Schedule(残りの予定)

11/24(Thu): Today

09:00-10:40 Ring, Field

12:30 (pls submit till 10:40…) deadline of Report (3) (レポート(3)締切出題);

13:30-15:10 Ans & Cmts by Duc, and Field, (Number Theory?)

- Last class (最後の講義); I'll make questionnaire in the last 10 minutes

11/28(Mon): final exam (期末試験) (by TA Duc)

40 points

Choices are;

1. Pens and pencils
2. +hand written notes
3. +copy of slides
4. +textbooks
5. +anything without electricity

Range of exam: Lesson 8~11?（講義8~11?）

11
Ring, Field
(Ideal, Euclidean ring, field, finite field)

Ryuhei Uehara

第11回
環・体
(イデアル，Euclid環，体，有限体)

上原　隆平

Contents

- Ideal
- Euclidean ring
- Factor ring
- Field
- Finite field

本講義の内容

- イデアル
- Euclid環
- 剰余環
- 体
- 有限体

Ideal

Hereafter, we assume that R is commutative ring.

Definition 11.1

When a subset I of a ring R satisfies the following two conditions, I is called an ideal of R:

① $I \ni b, c \Rightarrow b + c \in I$

② $R \ni r, I \ni b \Rightarrow rb \in I$

Theorem 11.1

An ideal I of a ring R is a submodule of R for addition.

Proof

It is sufficient to show that I is a subgroup, that is, $a \circ b^{-1} \in I$ for $\forall a, b \in I$.

By ②, we have $(-1)b \in I$ for $R \ni -1, I \ni b$.

By ①, we have $a + (-1)b \in I$ for $I \ni a, (-1)b$

Therefore, I is a submodule of R for addition.

イデアル

これ以降，Rは可換環のみを扱うことにする

定義11.1

環Rの部分集合Iが次の2つの条件を満たすとき，IはRのイデアルという

① $I \ni b, c \Rightarrow b + c \in I$

② $R \ni r, I \ni b \Rightarrow rb \in I$

定理11.1

環RのイデアルIは，加法に関してRの部分加群である

証明

部分群であること，すなわち$\forall a, b \in I$に対して$a \circ b^{-1} \in I$を示せばよい

②より，$R \ni -1, I \ni b$に対して$(-1)b \in I$が成り立つ

①より，$I \ni a, (-1)b$に対して$a + (-1)b \in I$が成り立つ

以上により，Iは加法に関してRの部分加群である

Principal ideal

Theorem 11.2

For an element a in a ring R, $(a) = aR = \{ar | r \in R\}$ is an ideal of R (this aR is a principal ideal generated by a).

Proof

For $aR = \{ar | r \in R\} \ni ar_1, ar_2, R \ni r_3$, since we have $ar_1 + ar_2 = a(r_1 + r_2) \in aR$, $r_3(ar_1) = a(r_1 r_3) \in aR$, aR is an ideal.

Definition 11.2

When any ideal of a ring R is a principal, we say that R is a principal ideal ring.

Example 11.1

For ring of integers $\mathbb{Z}$, describe the following ideals as principal ideals;

$$(2) = 2\mathbb{Z}$$
$$(3) = 3\mathbb{Z}$$

単項イデアル

定理11.2

環Rの元aに対して，$(a) = aR = \{ar | r \in R\}$は，$R$のイデアルになる（この$aR$を$a$で生成された単項イデアルという）．

証明

$aR = \{ar | r \in R\} \ni ar_1, ar_2, R \ni r_3$に対して，$ar_1 + ar_2 = a(r_1 + r_2) \in aR$，$r_3(ar_1) = a(r_1 r_3) \in aR$より，$aR$はイデアルとなる

定義11.2

環Rの任意のイデアルが単項イデアルであるとき，Rは単項イデアル環であるという

例11.1

整数環$\mathbb{Z}$において，次のイデアルを単項イデアルとして表せ

$$(2) = 2\mathbb{Z}$$
$$(3) = 3\mathbb{Z}$$

Definition of Euclidean ring

Definition 11.3

For a ring R, if there is a mapping $\varphi\,(\varphi\colon R \to \{0\} \cup \mathbb{N})$ from R to $\{0\} \cup \mathbb{N}$ and they satisfy the following two conditions, R is called Euclidean ring.

