環論入門セミナー

yui_poya0527

March 6, 2022

自己紹介

- 名前 $\cdots$ ゆい (Twitter: https://twitter.com/yui_poya0527)
- 所属 $\cdots$ 東京学芸大学 教育学部 算数科
- 専門 $\cdots$ 代数幾何学 (興味があるのはモチーフ理論)
- 最近のトピック
  - 数物系サーバーを作った！
  - 数物セミナーがんばった！
  - 親知らずを抜きました、つらいです。
  - 大学卒業できそう！ でも教員免許 1 つ落とした。

さっそく環論に入っていきたいところですが $\cdots$
まずは集合について考えよう！

数学的構造

土台となる集合に対して考えることでも面白い理論が発展していくが,
集合に数学的構造を入れることでより豊かな理論を得ることができる.
まずは数学的構造のうち大きな 3 つをとらえよう.

代数的構造

集合とその演算 (写像) により定まる構造.

順序的構造

集合とその元の順序関係により定まる構造.

位相的構造

集合とその部分集合の族 (開集合系, 閉集合系, 距離) で定まる構造.

今回は代数的構造, すなわち集合の上の演算とその性質に注目する.
特に身近な例である整数の演算に注目しよう！

整数の代数的構造

整数の演算

整数の四則演算は加法, 減法, 乗法, 除法. このうち加法と減法, 乗法と除法が対応する.
(加法の性質) すべての 2 整数に対して, その和が一意に定まる.
1.$a+b=b+a$
2.$a+(b+c)=(a+b)+c$
3.$a+0=0+a=a$
4.$a+(-a)=(-a)+a=0$
(乗法の性質) すべての 2 整数に対して, その積が一意に定まる.
1.$a\cdot b=b\cdot a$
2.$a\cdot(b\cdot c)=(a\cdot b)\cdot c$
3.$a\cdot 1=1\cdot a=a$
4.$a(b+c)=ab+bc$

群の定義

定義 1 (群の定義)

集合 A に対して, 演算 $+ : A \times A \to A, +(a, b) \mapsto a + b$ が定まって,
1.$a + (b + c) = (a + b) + c$
2.$a + 0 = 0 + a = a$
3.$a + (-a) = (-a) + a = 0$
特に演算に対して可換な群, $a + b = b + a$, をアーベル群という.

例 1

整数全体 $\mathbb{Z}$ は和に対してアーベル群になる.(単位元が 0, n に対して逆元が $-n$)
積に対しては群にならない. 積に対する単位元は 1 だが, 例えば 2 の逆元は?

環の定義

定義 2 (環の定義)

集合 A に対して, 2 つの演算

$$
\begin{aligned}
+ &: A \times A \to A, +(a,b) \mapsto a+b \\
\times &: A \times A \to A, \times(a,b) \mapsto ab
\end{aligned}
$$

が定まって,
1.A は和に対してアーベル群
2.$a,b,c \in A$ に対して, $a(bc) = (ab)c$
3.$a,b,c \in A$ に対して, $a(b+c) = ab+ac, (a+b)c = ac+bc$
4.$1a = a1 = a$

※今回は乗法について可換性の成立する環 (可換環) のみ考える.

単数群と体

定義 3 (単数群)

可換環 A に対して, A の単数群 $A^\times$ を A の元で積の逆元を持つもの全体とする.

例 2

整数で積の逆元を持つものは 1 と -1 のみ. よって $\mathbb{Z}^\times = \{1, -1\}$

定義 4 (体)

可換環 A が体 $\overset{\text{def}}{\iff} A - \{0\} = A^\times$

例 3

$\mathbb{Z}$ は体ではない. 逆に $\mathbb{Q}$ は体.

整域

0 の乗法

整数において, 0 に何をかけても 0. 0 を含まない掛け算で 0 を作ることはできない.

定義 5

可換環 A が整域 (integral domain) $\overset{\text{def}}{\Longleftrightarrow}$ 任意の $a, b \in A - \{0\}$ に対して, $ab \neq 0$

命題 6

体は整域である.

Proof.

体 A において $A - \{0\}$ の各元は逆元を持つ.
$a, b \in A - \{0\}$ に対して $ab = 0$ とすると, $a^{-1}abb^{-1} = 1 \neq 0$ より矛盾. $\square$

イデアル

n の倍数

整数において n の倍数全体とは, 自然数 n に整数全体をかけたもの.
n の倍数全体は和と積に対して閉じている.

