**Abstract Algebra 2**

**References:**

* Introduction to Modern Abstract Algebra, by David M. Burton.
* Contemporary abstract algebra, by Gallian and Joseph.
* Groups and Numbers, by R. M. Luther.
* A First Course in Abstract Algebra, by J. B. Fraleigh.
* Group Theory, by M. Suzuki.
* Abstract Algebra Theory and Applications, by Thomas W. Judson.
* Abstract Algebra, by I. N. Herstein.
* Basic Abstract Algebra, by P. B. Bhattacharya, S. K. Jain and S. R. Nagpaul.
1. **Definition and Examples of Rings**

**Definition(1-1):**

A ring is an ordered triple consisting of a non-empty set and two binary operations and on such that

1. is a commutative group,
2. is a semigroup (satisfies the axioms i , ii of group),
3. The two operations are related by the distributive laws

,

.

**Definition(1-2):**

A commutative ring is a ring in which is a commutative.

**Examples(1-3):**

1. Each one of the following is a commutative ring:

.

1. The set is a commutative ring with identity.

 ,

 .

1. Let denote the set of all functions . The sum and product of two functions are defined as usual, by the equations

,

.

 The triple is a commutative ring with identity.

1. The triple is not a ring.

The left distributive law .

1. Let be an arbitrary commutative group and Hom be the set of all homomorphisms from into itself. (Hom is a semigroup with identity, then the triple (Hom forms a ring with identity.

(Hom is a commutative group.

,

So that .

.

Therefore,.

1. The triple is a commutative ring with identity.
2. Consider the set of ordered pairs of real numbers. We define addition and multiplication in by the formulas

.

 is a commutative ring with identity.

1. The triple is a commutative ring with identity.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Here, we have , the product of nonzero elements being zero. Note also that , yet it is clearly not true that . The multiplicative semigroup does not satisfy the cancellation law.

1. The triple is a commutative ring with identity.
2. The triple is a ring with identity, but not commutative.
3. The triple is not ring, since the sum of two odds equal into even number.
4. **Basic Properties of Rings**

**Theorem(2-1):** If be a ring, then

1. ,
2.

**Proof:** (1)

Substitute in , we get

.

**Proof:** (2) Substitute in and by using , we have

.

**Proof:** (3) Substitute in , we get

**Corollary(2-2):** If be a ring with identity and , then ,

**Proof:** since , suppose that

, but by assumption, thus

To prove

**Corollary(2-3):** If be a ring, if has an identity element, then it is a unique.

**Proof:** let are two identity elements of , then

**Corollary(2-4):** If are two inverses of in a ring with identity, then

**Proof:**

**Theorem(2-5):** If be a ring with identity and be a set of units of , then is a group.

**Proof:** , since

Let

This means

Since is associative, then is associative (since )

Therefore, is a group.

1. **Subrings, Examples and Properties**

**Definition(3-1):** Let be a ringand be a nonempty subset of . If the triple is itself a ring, then is said to be a subring of .

**Theorem(3-2):** Let be a ringand . Then the triple is a subring of if and only if

1. (closed under differences),
2. (closed under multiplication).

**Proof:** let be a subring of is a subgroup of

Since is a subring of .

 let is a subgroup of

Since the operation of addition is a commutative on ,

 the operation of addition is a commutative on

 is an abelian subgroup of

Also, similarly the associative and distributed the multiplication on addition are true on since.

 is a subring of .

**Examples(3-3):**

1. Every ring has two trivial subrings; for, if denotes the zero element of the ring , then both and are subrings of .
2. In the ring of integers , the triple is a subring, while is not.
3. Consider the ring of integers modulo. If , then , whose operation tables are given at the below, is a subring of .

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. Let . Then is a subring of , since for , we get

,

.

1. The triple is a subring of .
2. Let the set, then the triple is a subring of .
3. is a subring of .
4. is a subring of .
5. Let be a ring and , then is a subring of .
6. is a subring of . We note that , but .
7. Give example to ring with identity and subring with different identity.

Take and

The identity of is

The identity of is

1. **Characteristic of the Ring and Related Concepts**

**Definition(4-1):** Let be an arbitrary ring. If there exists a positive integer such that for all, then the least positive integer with this property is called the characteristic of the ring. If no such positive integer exists (that is, for all implies ), then we say has characteristic zero.