① $R \ni a \neq 0 \Rightarrow \varphi(0) < \varphi(a)$

② For $R \ni a \neq 0, R \ni b$, there exist $q, r \in R$ such that $b = aq + r, \varphi(r) < \varphi(a)$.

Example 11.2

The ring of integers $\mathbb{Z}$ is Euclidean ring. The following mapping from an integer a to its absolute value with $\mathbb{Z}$, they satisfy these two conditions of the Euclidean ring.

$$\varphi\colon \mathbb{Z} \to \{0\} \cup \mathbb{N} \quad (a \longmapsto |a|)$$

Euclid環の定義

定義11.3

環Rから$\{0\} \cup \mathbb{N}$への写像φ（$\varphi: R \to \{0\} \cup \mathbb{N}$）があって，次の2つの条件を満たすとき，$R$はユークリッド環であるという．

① $R \ni a \neq 0 \Rightarrow \varphi(0) < \varphi(a)$

② $R \ni a \neq 0, R \ni b$ならば，$b = aq + r, \varphi(r) < \varphi(a)$を満たす$q, r \in R$が存在する

例11.2

整数環$\mathbb{Z}$はユークリッド環である．整数aに対してその絶対値を対応させる次の写像を考えると，$\mathbb{Z}$はユークリッド環の条件を満たす．

$$\varphi: \mathbb{Z} \to \{0\} \cup \mathbb{N} \quad (a \longmapsto |a|)$$

Theorem for Euclidean ring (1/2)

Theorem 11.3

Any Euclidean ring is a principal ideal ring. (Any ideal in an Euclidean ring is a principal ideal.)

Proof

Let R be an Euclidean ring, and I its ideal.

Since R is an Euclidean ring, there exists $\varphi: R \to \{0\} \cup \mathbb{N}$.

Letting $S = \{\varphi(x) | I \ni x \neq 0\}$, since $S \subseteq \{0\} \cup \mathbb{N}$, S has a minimum element. Let $\varphi(a)$ $(a \in I)$ be this minimum element. We show that $I = aR$

Euclid環の定理(1/2)

定理11.3

ユークリッド環は単項イデアル環である(ユークリッド環の任意のイデアルは単項イデアルである)

証明

Rをユークリッド環，Iをそのイデアルとする

Rがユークリッド環より，$\varphi: R \to \{0\} \cup \mathbb{N}$が存在する

$S = \{\varphi(x) | I \ni x \neq 0\}$とおくと，$S \subseteq \{0\} \cup \mathbb{N}$より，$S$には最小の元が存在

これを $\varphi(a)$ $(a \in I)$ とおく

次ページで $I = aR$ を示す

Theorem for Euclidean ring（2/2）

Proof（continued）

① $I \supset aR$:

Since aR is a principal ideal, it belongs to I.

② $I \subset aR$:

For $I \ni b$, by the property of an Euclidean ring, there exist $q, r \in R$ that satisfy $b = aq + r, \varphi(r) < \varphi(a)$.

By $I \ni b, aq$, we can say that $r = b - aq$ is also an ideal.

By the assumption that $\varphi(a)$ is a minimum element in S, to satisfy both of $r \in I$ and $\varphi(r) < \varphi(a)$, it should be that $r = 0$.

Therefore, $b = aq \in aR$

By ①②, R is a principal ideal.

By Example 11.2 and Theorem 11.3, the ring of integers is a principal ideal.