定義 7 (イデアル)

環 A とその空でない部分集合 I に対して, I が A のイデアル
$\overset{\text{def}}{\Longleftrightarrow}$ I は和について閉じていて, 任意の $a \in A, x \in I$ に対して $ax \in I$.

整数環のイデアル

例 4

整数環におけるイデアルは $(n) := \{\cdots, -2n, -n, 0, n, 2n, \cdots\}$ の形に限る.
これを n が生成するイデアルと呼ぶ. 例えば 2 の倍数と 3 の倍数全体 $(2) \cup (3)$ のようなものはイデアルにはならない.
$2, 3 \in (2) \cup (3)$ だが, $2 + 3 = 5 \notin (2) \cup (3)$ となり和について閉じない.

問題 1

整数環 $\mathbb{Z}$ において,
1) イデアルの共通部分 $(2) \cap (3)$ はどのように表せるだろうか.
2) イデアル (3) に含まれるようなイデアルを 3 つあげよう.

整数環のイデアル 2

問題の解答

1) $(2) \cap (3) = (6)$.2 つのイデアルの共通部分はその最小公倍数が生成するイデアル.
2) (3) に含まれるイデアルは, 3 の倍数が生成するイデアル.

問題から考えよう

整数環 $\mathbb{Z}$ にはイデアルの包含関係
$(2) \supset (4) \supset (8) \supset (16) \supset \cdots \supset (68719476736) \supset \cdots$
$(3) \supset (6) \supset (18) \supset (72) \supset (360) \supset \cdots$
こういった包含の列 (降差列) の極大元にはどういった法則があるだろうか？

素数の性質を考えよう

定義 8 (素数)

整数 $p(p \geq 2)$ が素数 (prime number)$\overset{\text{def}}{\Longleftrightarrow}$ p の正の約数全体は $\{1, p\}$
素数全体を $\mathbb{P}$ で表す.

素数の性質

素数は自分自身を含まない自然数の積の形に分解できない.
これを 2 つの形に言い換える.
1) 整数 m, n に対して, mn が p の倍数ならば m か n の少なくとも一方は p の倍数.
2) 素数の生成するイデアル (p) を含むようなイデアルは $\mathbb{Z}$ 以外存在しない.
整数環においては同じことを主張しているようにみえるが、一般の環でも同様の性質を持ったイデアルを考えたいのであえて 2 つの表記をした. それぞれイデアルとして定義していこう.

素イデアル・極大イデアル

定義 9 (素イデアル)

可換環 A に対して, A のイデアル $\mathfrak{p}(\mathfrak{p} \neq A)$ が素イデアル (prime ideal)
$\overset{\text{def}}{\iff}$ $a, b \notin \mathfrak{p}$ ならば $ab \notin \mathfrak{p}$.
※素数の性質 1

定義 10 (極大イデアル)

可換環 A に対して, A のイデアル $\mathfrak{m}(\mathfrak{m} \neq A)$ が極大イデアル (maximal ideal)
$\overset{\text{def}}{\iff}$ $\mathfrak{m} \subsetneq I \subsetneq A$ を満たすような A のイデアル I が存在しない.
※素数の性質 2

命題 11

可換環において, 極大イデアルは素イデアル.

整数環の素イデアルと極大イデアル

素数の生成するイデアル

$p \in \mathbb{P}$ に対して, (p) は極大イデアル.(つまり素イデアルでもある.)

合成数の生成するイデアル

合成数 $n = pq(p, q \in \mathbb{P})$ の生成するイデアル (n) は,
$(p) \supset (n)$ より極大イデアルではない.
$p, q \notin (n)$ だが, $pq = n \in (n)$ より素イデアルでもない.

0,1 が生成するイデアル

素数でも合成数でもない自然数は $0, 1$ のみ.
1 の生成するイデアルは, 1 の倍数全体なので $(1) = \mathbb{Z}$. これは素イデアルではない.
0 の生成するイデアルは, 0 の倍数の集まり.
よって $(0) = \{0\}$. これは素イデアルだが極大イデアルではない.