**Example(4-2):** the rings of integers, rational numbers and real numbers are standard examples of characteristic zero.

**Example(4-3):** the ring is of characteristic two.

Since

 for every subset of .

**Theorem(4-4):** Let be a ring with identity. Then has characteristic if and only if is the least positive integer for which .

**Proof:** if the ring is of characteristic , it follows trivially that . If, where , then

For every element . This would mean the characteristic of is less than , an obvious contradiction. The converse is established in much the same way.

**Example(4-5):** the characteristic of the ring is zero.

**Example(4-6):** the characteristic of the ring is .

**Example(4-7):** the characteristic of the ring is .

1. **Ideals and their Properties**

**Definition(5-1):** A subring of the ring is an ideal of if and only if and imply both and .

**Definition(5-2):** Let be a ring and a nonempty subset of . Then is an ideal of if and only if

1. imply ,
2. and imply both and .

**Example(5-3):** In any ring , the trivial subrings and are both ideals.

**Remark(5-4):** A ring which contains no ideals except these two is said to be simple. Any ideal different from is a proper.

**Example(5-5):** The subring is an ideal of , the ring of integers modulo.

**Example(5-6):** For a fixed integer , let denote the set of all integral multiples of, that is,

The following relations show the triple to be an ideal of the ring of integers :

,

, .

**Example(5-7):** , the ring of even integers is an ideal of .

**Example(5-8):** Suppose is the commutative ring of functions . The sum and product of two functions are defined as usual, by the equations

,

.

Define

.

For functions and , we have

And also

.

Since both and belong to , is an ideal of .

**Example(5-9):** Let be a ring, then is a left ideal of , but it is not right ideal of .

Let and

Therefore, is a left ideal of

 is not right ideal of , since

 and

But

**Example(5-10):** Let be the set of all functions on , then is an ideal of .

**Example(5-11):** the triple is an ideal of .

**Theorem(5-12):** If is a proper ideal of a ring with identity, then no element of has a multiplicative inverse; that is, .

**Proof:** suppose exists

 (since is closed under multiplication)

Thus, , but this is contradiction. ( a proper).

**Theorem(5-13):** If is an arbitrary indexed collection of ideals of the ring , then so also is .

**Proof:**

Let and and

 and

Therefore, is an ideal of .

**Note(5-14):** Consider be a ring and. Define the set

.

, since

**Theorem(5-15):** The triple is an ideal of the ring , known as the ideal generated by the set .

**Theorem(5-16):** If is a commutative ring with identity and , then the principle ideal generated by is such that .

**Theorem(5-17):** If is an ideal of the ring , then for some nonnegative integer .

**Proof:** If , the theorem is trivially true, for the zero ideal is the principal ideal generated by .

Let , suppose the least positive integer in

Thus, , any integer where

Since

Thus every member of is a multiple of .

**Theorem(5-18):** Let be nonzero element of a principal ideal ring . Then , where is a least common multiple of .

**Proof:**  is an ideal of .

But every ideal of is a principle ideal;

Since for some .

So, is a common multiple of .

Let any common multiple of , say

If , then

Therefore, and must be a multiple of , thus is a least common multiple of .

**Example(5-19):** Consider the principal ideal and generated by the integers and in the ring .Then , where is the least common multiple of and.

1. **Quotient Ring and Related Concepts.**

**Notes(6-1):** Let is an ideal of the ring , then

1. ,
2. ,
3. .

**Theorem(6-2):** If is an ideal of the ring , then is a ring, known as the quotient ring of by .

The zero element of is the cose, while .

**Example(6-3):** In the ring of integers, consider the principal ideal , where is a nonnegative integer. The coset of in take the form

**Example(6-4):** The triple is an ideal of the ring , then

is a ring with an identity.

**Example(6-5):** Let be a ring and is an ideal of the ring , then is a commutative ring with identity.

1. **Homomorphisms of Ring. Examples and Properties**

**Definition(7-1):** Let and be two rings and a function from into ; in symbols, . Then is said to be a ring homomorphism from into if and only if

for every pair of elements .

**Example(7-2):** Let and be arbitrary rings and be the function that maps each element of onto the zero element of .

,

.