Euclid環の定理(2/2)

証明(つづき)

① $I \supset aR$:

aRは単項イデアルであるので当然Iに含まれる

② $I \subset aR$:

$I \ni b$に対して, ユークリッド環の性質より, $b = aq + r, \varphi(r) < \varphi(a)$を満たす$q, r \in R$が存在する

$I \ni b, aq$より, $r = b - aq$もイデアルとなる

$\varphi(a)$がS内の最小の元であることから, $r \in I$かつ$\varphi(r) < \varphi(a)$を満たすには$r = 0$以外あり得ない

よって, $b = aq \in aR$

①②より, Rは単項イデアル環である

例11.2と定理11.3より, 整数環は単項イデアル環である

Factor ring (1/2)

Theorem 11.4

Let I be an ideal in a ring R. For the set R/I of residue classes modulo I, we define addition and multiplication as follows; that is, for any elements a, b in R, we define the following operations.

$$\overline{a} + \overline{b} = \overline{a+b}, \qquad \overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

Then for these operations, the set R/I of residue classes is a ring.

Proof

We show that $R/I = \{g + I | g \in R\}$ is a ring.

Since I is a normal subgroup of R, R/I is quotient module and commutative group.

①(Closure) For $R/I \ni a+I, b+I, (a+I)+(b+I) = (a+b)+I \in R/I$

②(Associative) For $R/I \ni a+I, b+I, c+I$, $(a+I+b+I)+c+I = a+I+(b+I+c+I)$

③(Identity element) For $R/I \ni \forall(a+I)$, since we have $(a+I)+I = a+I$, there is an identity element $I \in R/I$.

④(Inverse) For $R/I \ni \forall(a+I)$, there is $(-a+I) \in R/I$ with $(a+I)+(-a+I) = I$.

剰余環(1/2)

定理11.4

Iを環Rのイデアルとすると，Iを法とする剰余類全体の集合R/Iに対して，加法と乗法を次のように定義する，すなわち，Rの元a, bに対して，以下を定義すると，これらの演算に関して，剰余類の全体R/Iは環になる．

$$\overline{a}+\overline{b}=\overline{a+b}, \qquad \overline{a}\cdot\overline{b}=\overline{a\cdot b}$$

証明

$R/I=\{g+I|g\in R\}$が環になることを示す

IはRの正規部分(加)群になるので，R/Iは剰余(加)群かつ可換群となる

①(演算に関して閉じる)$R/I \ni a+I, b+I$に対して，$(a+I)+(b+I)=(a+b)+I\in R/I$

②(結合律)$R/I \ni a+I, b+I, c+I$に対して，$(a+I+b+I)+c+I=a+I+(b+I+c+I)$

③(単位元(零元)の存在)$R/I \ni \forall(a+I)$に対して，$(a+I)+I=a+I$となるので，零元$I\in R/I$が存在

④(逆元の存在)$R/I \ni \forall(a+I)$について，$(a+I)+(-a+I)=I$となる$(-a+I)\in R/I$が存在

Factor ring（2/2）

Proof（Continued）

For the multiplication $\cdot$, it is sufficient to show the following properties.

① （Associative）$\big((a+I)\cdot(b+I)\big)\cdot(c+I)=(a+I)\cdot\big((b+I)\cdot(c+I)\big)$

② （Commutative）Trivial because it is commutative ring.

③ （Identity element）Since $(a+I)\cdot(1+I)=a+I$, $1+I$ is the identity element.

④ （Distributive）$(a+I)\cdot\big((b+I)+(c+I)\big)=(a+I)\cdot\big((b+c)+I\big)=a\cdot(b+c)+I=a\cdot b+a\cdot c+I=(a\cdot b+I)+(a\cdot c+I)=(a+I)\cdot(b+I)+(a+I)\cdot(c+I)$

When $a,b\in R$ satisfy $a-b\in I$, we denote by $a\equiv b(\mathrm{mod}\ I)$.