法として考える

mod n

整数において，ある自然数で割った余りを考えるという手法は有用だった．
"n を法として考える" というのは，n で割った余りだけを考えること．
言い換えればこのとき，私たちは n の倍数を 0 とみなして考えている．

問題 2 (mod の考え方を使ってみよう)

7 を法として考えよう．
1)67 を 7 を法として考えるといくつになるか．
2)6^{24} を 7 で割った余りはいくつになるか．
3)$6^{57}-6^{38}+6^{91}-6^{72}$ を 7 で割った余りはいくつになるか．

この法として考えることを，一般の環でも考えよう．

剰余環

定義 12 (剰余環)

可換環 A とそのイデアル I に対して, 剰余環 A/I を
$x, y \in A$ を, $x - y \in I$ のとき x と y を同じ元としてみなしてできる環とする.

例 5 ($\mathbb{Z}$ の場合)

$\mathbb{Z}$ をイデアル (7) で割った剰余環 $\mathbb{Z}/(7)$ を考えよう.
7 の倍数に対して $7k - 0 \in (7)$ より, $\mathbb{Z}/(7)$ において 7 の倍数は 0 と見なされる.
7 で割った余りが同じ二数の差は 7 の倍数.
よってそれらは, $\mathbb{Z}/(7)$ においては同じ数と見なされる.
すなわち $\mathbb{Z}/(7)$ は $\{0, 1, 2, 3, 4, 5, 6\}$ に 7 を 0 と見なすように和と積を入れたもの.

確認 1

$\mathbb{Z}/(n)$ を一般的には $\mathbb{Z}/n\mathbb{Z}$ と表すことの方が多い.

剰余環の性質

命題 13

可換環 A とその素イデアル $\mathfrak{p}$, 極大イデアル $\mathfrak{m}$ に対して,
1)$A/\mathfrak{p}$ は整域
2)$A/\mathfrak{m}$ は体

さっき省略した命題を示そう.

系 14

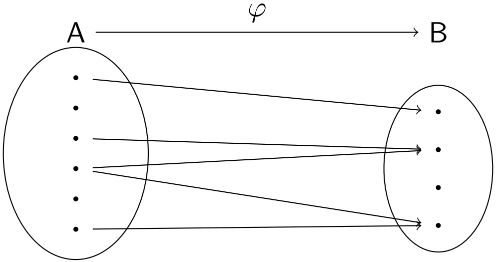
極大イデアルは素イデアル

Proof.

可換環 A の極大イデアル $\mathfrak{m}$ に対して, $A/\mathfrak{m}$ は体なので整域.
よって $\mathfrak{m}$ は A の素イデアル. □

確認 2 (写像)

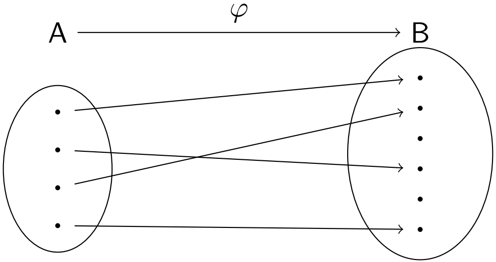
集合 A, B に対して, 写像 $\varphi : A \to B$ とはすべての A の元に対して B の元を返す対応のこと.
注意すべきは A の元 1 つに対して, B の元は 1 つしか対応づかない.



写像あれこれ 2

確認 3 (単射)

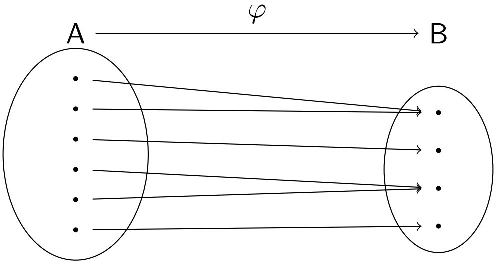
$\varphi(a) = \varphi(b) \Rightarrow a = b$



写像あれこれ 3

確認 4 (全射)

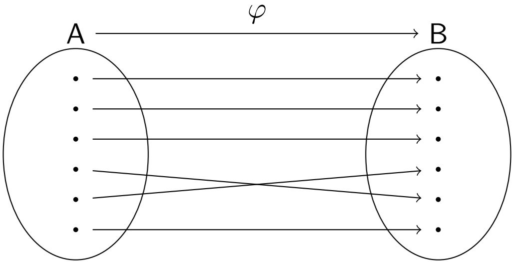
任意の $b \in B$ に対して, $a \in A$ が存在して $\varphi(a) = b$



