の代数学で学んだはずではあるが、実例を触ることにより始めて定義の意味などが分かることも多いことと思う。

ついで多項式系の解の個数と、それを支配している母関数 (ヴェイユゼータ関数) について述べる。ヴェイユゼータ関数については極めて深い理論があって、ここではそれを紹介することはできないのだが、その入口ぐらいまでは案内できるかも知れない。

ではまず体の定義から始めよう。公理的にきちんと述べると理解してくれない方が多いので、まず次の大筋を理解して頂きたい。

定義 1.1.

(1) 環とは、そのなかで和、差、積が自由に行えるような集合である。
(2) 体とは、そのなかで和、差、積および 0 以外の元による割り算が自由に行えるような集合である。

この講義で使う環は、単位元 1 を持ち、乗法が可換なもの (可換環) である。体も、乗法が可換なもの (可換体) のみを扱う。以後、特に断らない限り、環や体と言えばそのようなものを指すものと理解されたい。

環の正確な定義は次のようになる.

定義 1.2 (環の正確な定義). 集合 R が環であるとは、足し算と呼ばれる写像

$$+ : R \times R \to R$$

と掛け算と呼ばれる写像

$$\times : R \times R \to R$$

が定義されていて次の性質を満たす時に言う。

(1) R は足し算に関して可換群をなす。
(2) R の積は結合法則を満たす。
(3) R の足し算と掛け算は分配法則を満たす。
(4) R は積に関して単位元を持つ。

忘れた人は 2 回生の代数学の講義に戻るか、本講義の参考書

「群・環・体入門」新妻弘・木村哲三著 (共立出版)

などを参考にするとよい。なお、上記の本はよい本ではあるが、本講義と記号が一つだけ異なる点がある。本講義で $\mathbb{Z}/n\mathbb{Z}$ と呼ぶ環のことを上記の本ではしばしば $\mathbb{Z}_n$ と書いている。本講義では記号 $\mathbb{Z}_n$ は使わない(本講義では使わないが $\mathbb{Z}_n$ には上記とは全く別の意味がある。) ので注意されたい。

環の例としては、まず整数全体のなす環 $\mathbb{Z}$ がある。もう一つの例は $\mathbb{Z}/n\mathbb{Z}$ である。これは、$\mathbb{Z}$ をそのイデアル $n\mathbb{Z}$ で割った剰余環である。これを復習しよう。整数 x, y に対して,

$$x \text{ と } y \text{ とは同じクラス} \quad \Leftrightarrow \quad x - y \in n\mathbb{Z}$$

ときめることに $\mathbb{Z}$ に「n を法としたクラス分けをほどこし、$[x]_n$ は「x の n を法としたクラス」と決めたとき、集合として、

$$\mathbb{Z}/n\mathbb{Z} = \{[x]_n; x \in \mathbb{Z}\}$$

と定義する。$\mathbb{Z}/n\mathbb{Z}$ には加法、乗法が、

$$[a]_n + [b]_n = [a+b]_n, \quad [a]_n + [b]_n = [a+b]_n$$

でうまく定義され、この演算によって $\mathbb{Z}/n\mathbb{Z}$ は環になるのである。なお、「うまく定義され」という言葉は伊達ではない。よいクラス分けで分けないとうまく加法、乗法が定義されるとは限らないのである。問題を参照のこと

問題 1.1. $\mathbb{Z}$ にクラス分けを

$$x \text{ と } y \text{ とは同じクラス} \quad \Leftrightarrow \quad |x| = |y|$$

で決めたとする。x のこのクラス分けによるクラスを $[x]$ と書き、$\mathbb{Z}$ をこのクラス分けで分けたクラスの全体を A と書くことにする。このとき、

(1) $[x][y]=[xy]$ によって A には乗法がうまく定義されることを示せ。
(2) $[x]+[y] = [x+y]$ によっては A には加法がうまく定義されないことを示せ。

各回の問題はレポートで提出すること。提出は特に指定しない限り次回の講義の終了時間に行うものとする。(介護等実習など、やむを得ない場合にはその旨告げれば受け取ります。)