As with the case of groups, this mapping is called the trivial homomorphism.

**Example(7-3):** The mapping defined by is not a homomorphism from into ,

but

**Example(7-4):** Consider , the ring of integers, and , the ring of integers modulo . Define by taking ; that is, map each integer into the congruence class containing it. Then

,

,

so that is a homomorphism mapping.

**Example(7-5):** Let be any ring with identity. For each invertible element , the function given by

is a homomorphism from into itself. Indeed, if , we see that

,

,

**Theorem(7-6):** Let be a homomorphism from the ring into the ring . Then the following hold:

1. , where is the zero element of .
2. for all .
3. The triple is a subring of .
4. .
5. for each invertible element .

**Proof:**

**Proof:**

**Theorem(7-7):** If is a homomorphism from the ring into the ring , then the triple ker is an ideal of .

**Proof:**

, since

Let

If .

Thus,ker is an ideal of .

**Example(7-8):** Consider an arbitrary ring with identity element and the mapping given by . Then is a homomorphism from the ring of integers into the ring :

,

.

**Theorem(7-9):** That for some nonnegative integer .

**Definition(7-10):** A ring is embedded in a ring if there exists some subring of such that .

**Theorem(7-11):** Any ring can be embedded in a ring with identity.

**Proof:** Let be an arbitrary ring and

Define

,

,

The triple forms a ring. This ring has multiplicative identity, namely the pair ; for

,

.

Next, consider the subset of consisting of all pairs of the form . Since

Therefore, is a subring of .

The proof is completed by showing is isomorphic to the given ring . To this end, define the function by taking

.

The function is a one-to-one mapping of onto the set .

,

.

Thus, .

1. **Fundamental Theorems of Homomorphisms of Rings.**

**Theorem(8-1):** (The first fundamental theorem of homomorphism of ring)

**Proof:** let defined by

To prove that is well define

To prove that is a homomorphism

Also

To prove is an onto

If

To prove is an one-to-one

**Example(8-2):** Let be a function defined by .

The operation tables for the quotient ring are as shown:

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

Therefore,

**Theorem(8-3):** (The second fundamental theorem of homomorphism of ring)

Let be a ring, be an ideal of and be a subring of, then

**Proof:** let

, since

, since

, since

, since

Let defined by

To prove that is a homomorphism

Also

To prove that is an onto

By the first theorem, we get

Therefore, .

**Theorem(8-4):** Let be a ring with identity and be a homomorphism from into , then

1. is an identity of .
2. is an inverse in .

**Proof:** (1) if

Thus, is an identity element of

**Proof:** (2)

Hence, is an inverse of in .

**Theorem(8-5):** (The third fundamental theorem of homomorphism of ring)

If be two ideals in with , then

1. is ideal in.
2. .

**Proof:** (1)

**Proof:** (2) let defined by

To show that is a homomorphism

 Also

 To prove

Let

Let

Hence, .

1. **Properties of Ideals and Quotient Ring by Using Homomorphisms.**

**Theorem(9-1):** Let be two ideals in a ring , then is an ideal in a ring .

**Proof:**

Therefore, is an ideal in a ring .

**Theorem(9-2):** Let be two ideals in a ring , then is an ideal in a ring .

**Proof:**

Hence, is an ideal in a ring .

**Theorem(9-3):** Let be two ideals in a ring , then is an ideal in a ring .

**Proof:**

Thus, is an ideal in a ring .

**Theorem(9-4):** Let be two ideals in a ring , then is an ideal in a ring .

**Proof:**

Hence, is an ideal in a ring .

**Theorem(9-5):** Let be a commutative ring, then is an ideal in contains .

**Proof:**

To show

**Example(9-6):** Let be ideals in a ring with , then

**Solution:** let

Also

Let

1. **Zero Divisors Elements and Integral Domains.**

**Definition(10-1):** A ring is said to have divisors of zero if there exist nonzero elements such that the product .

**Theorem(10-2):** A ring is without divisors of zero if and only if the cancellation law holds for multiplication.

**Proof:** Assume contains no divisors of zero.

let , then

Since has no zero divisors, or

 suppose that the cancellation law holds and

If , then .

