

# 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?)

# Overview of Group ▪ Ring ▪ Field

## Field

Like set of real numbers, arithmetic operations ( $+$ ,  $-$ ,  $\times$ ,  $/$ ) can be defined over the set.

## Finite field

Sets consists of discrete and finite elements, and we can define arithmetic operations.

In cryptography/coding theories, we need this notion since we cannot deal with real numbers directly.

## Ring

Sets without “identity element”, “inverse”, “commutative” for products in the properties of fields

## Group

Sets with one operation that satisfies “closed”, “identity element”, “inverse”, and “associativity”.

Intuitively, group has  $+$  and  $-$ , ring has  $+$ ,  $-$ , and  $\times$ , and field has  $+$ ,  $-$ ,  $\times$ , and  $/$ , respectively.

# 群・環・体

## 体

実数の集合のように、その上で加減乗除の四則演算が定義できる集合

## 有限体

離散的な有限個の要素からなり、四則演算が定義できる集合

暗号や符号等では実数を直接取り扱うことができないためこれが必要

## 環

体の条件のうち、乗法に関する「単位元の存在」「逆元の存在」「可換則」の条件を除いたものを満たす集合

## 群

1つの演算が定義されていて、その1つの演算に関して「演算が閉じている」「単位元の存在」「逆元の存在」「結合則」の条件を満たす集合

直感的には、群は加減算、環は加減乗算、体は加減乗除算が定義されている集合と考えることができる

10  
Group (3)  
Ring,  
Homomorphism  
(Homomorphism Theorem),  
Axioms of Ring

第10回  
群(3) 環, 準同型写像(準同型定理),  
環の公理

上原隆平

# Contents

- Isomorphism
- Homomorphism
- Homomorphism Theorem
- Axioms of Ring

# 本講義の内容

- 同型写像
- 準同型写像
- 準同型定理
- 環の公理

# Isomorphism

- Consider two groups:  $G_1 = \{0^\circ, 120^\circ, 240^\circ\}$ ,  $G_2 = \{f_1, f_2, f_3\}$

+	$0^\circ$	$120^\circ$	$240^\circ$
$0^\circ$	$0^\circ$	$120^\circ$	$240^\circ$
$120^\circ$	$120^\circ$	$240^\circ$	$0^\circ$
$240^\circ$	$240^\circ$	$0^\circ$	$120^\circ$

$\circ$	$f_1$	$f_2$	$f_3$
$f_1$	$f_1$	$f_2$	$f_3$
$f_2$	$f_2$	$f_3$	$f_1$
$f_3$	$f_3$	$f_1$	$f_2$

- These two groups have the same property if you observe only the structure, regardless of meaning  $G_1$  of  $G_2$  and .
- This relationship is called **isomorphic**
  - $G_1$  and  $G_2$  are isomorphic.



# 同型について

- 2つの群を考える:  $G_1 = \{0^\circ, 120^\circ, 240^\circ\}$ ,  $G_2 = \{f_1, f_2, f_3\}$

+	$0^\circ$	$120^\circ$	$240^\circ$
$0^\circ$	$0^\circ$	$120^\circ$	$240^\circ$
$120^\circ$	$120^\circ$	$240^\circ$	$0^\circ$
$240^\circ$	$240^\circ$	$0^\circ$	$120^\circ$

◦	$f_1$	$f_2$	$f_3$
$f_1$	$f_1$	$f_2$	$f_3$
$f_2$	$f_2$	$f_3$	$f_1$
$f_3$	$f_3$	$f_1$	$f_2$

- $G_1$ と $G_2$ の意味を完全に捨てて構造だけに着目すると, この2つの群は全く同じ振る舞いをする
- この関係が成り立つことを**同型**という
  - $G_1$ と $G_2$ は同型

# Isomorphism map

## Definition 10.1

For a group  $(G_1, \circ)$  with operation  $\circ$  and another group  $(G_2, *)$  with operation  $*$ , when a mapping  $f: G_1 \rightarrow G_2$  from  $G_1$  to  $G_2$  satisfies the following, this is called **isomorphism map**

$$\forall a, b \in G_1, f(a \circ b) = f(a) * f(b), \quad f \text{ is bijective}$$

- If there exists an isomorphism map for  $G_1$  and  $G_2$ ,  $G_1$  and  $G_2$  are said to be **isomorphic**, and denoted by  $G_1 \cong G_2$ .
- $f$  associates two groups
  - $f(a \circ b) = f(a) * f(b)$  means that **two operators work the same**.
  - “ $f$  is bijective” means **the order of two groups are the same**.