Since R/I is a ring, the multiplicative inverse（$a^{-1}+I\in R/I$）does not necessarily exist

剰余環(2/2)

証明(つづき)

乗法 $\cdot$ について次の性質が成り立つことを示せばよい

① (結合法則) $\big((a+I)\cdot(b+I)\big)\cdot(c+I)=(a+I)\cdot\big((b+I)\cdot(c+I)\big)$

② (交換法則) 可換環より明らか

③ (単位元) $(a+I)\cdot(1+I)=a+I$より, $1+I$が単位元

④ (分配法則) $(a+I)\cdot\big((b+I)+(c+I)\big)=(a+I)\cdot\big((b+c)+I\big)=a\cdot(b+c)+I=a\cdot b+a\cdot c+I=(a\cdot b+I)+(a\cdot c+I)=(a+I)\cdot(b+I)+(a+I)\cdot(c+I)$

$a,b\in R$ が $a-b\in I$ となるとき, $a\equiv b(\mathrm{mod}\ I)$ と書く

R/Iは環であるため, 乗法逆元($a^{-1}+I\in R/I$)が必ず存在するとは限らない

Example of factor ring (1/2)

The ring $\mathbb{Z}$ of integers is a commutative ring.

In the factor ring of $\mathbb{Z}$ modulo an ideal $m\mathbb{Z}$, for two integers a, b, we denote as follows;

$$a - b \in m\mathbb{Z} \Leftrightarrow a \equiv b \pmod{m}$$

The reminder r of an integer a divided by $m \neq 0$ satisfies $0 \leq r \leq m - 1$, and hence the number of residue classes modulo m is m.

Example 11.3

The residue classes modulo 3 are the following three subsets;

$$3\mathbb{Z} = \{\cdots, -3, 0, 3, \cdots\}$$
$$1 + 3\mathbb{Z} = \{\cdots, -2, 1, 4, \cdots\}$$
$$2 + 3\mathbb{Z} = \{\cdots, -1, 2, 5, \cdots\}$$

Since $3\mathbb{Z}$ is an ideal, $\mathbb{Z}/3\mathbb{Z}$ is a factor ring.

How can you represent $\mathbb{Z}/3\mathbb{Z}$ by representative elements?

剰余環の例(1/2)

整数環$\mathbb{Z}$は可換環である

$\mathbb{Z}$のイデアル$m\mathbb{Z}$を用いた剰余環では，2整数a, bに対して，以下のように表す

$$a - b \in m\mathbb{Z} \Leftrightarrow a \equiv b \pmod{m}$$

整数aを$m \neq 0$で割った余りrは$0 \leq r \leq m - 1$であるから，mを法とした剰余類はm個存在する

例11.3

3を法とした剰余類は，以下の3個である

$$3\mathbb{Z} = \{\cdots, -3, 0, 3, \cdots\}$$
$$1 + 3\mathbb{Z} = \{\cdots, -2, 1, 4, \cdots\}$$
$$2 + 3\mathbb{Z} = \{\cdots, -1, 2, 5, \cdots\}$$

$3\mathbb{Z}$はイデアルなので，$\mathbb{Z}/3\mathbb{Z}$は剰余環

$\mathbb{Z}/3\mathbb{Z}$を代表元で表すと？

Example of factor ring（2/2）

In the case of $\mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$:

- The (multiplicative) inverse of $\mathbb{Z}/3\mathbb{Z} \ni 2$?
- Reduced residue classes modulo 3 : $U(\mathbb{Z}/3\mathbb{Z})$

  $U(\mathbb{Z}/3\mathbb{Z}) = \{\mathbb{Z}/3\mathbb{Z} \ni a | a^{-1} \in \mathbb{Z}/3\mathbb{Z}\} = \{1,2\} = \mathbb{Z}/3\mathbb{Z} \setminus \{0\}$
- Zero divisor?

In the case of $\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$:

- The (multiplicative) inverse of $\mathbb{Z}/4\mathbb{Z} \ni 2$?
- Reduced residue classes modulo 4 : $U(\mathbb{Z}/4\mathbb{Z})$

  $U(\mathbb{Z}/4\mathbb{Z}) = \{\mathbb{Z}/4\mathbb{Z} \ni a | a^{-1} \in \mathbb{Z}/4\mathbb{Z}\} = \{1,3\}$
- Zero divisor?