This shows is free of divisors of zero.

**Corollary(10-3):** Let be a ring with identity which has no zero divisors. Then the only solutions of the equation are and .

**Proof:** if , with , then .

**Definition(10-4):** An integral domain is a commutative ring with identity which does not have divisors of zero.

**Corollary(10-5):** In an integral domain, all the nonzero elements have the same additive order, which is the characteristic of the domain.

**Proof:** suppose the integral domain has positive characteristic .

Any will then possess a finite additive order, with .

But , since is free of zero divisors.

**Corollary(10-6):** The characteristic of an integral domain is either zero or a prime number.

**Proof:** let be of positive characteristic and assume that is not a prime.

 with .

.

 Since is without zero divisors, either or .

 But this is contradiction, the least positive integer such that .

 Hence, we are led to conclude that the characteristic must be prime.

**Example(10-7):** Let be a ring. Then is a right zero divisor and is a left zero divisor in .

**Solution:**

**Example(10-8):** The number is a zero divisor in a ring and the numbers are zero divisors in a ring . (**check**)

**Example(10-9):** Let be a commutative ring with identity and define

The identity element with is , and the identity with is .

Also, is a zero divisor, since

.

**Example(10-10):** The triple is an integral domain, since is a commutative with identity .

 or .

**Example(10-11):** Let be a ring, where is a prime number, then is an integral domain.

**Solution:** the tripleis a commutative with identity .

To show has no zero divisors.

Let

But is a prime number, or or .

**Example(10-12):** is not an integral domain, since it is not commutative ring.

**Example(10-13):** Solve the equation in a ring .

**Solution:**

But, in , we have

Since

So,

Hence, is a set of solution of in .

**Example(10-14):** Let is an integral domain with and . Show that .

**Solution:** If .

Let

Since, is an integral domain and

By , we get

**Corollary(10-15):** Let be a ring with identity and is an invertible, then is not zero divisor.

**Proof:** let

Also,

.

1. **Fields and their properties**

**Definition(11-1):** A ring is said to be a field provided the pair forms a commutative group.

**Example(11-2):** Both and are fields. (**check**)

**Example(11-3):** The triple is a field.

**Example(11-4):** The triple , is a field. Where

,

.

The pair is the multiplicative identity and is the zero element of the ring.

Now, suppose , either or , so that ; thus

**Example(11-5):** The field contains a subring which is isomorphic to the ring of real numbers.

It follows that via the mapping defined by

 (**check**)

**Example(11-6):** The triple is a field.

Let

 is a multiplicative inverse of .

**Example(11-7):** The triple is a field. (**check**)

**Corollary(11-8):** In a field , with , then there exist a unique element satisfies .

**Proof:** is an abelian group, then

**Example(11-9):** The triple is a field, where are defined by

 (**check**)

**Theorem(11-10):** If is a field and with , then either or .

**Proof:** if , the theorem is already established.

Suppose that and prove that .

.

1. **More Results of Fields and Integral Domains.**

**Theorem(12-1):** Any finite integral domain is a field.

**Proof:** suppose and

are all distinct, for if , then by the cancellation law. So each element of is of the form . In particular, ; since multiplication is commutative, we have . This shows that every nonzero element of is invertible, so is a field.

**Example(12-2):** Prove or disprove, every integral domain is a field.(**check**)

**Example(12-3):** Prove or disprove, every ring is a field.(**check**)

**Example(12-4):** Prove or disprove, every ring is an integral domain.(**check**)

**Theorem(12-5):** The ring of integers modulo is a field if and only if is a prime number.

**Proof:** We first show that if is not prime, then is not a field.

Thus assume , where and .

,

Both . This means that is not an integral domain, and hence not a field.

Suppose that is a prime number. To show that is a field.

Let , where .

,

Showing the congruence class to be the multiplicative inverse of .

Therefore, is a field.

**Theorem(12-6):** Let be a commutative ring with identity. Then is a field if and only if has no nontrivial ideals.

**Proof:** Assume first that is a field. We wish to show that the trivial ideals and are its only ideals.

Let be nontrivial ideal of and

, since is a field

But, this is contradiction.

 suppose that has no nontrivial ideals.

Let , consider the principal ideal generated by:

Now cannot be the zero ideal, since , with .