# 同型写像

- 定義10.1

- 演算 $\circ$ を持つ群 $(G_1, \circ)$ と演算 $*$ を持つ群 $(G_2, *)$ に対して,  $G_1$ から $G_2$ への写像 $f: G_1 \rightarrow G_2$ が以下を満たすとき,  $f$ を $G_1$ から $G_2$ への同型写像という

$$\forall a, b \in G_1, f(a \circ b) = f(a) * f(b), \quad f \text{が全単射}$$

- $G_1$ と $G_2$ の間に同型写像が存在するとき $G_1$ と $G_2$ は同型であるといい,  $G_1 \cong G_2$ と表す
- $f$ は2つの群の対応を意味する
  - $f(a \circ b) = f(a) * f(b)$ は, 演算子の振る舞いが同じであることを表す
  - 「 $f$ が全単射」は, 2つの群の位数が同じであることを表す

# Homomorphism map

## Definition 10.2

For a group  $(G_1, \circ)$  with operation  $\circ$  and another group  $(G_2, *)$  with operation  $*$ , when a mapping  $f: G_1 \rightarrow G_2$  from  $G_1$  to  $G_2$  satisfies the following, this is called **homomorphism map**

$$\forall a, b \in G, f(a \circ b) = f(a) * f(b)$$

- Image

$$\text{Im } f = \{f(a) | a \in G_1\}$$

- Kernel

$$\text{Ker } f = \{a \in G_1 | f(a) = 1_{G_2}\}$$

- Surjective

- For  $G_2 \ni \forall b$ , there exists  $a \in G_1$  with  $f(a) = b$ .

- Injective

- For  $G_1 \ni a, b$ , we have  $f(a) = f(b) \Rightarrow a = b$

# 準同型写像

## 定義10.2

演算 $\circ$ を持つ群 $(G_1, \circ)$ と演算 $*$ を持つ群 $(G_2, *)$ に対して,  $G_1$ から $G_2$ への写像 $f: G_1 \rightarrow G_2$ が以下を満たすとき,  $f$ を $G_1$ から $G_2$ への準同型写像という

$$\forall a, b \in G, f(a \circ b) = f(a) * f(b)$$

- 像

$$\text{Im } f = \{f(a) | a \in G_1\}$$

- 核

$$\text{Ker } f = \{a \in G_1 | f(a) = 1_{G_2}\}$$

- 全射

- $G_2 \ni \forall b$ に対して,  $f(a) = b$ となる $a \in G_1$ が存在する

- 単射

- $G_1 \ni a, b$ に対して,  $f(a) = f(b) \Rightarrow a = b$ となる

# Theorem of Homomorphism (1/3)

## Theorem 10.1

Let  $f: G_1 \rightarrow G_2$  be a homomorphism from a group  $G_1$  to another group  $G_2$ . Then we have the following:

- (1)  $f(1_{G_1}) = 1_{G_2}$
- (2)  $f(a^{-1}) = f(a)^{-1} (\forall a \in G)$
- (3)  $\text{Im } f$  is a subgroup of  $G_2$
- (4)  $\text{Ker } f$  is a normal subgroup of  $G_1$

## Proof of (1)

- $f(1_{G_1}) = f(1_{G_1} \circ 1_{G_1}) = f(1_{G_1}) * f(1_{G_1})$
- Applying  $f(1_{G_1})^{-1}$  on both sides by  $*$ , we have  $f(1_{G_1}) = 1_{G_2}$ .

