Rings MA113

Definition: In ring R, a is a **divisor of zero** if it is a non-zero element and if $\exists b \in R$ such that $ab = 0$.

Definition: An **integral domain** is a commutative ring with no divisors of zero.

- $\mathbb{Z}$ and $2\mathbb{Z}$ are integral domains but NOT fields.

Definition: A **division ring** or skew field is a ring in which every non-zero element has an inverse under TIMES.

- eg. The Real Quaternions.
- Definition: A **field** is a commutative division ring.

: a double Abelian group.

Theorem: A finite integral domain is a field.

Theorem: Every field is an integral domain.

Theorem: In an integral domain D if $\exists m \in \mathbb{Z} \& a \in D$ such that $ma = 0$, then $mx = 0 \forall x \in D$.

Definition: In an integral domain D **the characteristic** of D is the least positive integer m such that $md = 0$ for $d \in D$.

m is prime.

- Only in an integral domain is characteristic well defined.

****

Definition: A **homomorphism** defined on a ring R is a mapping from R to a ring $\overline{R}$ such that

i $\phi(a+b) = \phi(a) + \phi(b)$

ii $\phi(ab) = \phi(a)\phi(b)$

- Given a subgroup N of R under +

$\exists$ homomorphism $\phi : R \longrightarrow \dfrac{R}{N}$

i $\phi(0) = \overline{0}$

ii $\phi(-a) = -\phi(a)$

iii $\phi(1) \neq \overline{1}$

If

i $\overline{R}$ is an integral domain

or

ii $\overline{R}$ is arbitrary but ϕ is onto

then $\phi(1) = \overline{1}$

Definition: If $\phi : R \longrightarrow \overline{R}$ is a Homomorphism

- $\ker(\phi) = \{r \in R : \phi(r) = \overline{0}\}$

$\phi(R)$ is a subring of $\overline{R}$

- PROPERTIES of $\ker(\phi)$ in R

i subgroup of R under +

ii absorbs all products (under .)

1 IDEALS

Definition: An ideal U of ring R

is a subset U of R

such that

i U is a subgroup of R under +

ii U absorbs products with its elements

Lemma: $\frac{R}{U}$ is a ring

i $(U + a)+(U + b) = U + a + b$

ii $(U + a).(U + b) = U + ab$

i U is a subgroup of R under +

ii U absorbs products with its elements

Lemma

- R Abelian $\Longrightarrow \frac{R}{U}$ Abelian
- R has the unit element 1 $\Longrightarrow \frac{R}{U}$ has the unit coset $U + 1$

****

- Isomorphism Theorems
- Homomorphism $\phi : R \longrightarrow \overline{R}$ is onto with kernel U
- There is a $1 - 1$ correspondence between the set of ideals of $\overline{R}$ onto the set of ideals of R which contain U.
- R commutative $\Longrightarrow \overline{R}$ commutative.

Lemma: Ideal U is a subring of R

Lemma: The intersection of a finite number of ideals is an ideal.

Lemma: $R[x]$ is a ring.

Lemma: A subring of an integral domain is an integral domain.
****

Lemma: The GAUSSIAN INTEGERS $\mathbb{Z}[i]$ form an integral domain.

Lemma: If $\phi : R \longrightarrow \overline{R}$

is an isomorphism onto $\overline{R}$

then so is $(\phi)^{-1}$
****

Theorem: A field has only two ideals.

Converse: If R is a commutative ring with 1 whose only two ideals are $\{0\}$ and R then R is a field

Theorem: If R is a commutative ring with 1 then R is a field $\Longleftrightarrow$ R has only two ideals.

Examples:

1. $\{0, 1\}$ is a field.
2. $\mathbb{Z}$ is not a field.

Definition:

> An IDEAL M of ring R is MAXIMAL
> if M⊆U⊆R $\Longrightarrow$ M=U or U=R

Lemma: In $\mathbb{Z}$ ideal $< n >$ is maximal

$\Longleftrightarrow$

n is prime.

Lemma: If R is a ring and U an ideal then

Homomorphism $\phi : R \longrightarrow \dfrac{R}{U}$ is order-preserving.

i.e. If R has two ideals J⊂K then $\phi(J) \subset \phi(K)$

- $\ker(\phi) = U$ ⊂J

Theorem: If R is a commutative ring with 1 and M an ideal of R

then M is a maximal ideal $\iff \dfrac{R}{M}$ is a field.