写像あれこれ 4

確認 5 (全単射)

φ は単射かつ全射.(すなわち一対一に対応するような写像)



準同型写像

定義 15 (準同型写像)

環 A, B と写像 $\varphi : A \to B$ に対して, φ が準同型
$\overset{\text{def}}{\Longleftrightarrow}$ φ は任意の $a, a' \in A$ に対して,

$$\varphi(a + a') = \varphi(a) + \varphi(a')$$
$$\varphi(aa') = \varphi(a)\varphi(a')$$

を満たし, かつ $\varphi(1_A) = 1_B$ を満たす.

定義 16 (同型)

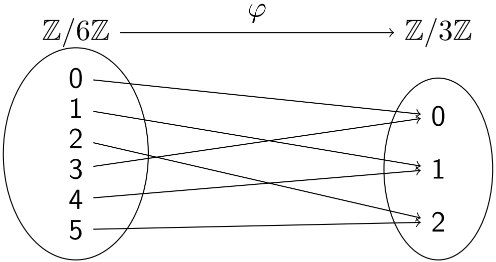
準同型 $\varphi : A \to B$ が同型 $\overset{\text{def}}{\Longleftrightarrow}$ φ が全単射

核と像 1

定義 17

準同型 $\varphi : A \to B$ に対して,
核 (kernel) を $\ker \varphi := \{a \in A \mid \varphi(a) = 0_B\}$
像 (image) を $\operatorname{im} \varphi := \{\varphi(a) \in B \mid a \in A\}$

次の準同型で核と像はそれぞれどうなっているだろう？



核と像 2

命題 18

環の準同型 $\varphi : A \to B$ に対して, $\ker\varphi$ は A のイデアル.

Proof.

任意の $a \in A$ と $x, y \in \ker\varphi$ に対して,
$\varphi(x+y) = \varphi(x) + \varphi(y) = 0_B$ より, $x + y \in \ker\varphi$.
$\varphi(ax) = \varphi(a)\varphi(x) = \varphi(a) \cdot 0_B = 0_B$ より, $ax \in \ker\varphi$. □

問題 3

以下の 2 つの準同型に対して, それぞれ核と像を考えよう.
1) 準同型 $\varphi : \mathbb{Z} \to \mathbb{Z}, n \mapsto 8n$
2) 準同型 $\pi : \mathbb{Z} \to \mathbb{Z}/13\mathbb{Z}, n \mapsto n \bmod 13$

準同型定理

定理 19

環の準同型 $\varphi : A \to B$ に対して, $A/\ker\varphi \simeq \operatorname{im}\varphi$.
すなわち, φ に対して $\varphi = \phi \circ \pi$ を満たすような同型射 $\phi : A/\ker\varphi \to \operatorname{im}\varphi$ が一意に存在する．ここで π は自然に定まる写像 $A \to A/\ker\varphi$, $a \mapsto a \bmod \ker\varphi$ を表している．

$$
\begin{tikzcd}
A \arrow[r, "\varphi"] \arrow[d, "\pi"'] & \operatorname{im}\varphi \subset B \\
A/\ker\varphi \arrow[ur, dashed, "\exists!\phi"'] &
\end{tikzcd}
$$

証明は省略して $\cdots$. $\mathbb{Z}$ における具体例を見てみよう！

中国式剰余定理

確認 6 (直積)

集合 A, B に対して，その直積 $A \times B$ は 2 つの集合の元の対 $\{(a, b) \mid a \in A, b \in B\}$.

定理 20 (中国式剰余定理)

互いに素な整数 m, n に対して，$\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Proof.