# 準同型写像の定理(1/3)

## 定理10.1

$f: G_1 \rightarrow G_2$ が「群 $G_1$ から $G_2$ への準同型写像」とする. このとき, (1)~(4)が成り立つ.

$$(1) f(1_{G_1}) = 1_{G_2}$$

$$(2) f(a^{-1}) = f(a)^{-1} (\forall a \in G)$$

(3)  $\text{Im } f$ は $G_2$ の部分群である

(4)  $\text{Ker } f$ は $G_1$ の正規部分群である

### (1)の証明

$$f(1_{G_1}) = f(1_{G_1} \circ 1_{G_1}) = f(1_{G_1}) * f(1_{G_1})$$

両辺に $f(1_{G_1})^{-1}$ を $*$ で演算すると,  $f(1_{G_1}) = 1_{G_2}$ を得る

# Theorem of Homomorphism (2/3)

## Proof of (2)

For  $G_1 \ni \forall a$ , since  $G_1$  is a group, we have  $a^{-1} \in G_1$ .

By (1), since  $f(a) * f(a^{-1}) = f(a \circ a^{-1}) = f(1_{G_1}) = 1_{G_2}$  we have  $f(a^{-1}) = f(a)^{-1}$

## Proof of (3)

For  $\text{Im } f \ni \forall f(a), f(b)$  with  $(a, b \in G_1)$ , by (2), we have  $f(a) * f(b)^{-1} = f(a) * f(b^{-1}) = f(a \circ b^{-1}) \in \text{Im } f$ .

Therefore,  $\text{Im } f$  is a subgroup of  $G_2$ .



# 準同型写像の定理(2/3)

## (2)の証明

$G_1 \ni \forall a$ に対し,  $G_1$ は群より $a^{-1} \in G_1$

(1)を利用して,  $f(a) * f(a^{-1}) = f(a \circ a^{-1}) = f(1_{G_1}) = 1_{G_2}$ より,  $f(a^{-1}) = f(a)^{-1}$

## (3)の証明

$\text{Im } f \ni \forall f(a), f(b)$ に対して( $a, b \in G_1$ )

(2)より,  $f(a) * f(b)^{-1} = f(a) * f(b^{-1}) = f(a \circ b^{-1}) \in \text{Im } f$  が成り立つ

よって,  $\text{Im } f$ は $G_2$ の部分群である

# Theorem of Homomorphism (3/3)

## Proof of (4)

Let  $K = \text{Ker } f$ , and show the following two claims;

①  $K$  is a subgroup of  $G_1$ .

For  $K \ni a, b$ , since  $f(a) = f(b) = 1_{G_2}$  we have;  
 $f(a \circ b^{-1}) = f(a) * f(b^{-1}) = f(a) * f(b)^{-1} = 1_{G_2}$ .

Thus  $a \circ b^{-1} \in K$ .

Therefore,  $K$  is a subgroup of  $G_1$ .

②  $G_1 \triangleright K$

For  $G_1 \ni \forall a$ , by Theorem 9.2, it is sufficient to show  
 $a^{-1}Ka \subseteq K$ .

For  $K \ni k$ , we have  $f(a^{-1} \circ k \circ a) = f(a)^{-1} * f(k) * f(a)$   
 $= f(a)^{-1} * 1_{G_2} * f(a) = f(a)^{-1} * f(a) = 1_{G_2}$ .

Thus we have  $a^{-1}Ka \subseteq K$ .

# 準同型写像の定理(3/3)

## (4)の証明

$K = \text{Ker } f$  として, 以下の2つを示す

①  $K$ が $G_1$ の部分群である

$K \ni a, b$  に対して,  $f(a) = f(b) = 1_{G_2}$  より,  
 $f(a \circ b^{-1}) = f(a) * f(b^{-1}) = f(a) * f(b)^{-1} = 1_{G_2}$  が成り立つため,  
 $a \circ b^{-1} \in K$  がいえる

よって,  $K$ が $G_1$ の部分群になる

②  $G_1 \triangleright K$

$G_1 \ni \forall a$  に対して, 定理9.2より,  $a^{-1}Ka \subseteq K$  を示せばよい

$K \ni k$  に対して,  $f(a^{-1} \circ k \circ a) = f(a)^{-1} * f(k) * f(a)$   
 $= f(a)^{-1} * 1_{G_2} * f(a) = f(a)^{-1} * f(a) = 1_{G_2}$