If : that is, , since

Hence each nonzero element of has a multiplicative inverse in.

**Theorem(12-7):** Let be a homomorphism from the field onto the field . Then either is the trivial homomorphism or else and are isomorphic.

**Proof:** since is an ideal of , either or .

If is a one-to-one, in which case via .

If , then each element of must map onto zero; that is, is the trivial homomorphism.

**Definition(12-8):** By a subfield of the field is meant any subring of which is itself a field.

**Example(12-9):** The ring is a subfield of the field .

**Theorem(12-10):** The triple is a subfield of if and only if the following hold:

1. is a nonempty subset of with at least one nonzero element.
2. implies .
3. , where , implies .

**Theorem(12-11):** Let the integral domain be a subring of the field . If the set is defined by

,

then the triple forms a subfield of such that . In fact, is the smallest subfield containing .

**Proof:** if with

Since

Let , we have

If ,

**Note(12-12):** Let be an integral domain and the set of ordered pairs,

.

**Theorem(12-13):** The relation is an equivalence relation in .(**check** 1,2)

That is to say

1. ,
2. If , then ,
3. If and , then .

The least obvious statement is (3). In this case, the hypothesis and implies that

.

Multiplying the first of these equations by and the second by , we obtain

,

and, from the commutativity of multiplication, . Since , this factor may be cancelled to yield . But then .

**Note(12-14):** We label those elements which are equivalent to the pair by the symbol ; in other words,

.

,

.

let and . From the equations

it follows that

Thus, by the definition of equality of classes,

,

Proving addition to be well-defined. In much the same way, one can show that

.

**Lemma(12-15):** The triple is a field, generally known as the field of quotients of the integral domain.

**Proof:** the multiplicative identity , where is any nonzero element is

with in .

 as the zero element while is the negative of .

To show has an inverse under multiplication.

.

Since , is the identity element, so that .

**Theorem(12-16):** The integral domain can be embedded in its field of quotients .

**Proof:** Consider the subset of consisting of all element of the form ,

Where is the multiplicative identity of :

Let be the onto mapping defined by

Since implies or , we see that is a one-to-one function.

,

.

Therefore, .

**Note(12-17):** Any member of can be written in the form

.

**Note(12-18):** It should also be observed that for any , we have

.

**Note(12-19):** The field of quotients constructed from the integral domain is, of course, the rational number field .

**Definition(12-20):** A field which does not have any proper subfields is called a prime field.

**Example(12-21):** The field of rational numbers, , is a prime field.

To see this, suppose is a subfield of and let .

Since is a subfield, it must contain the product .

: in other words, contains all the integers. It follows then that every rational number , also belongs to , so that .

**Example(12-22):** For every prime , the field of integers modulo is a prime field. The reasoning here depends on the fact that the additive group of is a finite group of prime order, and therefore has no nontrivial subgroups.

**Theorem(12-23):** Any prime field is isomorphic either to , the field of rational numbers, or to one of the fields , where is a prime number.

**Proof:** let be the identity element of and define the mapping by

Then is a homomorphism from onto the subring consisting of integral multiples of , we see that

.

But the triple is an ideal of a principal ideal ring, for some nonnegative integer . if , then must in fact be a prime. Suppose where . Since ,

,

yielding the contradiction that the field has divisors of zero.

Therefore, is the characteristic of and as such must be prime. So

1. for some prime , or
2. .

Suppose first that the subring must itself be a field. But contains no proper subfield. and .

Next, , the subring is an integral domain, but not a field. The hypothesis is a prime field, then implies

.

The fields and are isomorphic under the mapping .

**Corollary(12-24):** Every field contains a subfield which isomorphic either to the field or to one of the fields , a prime.

1. **Maximal Ideals. Example, Properties and Results.**

**Definition(13-1):** An ideal of the ring is a maximal ideal provided and whenever is an ideal of with , then .

**Theorem(13-2):** Let be the ring of integers and . Then the principal ideal is maximal if and only if is a prime number.

**Proof:**  suppose is a maximal ideal of . If the integer is not prime, then, where . This implies the ideals and are such that

contrary to the maximality of

 assume that is prime.