$\varphi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ を $a \mapsto (a \bmod m,\ a \bmod n)$ とする．
$\varphi_m : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, a \mapsto a \bmod m$ において，$\ker \varphi_m = (m)$.
$\varphi_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, a \mapsto a \bmod n$ において，$\ker \varphi_n = (n)$.
$\ker \varphi = \ker \varphi_m \cap \ker \varphi_n = (m) \cap (n)$. m と n が互いに素より m と n の最小公倍数は mn なので，$\ker \varphi = (mn)$.
今 φ は定め方より全射なので，$\operatorname{im} \varphi = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.
よって準同型定理 $\mathbb{Z}/\ker \varphi \simeq \operatorname{im} \varphi$ より，$\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. $\square$

中国式剰余定理-使おう編-

確認 7 (中国式剰余定理)

互いに素な整数 m, n に対して, $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

問題 4

1)$\mathbb{Z}/12\mathbb{Z}$ を直積の形に直そう.
2)195 を 12 で割った余りを求めなさい.

環論の展望

環論の入り口と言える環や準同型，イデアルの定義について確認してきた．
環論にはまだまだ重要事項があるので，それらの概要だけさらっていこう．

- 環の局所化
- 環のクラス
- ネーター環
- 環上の加群

局所化

定義 21 (積閉集合)

可換環 A とその部分集合 S に対して, S が A の積閉集合
$\overset{\text{def}}{\Longleftrightarrow}$ $1 \in S, 0 \notin S$ で, $a, b \in S$ に対して $ab \in S$.

定義 22 (環の局所化)

可換環 A と積閉集合 $S \subset A$ に対して, A の S による局所化 (localization) $S^{-1}A$ を, $\{\frac{a}{s} \mid a \in A, s \in S\}$ に対して, ある $s \in S$ を用いて $s(a_1 s_2 - a_2 s_1) = 0$ となるような $\frac{a_1}{s_1}$ と $\frac{a_2}{s_2}$ を同じと考えたものとする．このとき $S^{-1}A$ の演算は,

$$\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{a_1 s_2 + a_2 s_1}{s_1 s_2}, \frac{a_1}{s_1} \times \frac{a_2}{s_2} = \frac{a_1 a_2}{s_1 s_2}$$

すなわち局所化とは, 元の環に対して
積閉集合の元を分母に持つ"分数"と約分による同値性を考えている.

整数環の局所化 1

命題 23

可換環 A とその素イデアル $\mathfrak{p}$ に対して, $A-\mathfrak{p}$ は A の積閉集合.

Proof.

素イデアルの定義より $0\in\mathfrak{p}, 1\notin\mathfrak{p}$ なので, $0\notin A-\mathfrak{p}, 1\in\mathfrak{p}$.
また, $a,b\notin\mathfrak{p}$ ならば $ab\notin\mathfrak{p}$ より, $a,b\in A-\mathfrak{p}$ ならば $ab\in A-\mathfrak{p}$.
よって $A-\mathfrak{p}$ は積閉集合. $\square$

このとき, $A-\mathfrak{p}$ による A の局所化を $A_{\mathfrak{p}}$ と表す.
$A_{\mathfrak{p}}$ は極大イデアルを"分子が $\mathfrak{p}$ に含まれるような元全体"の 1 つしか持たない.
極大イデアルを 1 つしか持たない環を局所環という.

整数環の局所化 2

$\mathbb{Z}$ の素イデアルは, (0) と (p) の 2 種類だった.$(p \in \mathbb{P})$

例 6 ((0) による局所化)

$\mathbb{Z}$ において, $(0) = 0$ だった. よって, $\mathbb{Z} - \{0\}$ は $\mathbb{Z}$ の積閉集合.
ここで $\mathbb{Z}_{(0)}$ は有理数体 $\mathbb{Q}$ になる.

例 7 ((p) による局所化)

素数 $p \in \mathbb{P}$ を用いて $\mathbb{Z} - (p)$ は $\mathbb{Z}$ の積閉集合.
$\mathbb{Z}_{(p)}$ は分母に p の倍数が来ないような有理数全体になる.

より一般的に,

命題 24 (整域の局所化)

整域 A に対して, $A - \{0\}$ は A の積閉集合で $A - \{0\}$ による A の局所化は体になる.

環のクラス

ここまでに整域や体といった"特別な性質を持った環"を定義した.
こういった環のクラスのうち, 整数の性質から見出されるものを3つ紹介する.

いくつかの環

A を整域とする.

- 一意分解環 (UFD)
  A の 0 でない元は逆元を持つか, 一意に素因数分解 (素元分解) される.
- 単項イデアル整域 (PID)
  A の任意のイデアルは $a \in A$ を用いて (a) の形で表される.
- ユークリッド環
  A において余りのあるわり算を考えることができる.