How about $\mathbb{Z}/5\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}$?

剰余環の例(2/2)

$\mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$の場合

$\mathbb{Z}/3\mathbb{Z} \ni 2$の(乗法)逆元は？

3を法とする既約剰余類の全体: $U(\mathbb{Z}/3\mathbb{Z})$

$$U(\mathbb{Z}/3\mathbb{Z}) = \{\mathbb{Z}/3\mathbb{Z} \ni a | a^{-1} \in \mathbb{Z}/3\mathbb{Z}\} = \{1,2\} = \mathbb{Z}/3\mathbb{Z} \setminus \{0\}$$

零因子は？

$\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$の場合

$\mathbb{Z}/4\mathbb{Z} \ni 2$の(乗法)逆元は？

4を法とする既約剰余類の全体: $U(\mathbb{Z}/4\mathbb{Z})$

$$U(\mathbb{Z}/4\mathbb{Z}) = \{\mathbb{Z}/4\mathbb{Z} \ni a | a^{-1} \in \mathbb{Z}/4\mathbb{Z}\} = \{1,3\}$$

零因子は？

$\mathbb{Z}/5\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}$の場合は？

Lemma for factor ring

Lemma 11.1

For a factor ring $\mathbb{Z}/m\mathbb{Z}\ (m > 1)$, we have the following;

(1) If $\mathbb{Z}/m\mathbb{Z}$ has a zero divisor different from 0 $\Leftrightarrow$ m is a composite number

(2) $\mathbb{Z}/m\mathbb{Z}$ is an integral domain $\Leftrightarrow$ m is a prime

Proof of (1)

($\Rightarrow$)

Assume that $\mathbb{Z}/m\mathbb{Z}$ has a zero divisor not equal to 0.

Now $a \cdot b \equiv 0 \pmod{m}$ for some pair of integers $a, b\,(1 < a, b < m)$.

Since $a \cdot b \equiv 0 \pmod{m}$, $\gcd(a \cdot b, m) = m > 1$ (great common divisor is m)

Therefore, we have $\gcd(a, m) > 1$ or $\gcd(b, m) > 1$.

If $\gcd(a, m) = d > 1$, since $d|m$, m is a composite number.

($\Leftarrow$)

When m is a composite number, there are two integers $m > d, t > 1$ such that $m = dt$.

Then since $\mathbb{Z}/m\mathbb{Z} \ni d, t\ (d \neq 0, t \neq 0)$ and $dt = 0 \pmod{m}$, both d and t are zero divisor different from 0.

剰余環の補題

補題11.1

剰余環$\mathbb{Z}/m\mathbb{Z}\ (m>1)$において，以下が成り立つ

(1)$\mathbb{Z}/m\mathbb{Z}$が0と異なる零因子を持つ ⇔ mは合成数

(2)$\mathbb{Z}/m\mathbb{Z}$が整域である ⇔ mは素数

(1)の証明

(⇒)

$\mathbb{Z}/m\mathbb{Z}$が0と異なる零因子を持つとする

$a\cdot b\equiv 0\ (\mathrm{mod}\ m)$となる整数$a,b\ (1<a,b<m)$が存在する

$a\cdot b\equiv 0\ (\mathrm{mod}\ m)$より，$\gcd(a\cdot b,m)=m>1$（最大公約数が$m$）

よって，$\gcd(a,m)>1$または$\gcd(b,m)>1$が成り立つ

$\gcd(a,m)=d>1$とすると，$d|m$より，mは合成数である

(⇐)

mを合成数とすると，$m=dt$となる整数$m>d,t>1$が存在する

$\mathbb{Z}/m\mathbb{Z}\ni d,t\ (d\neq 0,t\neq 0)$ かつ $dt=0\ (\mathrm{mod}\ m)$ より，dおよびtが0と異なる零因子

Field

Definition 11.4

For a commutative ring R, if all elements except additive identity 0 are all regular elements, R is called field.