If the ideal is not maximal in , then either or else there exists some proper ideal with . The first case is immediately ruled out by the fact that is not a multiple of a prime number.

The alternative possibility means for some integer ; this also is untenable, since is prime, not composite. We therefore conclude that is a maximal ideal.

**Example(13-3):** Let denote the collection of all functions . For two such functions and , we have

.

Then is a commutative ring with identity. Consider

.

The triple forms an ideal of ; we observe that it is a maximal ideal.

**Zorns Lemma(13-4):** Let be a nonempty family of subsets of some fixed set with the property that for each chain in , the union also belongs to . Then contains a set which is maximal in the sense that it is not properly contained in any member of.

**Theorem(13-5):** (Krull-Zorn). In a commutative ring with identity, each proper ideal is contained in a maximal ideal.

**Proof:** let be any proper ideal of . Define

is a proper ideal of.

, since . Let a chain in . Notice that , since for any .

Let and for which

The collection forms a chain, either or else ; say, for definiteness, . But is an ideal, so . For the same reason , . This shows the triple to be a proper ideal of the ring . , hence .

Thus, on the basis of Zorns Lemma, contains a maximal element . The triple is a proper ideal of the ring with. is a maximal ideal. To see this, suppose is any ideal of for which . Since is a maximal element of , the set , the ideal must be improper, which implies . We therefore conclude is a maximal ideal of .

**Corollary(13-6):** An element is invertible if and only if it belongs to no maximal ideal.

**Theorem(13-7):** In a ring having exactly one maximal ideal , the only idempotent elements are and .

**Proof:** assume the theorem is false; that is, suppose there exists an idempotent with . The relation implies , so that and are zero divisors. Hence, neither the element nor is invertible in . But this means the principle ideals and are both proper ideals of the ring . As such, they must be contained in : and , both and lie in ,

This leads at once to the contradiction .

**Theorem(13-8):** Let be a proper ideal of the ring . Then is a maximal ideal if and only if the quotient ring is a field.

**Proof:** let be a maximal ideal of . Since is a commutative ring with identity, the quotient ring also has these properties. If , then . The ideal generated by and must be the whole ring :

.

The identity element ,

,

. Hence is a field.

 suppose is a field and is any ideal of such that . Since is a proper subset of , there exists an element with . The coset . is a field,

for some coset . . But .

**Example(13-9):** Consider the ring of even integers , a commutative ring without identity. In this ring, the principle ideal generated by the integer is a maximal ideal.

**Solution:** if is any element not in , then is an even integer not divisible by ; the greatest common divisor of and must be . We have

,

This reasoning shows that there is no ideal of contained between and .

Now note that in ,

.

The ring therefore has divisors of zero and cannot be a field.

1. **Prime Ideals. Examples, Properties and Results.**

**Definition(14-1):** Anideal of the ring is a prime ideal if for all implies either or .

**Example(14-2):** The prime ideals of the ring are precisely the ideals , where is a prime number, together with the trivial ideals and .

**Example(14-3):** A commutative ring with identity is an integral domain if and only if the zero ideal is a prime ideal.

**Theorem(14-4):** Let be a proper ideal of the ring . Then is a prime ideal if and only if the quotient ring is an integral domain.

**Proof:** take is a prime ideal. Since is a commutative ring with identity, so is the quotient ring . Assume that

. Since is a prime ideal, or . But this means either or , hence is without zero divisors.

 suppose is an integral domain and .

.

By hypothesis, contains no divisors of zero, so that either or . So or , therefore is a prime ideal.

**Theorem(14-5):** In a commutative ring with identity, every maximal ideal is a prime ideal.

**Proof:** Assume is a maximal ideal of the ring and that with . is a maximal implies that . Hence there exist elements for which

.

Since both and are in , we conclude

,

from which it is clear that is a prime ideal.

**Example(14-6):** The ring , where forms a maximal ideal which is not prime.

**Theorem(14-7):** Let be a principal ideal domain. A (nontrivial) ideal of is prime if and only if it is a maximal ideal.

**Proof:** suppose is any ideal with . Since is a principal ideal ring, there exists for which . Now , hence . But is a prime ideal, so either or . leads to the contradiction . Therefore , which implies , or . Since and is an integral domain, we have . This means , or . Since no ideal lies between and , we conclude that is a maximal ideal.

 from theorem (14-5).