$\phi(J) \subset \phi(K)$

Examples:

1. $$\frac{\mathbb{Z}}{<3>}$$ is a field.
2. $$\frac{\mathbb{Z}}{<6>}$$ is a not a field.

Lemma: The homomorphic images of a field

are $\{0\}$ and F itself.

- EMBEDDING of a ring R in an integral domain

  $\mathbb{Z}$ can be embedded in the field of quotients $\mathbb{Q}$.

  Theorem: Every integral domain can be embedded in a FIELD

EUCLIDEAN RING

Examples:

1. $\mathbb{Z}$
2. GAUSSIAN INTEGERS
3. Polynomial Rings

Definition: A EUCLIDEAN RING R is an integral domain in which a a non-zero element $d(a)$ called NORM is defined on all non-zero elements $a \in R$ such that

1. $d(a) \leq d(ab)\ \forall a, b \in R,\ a \neq 0, b \neq 0$
2. $\forall a, b \in R,\ a \neq 0,\ b \neq 0,$
   $\exists t, s \in R$ such that$a = bt + r$
   where $d(r) < d(b)$ or $r = 0$.

Examples:

1. In $\mathbb{Z}$ $d(a) = |a|$
2. In the Gaussian Integers $\mathbb{Z}[i]$, $d(a + ib) = a^2 + b^2$
3. In a field F if $d(a) = 1$ for each non-zero $a \in F$
4. In $\mathbb{Q}[x]$ if $d(f) =$deg(f)
5. In $\mathbb{Z}[\sqrt{-d}]$ $d(a + b\sqrt{d}) = |a^2 - db^2|$
6. In $\mathbb{Z}[\sqrt{d}]$ $d(a + b\sqrt{d}) = a^2 + db^2$

Theorem: If R is a Euclidean ring and A an ideal of R

Then $A = \{ax : x \in R\}$

Definition: A PRINCIPAL ideal U of integral domain R with unit element 1

is a subset U of R such that $U =< a >= Ra$

Definition: A PRINCIPAL ideal domain or p.i.d. is an integral domain R with unit element 1 in which every ideal is principal

Theorem: A Euclidean ring has the unit element 1

Theorem: A Euclidean ring is a principal ideal ring.

The converse is false.

- ER$\subseteq$p.i.d. $\subseteq$UFD

2 NUMBER THEORY

- In a ring R, a divides b denoted by a/b

  if $\exists c \in R$ s.t. $ac = b$.

- g.c.d. of $a,\ b$ (denoted by a/b) is d if

  i d/a and d/b

  ii $\forall c \in R$ c/a and $c/b \implies c/d$

  Now R is a ring with 1.

- DEFINITIONS:

- u is a UNIT iff $\exists v \in R$ s.t. $uv = vu = 1$

- a, b are ASSOCIATES iff $\exists$a unit $u \in R$ s.t. $a = ub$

- π is IRREDUCIBLE in R iff $\pi \neq 0,\ \pi \not{a}$ unit and $\pi = ab \implies a$ or b is a unit

- p is PRIME in R iff $p \neq 0,\ p \not{a}$ unit and $p/ab \implies p/a$ or p/b

- In fields each element is a unit. So Primes and irreducibles are not defined.

- l.c.m. of $a,\ b$ is l if

  i a/l and b/l

  ii $\forall c \in R$ a/c and $b/c \implies l/c$

- $d \in \mathbb{Z}$ is SQUARE FREE if

  $d \neq 1$ and $x^2/d,\ x \in \mathbb{Z} \Longrightarrow x = 1$

- $(\mathbb{Z}[\sqrt{d}], +, .)$ where d is SQUARE FREE

  is an integral domain.

  $\text{Norm}(a + b\sqrt{d}) = N(\alpha) = |a^2 - db^2|$

  $N(\alpha) = |a^2 - db^2| \in \mathbb{Z}$

  $N(\alpha) = 0 \Longleftrightarrow \alpha = 0$

  $N(\alpha\beta) = N(\alpha)N(\beta)$

  $N(\alpha) \leq N(\alpha\beta)$

  u is a unit in $(\mathbb{Z}[\sqrt{d}], +, .)$

  $\Longrightarrow N(u) = 1$

- EUCLIDEAN ALGORITHM
- To find g.c.d. of $a,\ b$

  $b = aq_0 + r_1$ where $d(r_1) < d(a)$

  $a = r_1 q_1 + r_2$ where $d(r_2) < d(r_1)$

  $\vdots$

  $r_{n-1} = r_n q_n$
- then $(a, b) = r_n$

- THEOREM: In a EUCLIDEAN Ring
- π irreducible $\Longrightarrow \pi$ prime.