よって,  $a^{-1}Ka \subseteq K$  が成り立つ

# Examples

## Example of isomorphic map

$\mathbb{R}^+ = \{a \mid a \in \mathbb{R}, a > 0\}$  is a group with respect to multiplication. On the other hand,  $\mathbb{R}$  is a group with respect to addition  $+$ . Then the following is an isomorphic map:

$$\begin{aligned} f: \mathbb{R}^+ &\longrightarrow \mathbb{R} \\ x &\longmapsto \log_{10} x \end{aligned}$$

## Example of homomorphic map

$\mathbb{R}^+ = \{a \mid a \in \mathbb{R}, a > 0\}$  and  $\mathbb{R}^*$  is two groups with respect to multiplication. Then the following is a homomorphic map:

$$\begin{aligned} f: \mathbb{R}^* &\longrightarrow \mathbb{R}^+ \\ x &\longmapsto x^2 \end{aligned}$$

# 例

## 同型写像の例

$\mathbb{R}^+ = \{a \mid a \in \mathbb{R}, a > 0\}$ は、乗算に関して群である。一方、 $\mathbb{R}$ は、加算  $+$ に関して群である。このとき、以下は同型写像である

$$\begin{aligned} f: \mathbb{R}^+ &\rightarrow \mathbb{R} \\ x &\mapsto \log_{10} x \end{aligned}$$

## 準同型写像の例

$\mathbb{R}^+ = \{a \mid a \in \mathbb{R}, a > 0\}$ , 及び  $\mathbb{R}^*$ は乗算に関して群である。このとき、以下は準同型写像である

$$\begin{aligned} f: \mathbb{R}^* &\rightarrow \mathbb{R}^+ \\ x &\mapsto x^2 \end{aligned}$$

# Homomorphism Theorem (1/2)

## Theorem 10.2 (Homomorphism Theorem)

Let  $f: G_1 \rightarrow G_2$  be a homomorphism map from a group  $G_1$  to a group  $G_2$ . Then we have the following (1) and (2):

$$(1) G_1/\text{Ker } f \cong \text{Im } f$$

$$(2) \text{ Especially, if } f \text{ is surjective, } G_1/\text{Ker } f \cong G_2$$

## Proof of (1)

Let  $K = \text{Ker } f$ . Then by Theorem 10.1 (4), we have  $G_1 \triangleright K$  and hence a residue class group  $G_1/K$  is defined.

Now, for  $G_1 \ni a, b$ , we have the following;

$$f(a) = f(b) \Leftrightarrow f(a \circ b^{-1}) = 1_{G_2} \Leftrightarrow a \circ b^{-1} \in K \Leftrightarrow a \circ K = b \circ K \quad (1)$$

We define a mapping from  $G_1/K$  to  $\text{Im } f$  as follows;

$$\begin{aligned} \bar{f}: G_1/K &\rightarrow \text{Im } f \\ aK &\mapsto f(a) \end{aligned}$$

Now we are ready, and it is sufficient to show that  $\bar{f}$  is an isomorphism.

# 準同型定理(1/2)

## 定理10.2(準同型定理)

- $f: G_1 \rightarrow G_2$  が群  $G_1$  から群  $G_2$  への準同型写像とする. このとき, (1), (2) が成り立つ.

(1)  $G_1/\text{Ker } f \cong \text{Im } f$

(2) 特に,  $f$  が全射ならば,  $G_1/\text{Ker } f \cong G_2$

### (1)の証明

- $K = \text{Ker } f$  とすると, 定理10.1(4)より  $G_1 \triangleright K$  となり, 剰余群  $G_1/K$  が定義できる

- ここで,  $G_1 \ni a, b$  に対して以下が成り立つ

$$f(a) = f(b) \Leftrightarrow f(a \circ b^{-1}) = 1_{G_2} \Leftrightarrow a \circ b^{-1} \in K \Leftrightarrow a \circ K = b \circ K \quad (1)$$

- $G_1/K$  から  $\text{Im } f$  への写像を次のように定義する

$$\bar{f}: G_1/K \rightarrow \text{Im } f$$

$$aK \mapsto f(a)$$

- 準備が整ったので, 後は  $\bar{f}$  が同型写像であることを示せばよい

# Homomorphism Theorem (2/2)

## Proof of (1) (Continued)

Surjective by;

For  $\text{Im } f \ni \forall f(a)$ , since  $\bar{f}(aK) = f(a)$ ,  $\text{Im } \bar{f} = \text{Im } f$ .