**Corollary(14-8):** A nontrivial ideal of the ring is prime if and only if it is maximal.

**Definition(14-9):** A nonzero element of the ring is called a prime element of if is not invertible and in every factorization with , either or is invertible.

**Theorem(14-10):** Let be a principal ideal domain. The ideal is a prime (maximal) ideal of if and only if is a prime element of .

**Proof:** suppose is a prime element of and is any ideal for which . By hypothesis, is a principal ideal ring, so there is with . As for some . Since is a prime element that either or is invertible. , which implies , an obvious contradiction. The element must be invertible, so that . This argument shows that is a maximal ideal of and prime.

 Let be a prime ideal of . Assume that is not a prime element of . Then where , and neither nor is invertible. Now if , and . From the cancellation law, . But this contradiction that is invertible. By the same reasoning, if lies in , then , with , is a prime ideal. Hence our supposition is false and must be a prime element of .

**Definition(14-11):** The radical of a ring , denoted by rad , is the set

rad is a maximal ideal of.

If rad , then we say is a ring without radical or is a semisimple ring.

**Example(14-12):** The ring of integers is a semisimple ring.

**Solution:** the maximal ideals of are the principal ideals , where is a prime; that is,

rad a prime number.

Since no nonzero integer is divisible by every prime, rad .

**Theorem(14-13):** Let be an ideal of the ring. Then the set if and only if each element of the coset has an inverse in .

**Proof:** assume that and that there is , for which is not invertible. The element must belong to some maximal ideal of the ring . Since , , and therefore . But this means , which is clearly impssible.

 suppose each element of the coset has an inverse in , but . There exist a maximal ideal of with . If , .

Let , , so that possesses an inverse. The conclusion is untenable, since no proper ideal contains an invertible element.

**Theorem(14-14):** In any ring an element if and only if has an inverse for each .

**Corollary(14-15):** An element is invertible in the ring if and only if the coset is invertible in the quotient ring .

**Proof:** assume the coset has an inverse in , so that

for some . Then . With , to conclude that is invertible: this means has an inverse.

 (**check**)

**Corollary(14-16):** The only idempotent in the radical of the ring is .

**Proof:** let with . Taking in the preceding theorem, we see that has an inverse in ; say

**Corollary(14-17):** Let denote the set of all noninvertible elements of . Then the triple is an ideal of the ring if and only if .

**Proof:**  clearly holds. Suppose . is an ideal of the ring , then . , for otherwise

So must be invertible, . This shows , then .

 is clear.

**Theorem(14-18):** For any ring , the quotient ring is semisimple.

**Proof:** suppose

is invertible in for each . There exists a coset , such that

has an inverse . But

so that is invertible in . .

1. **Polynomials Rings. Examples and Basic Properties.**

**Definition(15-1):** For an arbitrary ring . The set of polynomials over may be regarded as the set

poly

 and

.

,

Where

**Theorem(15-2):** The triple forms a ring, known as the ring of polynomials over . Furthermore, the ring is commutative with identity if and only if is a commutative ring with identity.

**Definition(15-3):** If is a nonzero polynomial in (the set of ), we call the coefficient the leading coefficient of and the integer , the degree of the polynomial.

**Theorem(15-4):** Let be an integral domain and be two nonzero elements of . Then

1. deg degdeg, and
2. either or deg degdeg.

**Example(15-5):** Consider . Taking

we then have , so that

deg .

**Theorem(15-6):** (Division Algorithm). Let be a commutative ring with identity and be polynomials in, with the leading coefficient of an invertible element. Then there exist unique polynomials such that

,

where either or deg deg .

**Theorem(15-7):** (Remainder Theorem). Let be a commutative ring with identity. If and , then there is a unique polynomial in such that .

**Proof:** Applying the division algorithm to and , we obtain

,

where or deg deg . It follows in either case that is a constant polynomial . Substituting for , we have

.

**Corollary(15-8):** (Factorization Theorem). The polynomial is divisible by if and only if is a root of .

**Proof:** since if and only if .

**Theorem(15-9):** Let be an integral domain and be a nonzero polynomial of degree . Then has at most distinct roots in .