- THEOREM: In a UFD
- π irreducible $\Longleftrightarrow \pi$ prime.
- Lemma: In a EUCLIDEAN Ring
- $d(a) < d(ab)$ if b is not a unit.

  Definition: A UNIQUE FACTORIZATION domain or UFD is an integral domain with unit element 1
- in which every element a which is not zero or a unit
- is a unique product of a finite number of irreducible elements. (up to associates)

THEOREM: pid $\Longrightarrow$ UFD.

Lemma: In a EUCLIDEAN Ring R

$d =$ g.c.d(a,b) $\Longrightarrow d = \lambda a + \mu b$

Lemma: In an integral domain with unit element 1

a/b and $b/a \implies a = ub$ where u is a unit.

Lemma: In a commutative ring with unit element 1

the relation a is an associate of b is an equivalence relation.

Equivalence class $[a]$ is the set of associates of a.

Lemma: NORM(1) is MINIMUM norm.

- Norm(u)=Norm(1) for all units.
- Norm(a)=Norm(ab) $\iff$ b is a unit
- Norm(a)<Norm(ab) $\iff$ b is NOT a unit

Lemma: A unit generates R

Lemma: In a EUCLIDEAN Ring R

an element is either a unit or can be written as the product of a finite number of PRIMES

- Proof by induction on Norm(a)

Lemma: x = g.c.d. of a,b

and x = associate of y $\iff$ both x and y are g.c.d.'s

Definition: a, b are RELATIVELY PRIME if (a,b)=u.

- a, b are RELATIVELY PRIME $\iff$ (a,b)=1

UNIQUE FACTORIZATION THEOREM

THEOREM: : In a EUCLIDEAN Ring R

Every element is a unit or else

can be expressed UNIQUELY as THE FINITE PRODUCT OF Primes (up to ASSOCIATES)

Lemma: In a EUCLIDEAN Ring R

IDEAL Ra is MAXIMAL $\Longrightarrow$ a is PRIME.
****

Lemma: In$\mathbb{Z}$, p prime, (c,p)=1,

and $x^2 + y^2 = cp \Longrightarrow \exists$ a, b∈Z such that $a^2 + b^2 = p$

- $3^2 + 7^2 = 2 \times 29 \;\Longrightarrow 1^2 + 1^2 = 2$ and $2^2 + 5^2 = 29$

BECAUSE $p = a^2 + b^2 = (a + bi)(a - bi)$ is not irreducible in$\mathbb{Z}$[i]

FERMAT'S LITTLE THEOREM: :

THEOREM: : $a^p = a$ mod p, a ∈Z, p prime.

WILSON'S THEOREM: :

THEOREM: : $(p-1)! = -1$ mod p, p prime.

FERMAT'S 4n+1 THEOREM: :

THEOREM: : If p is prime and p=4n+1, n∈Z

then

- $x^2 = -1 \text{mod p}$
- p=$a^2 + b^2$

  ****

  Lemma: Ideal U is a subring of R

  Lemma: The intersection of a finite number of ideals is an ideal.

  Lemma: $R[x]$ is a ring.

  Lemma: A subring of an integral domain is an integral domain.

  Lemma: The GAUSSIAN INTEGERS $\mathbb{Z}[i]$ form an integral domain.

- The Gaussian primes are $\{x + iy : x^2 + y^2 = prime \in \mathbb{Z}\}$ and $p + i0 : p isaprimeoftheform 4n + 3$.

  Lemma: If $\phi : R \longrightarrow \overline{R}$

  is an isomorphism onto $\overline{R}$

  then so is $(\phi)^{-1}$

  Theorem: A field has only two ideals.

  Converse: If R is a commutative ring with 1

  whose only two ideals are $\{0\}$ and R

  then R is a field

Theorem: If R is a commutative ring with 1

then

R is a field

$\iff$

R has only two ideals

Examples:

1. $\{0, 1\}$ is a field.
2. $\mathbb{Z}$ is not a field.

Definition:

An IDEAL M of ring R
is MAXIMAL
if M⊆U⊆R $\Longrightarrow$ M=U or U=R

Lemma: In $\mathbb{Z}$

ideal $< n >$ is maximal

$\iff$

n is prime.