Injective by;

For  $G_1/K \ni aK, bK$ , by Eq. (1),  $\bar{f}(aK) = \bar{f}(bK) \Rightarrow aK = bK$

Homomorphism by;

$$\bar{f}(aKbK) = \bar{f}(abK) = f(ab) = f(a)f(b) = \bar{f}(aK)\bar{f}(bK)$$

Therefore,  $\bar{f}$  is isomorphism, and  $G_1/\text{Ker } f$  and  $\text{Im } f$  are isomorphic

## Proof of (2)

It is sufficient to show that  $\text{Im } f = G_2$  (of same cardinality).

It is clear by the assumption that  $f$  is surjective.



# 準同型定理(2/2)

## (1)の証明(つづき)

全射は以下より成り立つ

$\text{Im } f \ni \forall f(a)$  に対して,  $\bar{f}(aK) = f(a)$  であるので,  $\text{Im } \bar{f} = \text{Im } f$

単射は以下より成り立つ

$G_1/K \ni aK, bK$  に対して, 式(1)より  $\bar{f}(aK) = \bar{f}(bK) \Rightarrow aK = bK$

準同型は以下より成り立つ

$$\bar{f}(aKbK) = \bar{f}(abK) = f(ab) = f(a)f(b) = \bar{f}(aK)\bar{f}(bK)$$

よって,  $\bar{f}$ が同型写像であり,  $G_1/\text{Ker } f$  と  $\text{Im } f$  は同型である

## (2)の証明

- $\text{Im } f = G_2$  (濃度が等しい)ことを示せば十分
- $f$ が全射という仮定より明らか

# Exercise

For a mapping  $\pi: \mathbb{Z} \rightarrow \mathbb{Z}/3\mathbb{Z}$  ( $x \mapsto x \bmod 3$ ) over  $(\mathbb{Z}, +)$ ;

(1) show that  $\pi$  is homomorphic.

(2) find  $\text{Ker } \pi$ .

# 例題

$(\mathbb{Z}, +)$ 上の写像 $\pi: \mathbb{Z} \rightarrow \mathbb{Z}/3\mathbb{Z}$  ( $x \mapsto x \bmod 3$ )に対して, 以下に答えよ

- (1)  $\pi$ は準同型であることを示せ
- (2)  $\text{Ker } \pi$ を求めよ

# Axioms of Ring

## Definition 10.3

Let  $R$  be a set such that **two operators** of addition and multiplication are defined. Then  $R$  is a ring if it satisfies the following conditions;

(1)  $(R, +)$  is a commutative group, that is,

- ① **Associative law**
- ② **Commutative**
- ③ **Identity element 0**
- ④ **Inverse**

(2) For multiplication  $\circ$ , we have the following;

- ① **Associative**
- ② **Identity element 1**
- ③ **Distributive property** for operation  $+$

$$a \times (b + c) = a \times b + a \times c$$

# 環の公理

- 定義10.3

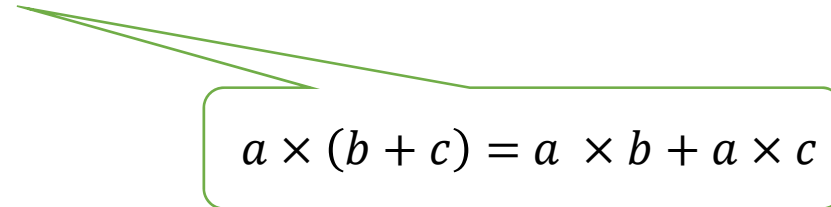
加法と乗法という2つの演算の定義された集合 $R$ が環であるとは、 $R$ が次の条件を満たすことである。

(1)  $(R, +)$ は可換群である

- ① 結合法則が成り立つ
- ② 交換法則が成り立つ
- ③ 単位元 $0$ がある
- ④ 逆元がある

(2) 乗法 $\circ$ について次の性質が成り立つ

- ① 結合法則が成り立つ
- ② 単位元 $1$ がある
- ③ 演算 $+$ との間に、分配法則が成り立つ


$$a \times (b + c) = a \times b + a \times c$$

# Property of ring

## Definition 10.4

For an  $R \ni a$ , if there is a  $R \ni b \neq 0$  with  $ab = 0$ ,  $a$  is called **zero divisor**.  
 $0$  is a zero divisor.