The set $\mathbb{Q}$ of rational numbers, the set $\mathbb{R}$ of real numbers, and the set $\mathbb{C}$ of complex numbers are all fields.

In a field K, every element except 0 has its inverse. Therefore, the group of unit K^* of K coincides with $K - \{0\}$. (K^* is called multiplicative group of the field K.)

The field of finite order is called "finite field" or "Galois field".

Factor ring $\mathbb{Z}/m\mathbb{Z}$ is a finite field $\mathbb{F}_p$ of order p when m is a prime p.

In coding theory, they use "$\mathrm{GF}(p)$", but they use "$\mathbb{F}_p$" in number theory.

体

定義11.4

可換環Rの零元0以外の元がすべて乗法に関して正則元であるとき，Rを体という

有理数全体の集合$\mathbb{Q}$，実数全体の集合$\mathbb{R}$，複素数全体の集合$\mathbb{C}$はすべて体である

体Kにおいて，0以外の元は逆元を持つので，Kの単元群K^*は$K - \{0\}$と一致する（K^*は体Kの乗法群とよぶ）

位数が有限の体を有限体（finite field）またはガロア体（Galois field）という

剰余環$\mathbb{Z}/m\mathbb{Z}$は，mが素数pのとき位数pの有限体$\mathbb{F}_p$になる

符号理論では$\mathrm{GF}(p)$を使うが，整数論では$\mathbb{F}_p$を使う

Lemma for field

Lemma 11.2

A factor ring $\mathbb{Z}/p\mathbb{Z}$ is a field for a prime p.

Proof

For $\mathbb{Z}/p\mathbb{Z} \ni \forall a\ (a \neq 0)$, we have $\gcd(a, p) = 1$. Thus there exist integers x and y with $ax + py = 1$ (by extended Euclidean algorithm, which I have no time to explain…)

Then since $ax \equiv 1 \pmod{p}$, $x \pmod{p}$ is an inverse of a in $\mathbb{Z}/p\mathbb{Z}$.

Thus we have that any non-zero element is a regular element. This implies that this is a field.

体の補題

補題11.2

素数pに対する剰余環 $\mathbb{Z}/p\mathbb{Z}$ は体である

証明

$\mathbb{Z}/p\mathbb{Z} \ni \forall a\ (a \neq 0)$ に対して，$\gcd(a,p) = 1$なので，$ax + py = 1$を満たす整数x, yが存在する（拡張ユークリッド互除法（説明できませんでした）より）

このとき，$ax \equiv 1 \pmod{p}$より，$x \pmod{p}$は，aの$\mathbb{Z}/p\mathbb{Z}$上の逆元になる

ゆえに，零元以外の任意の元が正則元（単元）なので体になる

Theorem for field

Theorem 11.5

A field is an integral domain.

Proof

It is sufficient to show that, for any elements a, b in a field K, we have $ab = 0, a \neq 0 \Rightarrow b = 0$. Letting $ab = 0, a \neq 0$, since K is a filed, there is a multiplicative inverse of $a \in K$;

$$a^{-1}(ab) = a^{-1} \cdot 0$$
$$(a^{-1}a)b = 0$$
$$b = 0$$

Thus we have $ab = 0, a \neq 0 \Rightarrow b = 0$.

We note that inverse of Theorem 11.5 does not hold;

For example, $\mathbb{Z}$ is an integral domain, but it is not a field.

体の定理

定理11.5

体は整域である

証明

体Kの任意の元a, bに対して，$ab = 0, a \neq 0 \Rightarrow b = 0$を示せばよい

$ab = 0, a \neq 0$とすると，Kは体なので$a \in K$の乗法逆元が存在する

$$a^{-1}(ab) = a^{-1} \cdot 0$$
$$(a^{-1}a)b = 0$$
$$b = 0$$

よって，$ab = 0, a \neq 0 \Rightarrow b = 0$が示された

逆は成り立たない

例えば，$\mathbb{Z}$は整域であるが体ではない

Characteristic

For a field K, if there is an integer n such that the summation of n 1s makes 0; then the minimum number of them is called characteristic of the field K, and denote it by $\mathrm{ch}(K)$.