Lemma: If R is a ring and U an ideal

then

Homomorphism $\phi : R \longrightarrow \dfrac{R}{U}$

is order-preserving.

i.e. If R has two ideals J⊂K

then

$\phi(J) \subset \phi(K)$

- $\ker(\phi) = U \subset$J

Theorem: If R is a commutative ring with 1

and M an ideal of R

then

M is a maximal ideal

$\Longleftrightarrow$

$\frac{R}{M}$ is a field.

$\phi(J) \subset \phi(K)$

Examples:

1. $$\frac{Z}{< 3 >} \text{ is a field.}$$
2. $$\frac{\mathbb{Z}}{< 6 >} \text{ is a not a field.}$$

Lemma: The homomorphic images of a field

are $\{0\}$ and F itself

EMBEDDING of a ring R in an integral domain

Z can be embedded in the field of quotients Q

Theorem: Every integral domain

can be embedded in a FIELD

Theorem: If R is a Euclidean ring and A an ideal of R

Then $A = \{ax : x \in R\}$

Definition: A PRINCIPAL ideal U of integral domain R with unit element 1

is a subset U of R such that $U =< a >= Ra$

Definition: A PRINCIPAL ideal domain or p.i.d. is an integral domain R with unit element 1

in which every ideal is principal

Theorem: A Euclidean ring has the unit element 1

Theorem: A Euclidean ring is a principal ideal ring.

The converse is false.

ER$\subseteq$p.i.d. $\subseteq$UFD

3 NUMBER THEORY

In a ring R, a divides b denoted by a/b

if $\exists c \in R$ s.t. $ac = b$.

g.c.d. of $a,\ b$ (denoted by a/b) is d if

i d/a and d/b

ii $\forall c \in R\ c/a$ and $c/b \implies c/d$

Now R is a ring with 1.

DEFINITIONS:

u is a UNIT iff $\exists v \in R$ s.t. $uv = vu = 1$

a, b are ASSOCIATES iff $\exists$a unit $u \in R$ s.t. $a = ub$

π is IRREDUCIBLE in R iff $\pi \neq 0,\ \pi \not a$ unit and $\pi = ab \implies a$ or b is a unit

p is PRIME in R iff $p \neq 0,\ p \not a$ unit and $p/ab \implies p/a$ or p/b

In fields each element is a unit. So Primes and irreducibles are not defined.

l.c.m. of $a,\ b$ is l if

i a/l and b/l

ii $\forall c \in R$ a/c and $b/c \implies l/c$

$d \in \mathbb{Z}$ is SQUARE FREE if

$d \neq 1$ and $x^2/d,\ x \in \mathbb{Z} \Longrightarrow x = 1$

$(\mathbb{Z}[\sqrt{d}], +, .)$ where d is SQUARE FREE

is an integral domain.

$\text{Norm}(a + b\sqrt{d}) = N(\alpha) = |a^2 - db^2|$

$N(\alpha) = |a^2 - db^2| \in \mathbb{Z}$

$N(\alpha) = 0 \Longleftrightarrow \alpha = 0$

$N(\alpha\beta) = N(\alpha)N(\beta)$

$N(\alpha) \leq N(\alpha\beta)$

u is a unit in $(\mathbb{Z}[\sqrt{d}], +, .)$

$\Longrightarrow N(u) = 1$

EUCLIDEAN ALGORITHM

To find g.c.d. of $a,\ b$

$b = aq_0 + r_1$ where $d(r_1) < d(a)$

$a = r_1 q_1 + r_2$ where $d(r_2) < d(r_1)$

$\vdots$

$r_{n-1} = r_n q_n$

then $(a, b) = r_n$

THEOREM: In a EUCLIDEAN Ring

π irreducible $\Longrightarrow \pi$ prime.

THEOREM: In a UFD

π irreducible $\Longleftrightarrow \pi$ prime.

Lemma: In a EUCLIDEAN Ring

$d(a) < d(ab)$ if b is not a unit.

Definition: A UNIQUE FACTORIZATION domain or UFD is an integral domain with unit element 1

in which every element a which is not zero or a unit

is a unique product of a finite number of irreducible elements. (up to associates)

THEOREM: pid $\Longrightarrow$ UFD.

Lemma: In a EUCLIDEAN Ring R

$d =$ g.c.d(a,b) $\Longrightarrow d = \lambda a + \mu b$

Lemma: In an integral domain with unit element 1

a/b and $b/a \implies a = ub$ where u is a unit.