**Proof:** when deg, the result is trivial, since cannot have any roots. If deg, say , then has at most one root; indeed, if is invertible, is only root of . Now, suppose the theorem is true for all polynomials of degree , and let deg . If has a root , then

,

where the polynomial has degree . Any root of distinct from must be a root of , for, by substitution

and, since has no zero divisors, . has at most distinct roots. As the only roots of are and those of cannot have more than distinct roots in .

**Corollary(15-10):** Let and be nonzero polynomials of degree over the integral domain . If there exist distinct elements for which, then .

**Proof:** the polynomial is such that deg and has at least distinct roots in . This is impossible unless , or .

**Example(15-11):** Consider the polynomial , where is a prime number. Since the nonzero elements of form a cyclic group, under multiplication, of order , we must have or for every. But the last equation clearly holds when , so that every element of is a root of the polynomial .

**Theorem(15-12):** Let be the field of complex numbers. If is a polynomial of positive degree, then has at least one root in .

**Corollary(15-13):** If is a polynomial of degree , then can be expressed in as a product of (not necessarily distinct) linear factors.

**Theorem(15-14):** If is a field, then the ring is a principal ideal domain.

**Proof:** is an integral domain. To see that any ideal of is principal. If , the result is trivially true, since. Otherwise, there is some nonzero polynomial of lowest degree in . For each polynomial , we may use the Division Algorithm to write , where either or deg deg . Now, lies in ; if the degree of were less than that of , a contradiction to the choice of . and ; hence, . But the opposite inclusion clearly holds, so that .

**Corollary(15-15):** A nontrivial ideal of is maximal if and only if it is a prime ideal.

**Definition(15-16):** A nonconstant polynomial is said to be irreducible in if and only if cannot be expressed as the product of two polynomials of positive degree. Otherwise, is reducible in .

**Example(15-17):** Any linear polynomial , is irreducible in . Indeed, since the degree of a product of two nonzero polynomials is the sum of the degree of the factors, it follows that a representation

,

with deg deg is impossible. Thus, every reducible polynomial has degree at least .

**Example(15-18):** The polynomial is irreducible in , where is the field of rational numbers. Otherwise, we have

,

where the coefficients . Accordingly,

,

 . Substituting in the relation , we obtain

Thus, , or , which is impossible because is not a rational number.

**Theorem(15-19):** If is a field, the following statements are equivalent:

1. is an irreducible polynomial in .
2. The principal ideal is a maximal (prime) ideal of .
3. The quotient ring is a field.

**Theorem(15-20):** (Unique Factorization Theorem). Each polynomial of positive degree is the product of a nonzero element of and irreducible monic polynomial of .

**Corollary(15-21):** If is of positive degree, then can be factored into linear and irreducible quadratic factors.

**Theorem(15-22):** (Kronecker). If is an irreducible polynomial in , then there is an extension field of in which has a root.

**Corollary(15-23):** If the polynomial is of positive degree, then there exists an extension field of containing a root of .

**Example(15-24):** Consider , the field of integers modulo , and the polynomial . Since neither of the elements or is a root of is irreducible in . Thus, the existence of an extension of , specifically the field

in which the given polynomial has a root. Denoting this root by , the discussion above tells us that

,

where, of course, .

with solution ; therefore, .

Finally, note that factors completely into linear factors in and has the three roots , and :

.

**Example(15-25):** The quadratic polynomial is irreducible in . For, If were reducible, it would be of the form

,

where . It follows at once that and

therefore , and

or, , which is impossible.

The extension field is described by

**Theorem(15-26):** If is a polynomial of positive degree, then there exists an extension field of in which factors completely into linear polynomials.

**Corollary(15-27):** Let with deg . Then there exists an extension of in which has roots.

**Example(15-28):** Let us consider the polynomial over the field of rational numbers.

We first extend to the field , where

and obtain the factorization

 does not factor completely, since the polynomial is irreducible in . For, suppose has a root in , say , with . Substituting, we find that

This equation implies that either or ; but neither nor can be zero, since otherwise we would have or , which is impossible. Thus remains irreducible in .

In order to factor into linear factors, it is necessary to extend the coefficient field further. We therefore constant the extension , where

The elements of may be expressed in the form

Observe that the four roots all lie in .