環のクラス

可換環 $\supset$ 整域 $\supset$UFD$\supset$PID$\supset$ ユークリッド整域 $\supset$ 体

ネーター環

$\mathbb{Z}$ において任意の整数は有限個の素数を用いて素因数分解される.

$\mathbb{Z}$ におけるイデアルの昇鎖

任意の $n \in \mathbb{Z}$ に対して, (n) から始まるイデアルの包含に関する昇鎖の長さは有限.
具体的には n の素因子 $p \in \mathbb{P}$ を用いて, $(n) \subset \cdots \subset (ap) \subset \cdots \subset (p)$

こういったある種の"有限性"を持った環を定義しよう.

定義 25 (ネーター環)

可換環 A がネーター環 $\overset{\text{def}}{\Longleftrightarrow}$ A のイデアルの包含列において極大元が存在する.
$I_1, I_2, \cdots : A$ のイデアルに対して, $I_1 \subset I_2 \subset \cdots$ とすると,
$n \in \mathbb{N}$ が存在して, $I_1 \subset I_2 \subset \cdots \subset I_n = I_{n+1} = \cdots .$($I_n$ が極大元)

※包含の降鎖に対して極小元が存在するような可換環を, アルティン環という.

ネーター環の性質 1

ネーター環における有限性を紹介しよう.

命題 26

可換環 A がネーター環 $\Longleftrightarrow$ A の任意のイデアルは有限生成

すなわち,

系 27

PID はネーター環

一般に UFD はネーター環とは限らない. 逆も同様である.

ネーター環の性質 2

定義 28 (準素イデアル)

可換環 A のイデアル $\mathfrak{q}$ が準素イデアル
$\overset{\text{def}}{\Longleftrightarrow}$ $xy \in \mathfrak{q}$ ならば, $x \in \mathfrak{q}$ または $n \in \mathbb{N}$ が存在して $y^n \in \mathfrak{q}$

ここで素イデアルは準素イデアルである.
$\mathbb{Z}$ において準素イデアルは (0) か $p \in \mathbb{P}, n \in \mathbb{N}$ を用いて (p^n) と表されるイデアルのみ.
$\Longrightarrow$ 準素イデアルは素数のべき乗の一般化.

命題 29

準素分解ネーター環 A とその任意のイデアル I に対して, 有限個の準素イデアル
$\mathfrak{q}_1, \mathfrak{q}_2, \cdots, \mathfrak{q}_n$ が存在して,

$$I = \bigcap_{i=1}^{n} \mathfrak{q}_i$$

と表される.

環上の加群

定義 30 (環上の加群)

可換環 A とアーベル群 M に対して, M が A 上の加群
$\overset{\text{def}}{\Longleftrightarrow}$ 演算 $A \times M \to M, (a, x) \mapsto ax$ が定まって, $a, b \in A, x, y \in M$ に対して

$$\begin{aligned} a(bx) &= (ab)x \\ (a+b)x &= ax + bx \\ a(x+y) &= ax + ay \\ 1_A x &= x \end{aligned}$$

特に体上の加群のことをベクトル空間という.
環上の加群は体上のベクトル空間の環上への一般化であり, イデアルの一般化でもある.

最後に

他にも面白い話はたくさんありますが、今回はここまでです。
整数 $\mathbb{Z}$ から始まる環論の面白さ, 代数構造の奥深さを感じてもらえたら嬉しいです！
今日はご清聴ありがとうございました。

参考文献

1. 雪江明彦, 代数学 2 環とガロア理論, 日本評論社,2010
2. 雪江明彦, 整数論 1 初等整数論から p 進数へ, 日本評論社,2013
3.Athiyah-MacDonald, 可換代数入門, 共立出版,2006
以下の本はこの先の内容を学ぶのに役に立ちます.
代数幾何学 (スキーム論)
4.Qing Liu,Algebraic Geometry and Arithmetic Curves,Oxford,2006
5.R. ハーツホーン, 代数幾何学, 丸善出版,2013
代数的整数論
6.J. ノイキルヒ, 代数的整数論, 丸善出版,2012
7. 加藤和也・黒川信重・斎藤毅, 数論 1 Fermat の夢と類体論, 岩波書店,2005