Lemma: In a commutative ring with unit element 1

the relation a is an associate of b is an equivalence relation.

Equivalence class $[a]$ is the set of associates of a.

Lemma: NORM(1) is MINIMUM norm.

Norm(u)=Norm(1) for all units.

Norm(a)=Norm(ab) $\iff$ b is a unit

Norm(a)<Norm(ab) $\iff$ b is NOT a unit

Lemma: A unit generates R

Lemma: In a EUCLIDEAN Ring R

an element is either a unit or can be written as the product of a finite number of PRIMES

Proof by induction on Norm(a)

Lemma: x = g.c.d. of a,b

and x = associate of y $\iff$ both x and y are g.c.d.'s

Definition: a, b are RELATIVELY PRIME if (a,b)=u.

a, b are RELATIVELY PRIME $\iff$ (a,b)=1

UNIQUE FACTORIZATION THEOREM

THEOREM: : In a EUCLIDEAN Ring R

Every element is a unit or else

can be expressed UNIQUELY as THE FINITE PRODUCT OF Primes (up to ASSOCIATES)

Lemma: In a EUCLIDEAN Ring R

IDEAL Ra is MAXIMAL $\Longrightarrow$ a is PRIME.

Lemma: In$\mathbb{Z}$, p prime, (c,p)=1,

and $x^2 + y^2 = cp \Longrightarrow \exists$ a, b∈Z such that $a^2 + b^2 = p$

$3^2 + 7^2 = 2 \times 29 \Longrightarrow 1^2 + 1^2 = 2$ and $2^2 + 5^2 = 29$

BECAUSE $p = a^2 + b^2 = (a + bi)(a - bi)$ is not irreducible in $\mathbb{Z}[i]$

FERMAT'S LITTLE THEOREM: :

THEOREM: : $a^p = a \bmod p$, $a \in$Z, p prime.

WILSON'S THEOREM: :

THEOREM: : $(p - 1)! = -1 \bmod p$, p prime.

FERMAT'S 4n+1 THEOREM: :

THEOREM: : If p is prime and p=4n+1, n∈Z

then

$x^2 = -1$mod p

p=$a^2 + b^2$

****

Lemma: Ideal U is a subring of R

Lemma: The intersection of a finite number of ideals is an ideal.

Lemma: $R[x]$ is a ring.

Lemma: A subring of an integral domain is an integral domain.

Lemma: The GAUSSIAN INTEGERS $\mathbb{Z}[i]$ form an integral domain.

The Gaussian primes are $\{x + iy : x^2 + y^2 = prime \in \mathbb{Z}\}$ and $p + i0 : pisaprimeoftheform4n + 3$.

Lemma: If $\phi : R \longrightarrow \overline{R}$

is an isomorphism onto $\overline{R}$

then so is $(\phi)^{-1}$

Theorem: A field has only two ideals.

Converse: If R is a commutative ring with 1

whose only two ideals are $\{0\}$ and R

then R is a field

Theorem: If R is a commutative ring with 1

then

R is a field

$\Longleftrightarrow$

R has only two ideals

Examples:

1. $\{0,1\}$ is a field.
2. $\mathbb{Z}$ is not a field.

Definition:

An IDEAL M of ring R

is MAXIMAL

if M⊆U⊆R $\Longrightarrow$ M=U or U=R

Lemma: In$\mathbb{Z}$

ideal $< n >$ is maximal

$\Longleftrightarrow$

n is prime.

Lemma: If R is a ring and U an ideal

then

Homomorphism $\phi : R \longrightarrow \frac{R}{U}$

is order-preserving.

i.e. If R has two ideals J$\subset$K

then

$\phi(J) \subset \phi(K)$

$\ker(\phi) = U \subset$J

Theorem: If R is a commutative ring with 1

and M an ideal of R

then

M is a maximal ideal

$\Longleftrightarrow$

$\frac{R}{M}$ is a field.

$\phi(J) \subset \phi(K)$

Examples:

1. $$\frac{\mathbb{Z}}{< 3 >} \text{ is a field.}$$

2. $$\frac{\mathbb{Z}}{< 6 >} \text{ is a not a field.}$$

Lemma: The homomorphic images of a field

are $\{0\}$ and F itself

EMBEDDING of a ring R in an integral domain

Z can be embedded in the field of quotients Q

Theorem: Every integral domain

can be embedded in a FIELD