## Definition 10.5

If ring  $R$  has no zero divisor except  $0$ , that is, if we always have  
 $a \neq 0, b \neq 0 \Rightarrow ab \neq 0$ ,  $R$  is called **integral domain**.

## Commutative ring

Ring that also satisfies commutative law for multiplication

## Module

Group for addition

## Additive identity

Identity element in module (identity element in a group for multiplication is just called identity element.)

# 環の性質

## 定義10.4

環  $R \ni a$  に対して,  $R \ni b \neq 0$  で  $ab = 0$  となる元が存在するとき,  $a$  を **零因子** とよぶ.  $0$  も零因子である.

## 定義10.5

環  $R$  が  $0$  以外の零因子を含まないとき, すなわち,  $a \neq 0, b \neq 0 \Rightarrow ab \neq 0$  が常に成り立つとき,  $R$  を **整域** とよぶ.

## 可換環

環の公理に加えて, 乗法の交換法則を満たす環のこと

## 加群

加法に関する群

## 零元

加群の単位元 (乗法群の単位元は単に単位元とよぶ)

# Examples of ring

## Example 1

$(\mathbb{Z}; +, \times)$  is a ring.

## Example 2

$(\mathbb{R}; +, \times)$  is a ring.

## Example 3

$\mathbb{Z}$  is an integral domain.



# 環の例

## 例1

$(\mathbb{Z}; +, \times)$ は環である

## 例2

$(\mathbb{R}; +, \times)$ は環である

## 例3

$\mathbb{Z}$ は整域である

# Subring

- If a subset  $S$  of a ring  $R$  satisfies the following, we call  $S$  a **subring** of  $R$ .
  - ①  $a, b \in S \Rightarrow a - b \in S$
  - ②  $a, b \in S \Rightarrow ab \in S$
  - ③  $1_R \in S$
- In a ring  $R$ , if an element  $R \ni a$  has its inverse for multiplication, that is, if there is an element  $b \in R$  with  $b = ba = 1_R$ ,  $a$  is called a **regular element** or **unitary element**, and we denote by  $b = a^{-1}$ .
- For a commutative ring  $R$ , the set of elements having inverse generates a group for multiplication. This group is called **group of units** of  $R$ , and denoted by  $R^*$  or  $U(R)$ .

# 部分環

- 環 $R$ の部分集合 $S$ が次の条件を満たすとき,  $S$ は $R$ の**部分環**であるという
  - ①  $a, b \in S \Rightarrow a - b \in S$
  - ②  $a, b \in S \Rightarrow ab \in S$
  - ③  $1_R \in S$
- 環 $R$ において,  $R \ni a$ が乗法に関して逆元をもつとき, すなわち,  $ab = ba = 1_R$ となる $b \in R$ が存在するとき,  $a$ は**正則元**あるいは**単元**であるとい  
い,  $b = a^{-1}$ と書く
- 可換環 $R$ において, 積に関して逆元をもつ元全体の集合は積に関して群  
をなす. この群を $R$ の**単元群**といい,  $R^*$ あるいは **$U(R)$** と表す.

## Exercise (10)

(1)  $x > 0$  のとき  $f(x) = 1$ ,  $x < 0$  のとき  $f(x) = -1$  によって定義される写像がある. この写像が, 乗法群  $R^*$  から乗法群  $\{1, -1\}$  への準同型写像であることを示せ (We have a mapping defined by  $f(x) = 1(x > 0)$  and  $f(x) = -1(x < 0)$ . Prove that this mapping is a homomorphism from multiplicative group  $R^*$  to multiplicative group  $\{1, -1\}$ .)

(2)  $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$  (ガウスの整数環という) は環である. これが整域であることを示せ. ( $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$  is a ring. Prove that this is an integral domain.)