If you have no upper bound the number of 1s to make 0, the characteristic of the field K is defined by 0.

The fields of rational numbers $\mathbb{Q}$, real numbers $\mathbb{R}$, and complex numbers $\mathbb{C}$ are 0.

The finite field $\mathbb{F}_p$ is of characteristic p

Example 11.4

$\mathbb{Z}/3\mathbb{Z} = \mathbb{F}_3$ is a finite field with $\mathrm{ch}(\mathbb{F}_3) = 3$

$$\mathrm{ch}(\mathbb{F}_5) = 5$$

$$\mathrm{ch}(\mathbb{F}_p) = p \ (p \text{ is a prime})$$

標数

体Kにおいて，n個の1の和：$1+\cdots+1$が0となるような整数があるとき，その最小の数を体Kの標数（characteristic）といい，$\mathrm{ch}(K)$と表す

いくつ加えても0にならないとき，体Kの標数は0

有理数体$\mathbb{Q}$，実数体$\mathbb{R}$，複素数体$\mathbb{C}$の標数は0

有限体$\mathbb{F}_p$の標数はp

例11.4

$\mathbb{Z}/3\mathbb{Z}=\mathbb{F}_3$は有限体で，$\mathrm{ch}(\mathbb{F}_3)=3$

$\mathrm{ch}(\mathbb{F}_5)=5$

$\mathrm{ch}(\mathbb{F}_p)=p$（$p$は素数）

Prime field

For a prime p, the finite field $\mathrm{GF}(p) = \{0,1,2,\cdots,p-1\}\ (= \mathbb{Z}_p)$ of order p is called prime field, it can be constructed easily by a system of residues modulo p.

Additive inverse of $\mathbb{Z}_p$

Define as $a + b = a + b \pmod{p}$

The additive inverse $-a$ is defined by $-a = 0\ (a = 0), -a = p - a\ (a \neq 0)$

Multiplicative inverse of $\mathbb{Z}_p^*$

Define as $a \cdot b = a \cdot b \pmod{p}$

For $\forall a \in \mathrm{GF}(p) - \{0\}\ (= \mathbb{Z}_p^*)$, we have two integer b and c with $a \cdot b + c \cdot p = 1$, thus we define the multiplicative inverse of a by b.

Example

Check two tables for addition and multiplication for $\mathrm{GF}(5)$.

素体

位数が素数pの有限体$\mathrm{GF}(p) = \{0,1,2,\cdots,p-1\}\ (= \mathbb{Z}_p)$は素体とよばれ，$p$を法とする剰余演算を用いることにより容易に構成できる

$\mathbb{Z}_p$上の加法逆元

$a + b = a + b \pmod{p}$で定義

このとき，加法の逆元$-a$は，$-a = 0\ (a = 0), -a = p - a\ (a \neq 0)$

$\mathbb{Z}_p^*$上の乗法逆元

$a \cdot b = a \cdot b \pmod{p}$ で定義

$\forall a \in \mathrm{GF}(p) - \{0\}\ (= \mathbb{Z}_p^*)$に対して，$a \cdot b + c \cdot p = 1$ を満たす整数b, cが必ず存在するため，bがaの乗法逆元になる

例

$\mathrm{GF}(5)$の加法の演算表と乗法の演算表

Exercise 11

剰余環$\mathbb{Z}/12\mathbb{Z} = \mathbb{Z}_{12}$の正則元および零因子を全て求めよ. ただし, $a + 12\mathbb{Z}$の代表元を$\overline{a}$とする.（Find all of invertible elements and zero divisors of a factor ring $\mathbb{Z}/12\mathbb{Z} = \mathbb{Z}_{12}$. Note that the representative element of $a + 12\mathbb{Z}$ is denoted by $\overline{a}$.）