Rings

Definition: A ring R is a triple $(R,+,.)$ satisfying:

- $(R,+)$ is an abelian group.

A1: $(a+b)+c = a+(b+c)$

A2: $\exists$ an element $0 \in R$ s.t $0+a=a+0=a$ for all $a \in R$.

A3: for every $a \in R$, $\exists -a \in R$ s.t $a+(-a)=(-a)+a=0$

A4: $a+b=b+a$.

- Multiplication is associative:

M1: $(a.b).c = a.(b.c)$

- The distributive Laws hold:

D: $a(b+c)=ab+ac$ and $(b+c).a = ba+ca$.

Remarks:

- If there exsit an element $1 \in R$ s.t

M2: $a.1 = 1.a = a$ for all $a \in R$

Then R is called ring with unity (or ring with identity).

The element $1 \in R$ is referred to the multiplicative identity.

- If R is a ring with unity satisfying:

M3: Every $r \in R \setminus \{0\}$ has a multiplicative inverse

Then R is called a division ring (or skew field).

- If the multiplication operation is commutative i.e

M4: $ab=ba$ for all $a,b \in R$

Then R is called commutative ring.

Examples:

1- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are all commutative ring with unity.

2- $M_2(R)$: the set of 2x2 matrices with real numbers as entries is non commutative ring. In general $AB \neq BA$.

3- $Z[i] = \{a+bi \mid a, b \in Z\}$: the set of Gaussian integer is a commutative ring with unity $1 = 1+0i$.

4- $mZ = \{ma \mid a \in Z\} = \{0, \pm a, \pm 2a, \ldots\}$: the set of all multiple of m - is a commutative ring without unity.

5- $O = \{0, \pm 1, \pm 3, \pm 5, \ldots\}$ - the set of odd integers - is not a ring since it is not closed under addition i.e odd + odd = even.

6- $Q[x] = \{a_0 + a_1 x + \cdots + a_n x^n \mid a_i \in Q\}$: the set of all polynomials in x with coefficients in Q [or in R or in C] is a commutative ring

7- $R = \{a + b\sqrt[3]{2} \mid a, b \in Q\}$. This is not a ring because it is not closed under multiplication. We have $\sqrt[3]{2} \in R$ but $\sqrt[3]{2} \cdot \sqrt[3]{2} = \sqrt[3]{4}$ wich is not a number of the form $a + b\sqrt[3]{2}$.

* Properties of ring:

1) $0 \cdot a = 0 \quad \forall a \in R$

2)- $a \cdot (-b) = -(a \cdot b)$

3)- $(-a)(-b) = -(a \cdot b)$

* proof:

see (The first cours in abstract algebra - p(170)).

* Special elements in a ring:

Definition: Let a be an element of a ring R. We say that a is

1- a **unit** if a has a multiplicative inverse i.e if there exsit an element $b = a^{-1}$ s.t $a.a^{-1} = a^{-1}.a = 1$. The set of units of R is denoted by R^{x}.

Examples:

1- In $\mathbb{Z}$ the only integers having multiplicative invers in $\mathbb{Z}$ are ± 1. Thus $\mathbb{Z}^{x} = \{\pm 1\}$.

2- In $\mathbb{Q}$ every nonzero fraction $\frac{a}{b}$ has a multiplicative inverse $\frac{b}{a}$. Thus $\mathbb{Q}^{x} = \mathbb{Q} \setminus \{0\}$. Also $\mathbb{R}^{x} = \mathbb{R} \setminus \{0\}$.

3- In $\mathbb{Z}_m$, the set of units denoted by U_m, are the elements that relatively prime to m. i.e

$$U_m = \{a \in \mathbb{Z}_m \mid \gcd(a, m) = 1\}.$$

In $\mathbb{Z}_6$, the set of units is given by $U_6 = \{1, 5\}$

2- a **zero divisor** if $a \neq 0$ and there is nonzero element b in R s.t $ab = ba = 0$. For example, 3 is a zero divisor in $\mathbb{Z}_6$ since $2.3 = 0$ but $2 \neq 0$, $3 \neq 0$.

Examples:

1- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ have no zero divisors.

2- In $\mathbb{Z}_m$, the zero divisors are precisely the non-zero element that are not relatively prime to m i.e

$$\text{zero divisors} = \{a \in \mathbb{Z}_m \mid \gcd(a, m) \neq 1\}$$

The zero divisors of $\mathbb{Z}_6 = \{2, 3, 4\}$.

3- **nilpotent**: If $a^{k} = 0$ for some k.

4- **Idempotent**: If $a^{2} = a$

Example: Find all idempotent and nilpotent elements in Z_6.

Sol:

The idempotent of Z_6 are the elements 1, 3 and 4 since $1^2 = 1$, $3^2 = 9 = 3 \pmod 6$, $4^2 = 16 = 4 \pmod 6$)

The only nilpotent element in Z_6 is zero.

Example: Find all idempotent, units, zero divisors, nil potent of Z_3.

- The units of Z_3 are 1, 2
- There are no zero divisors of Z_3
- The idempotent in Z_3 are 0 and 1.
- The nilpotent in Z_3 is 0.

H.W: Find all units, zero divisors, idempotent and nilpotent of $Z_3 \oplus Z_6$.

From the above examples we have:

* The units of $Z_3 \oplus Z_6$ are: $(1,1), (1,5), (2,1), (2,5)$.

* The zero divisors are $\{(a,b) \mid a \in Z_3, b \in \{2,3,4\}\}$

* The idempotents are $\{(a,b) \mid a = 0, 1 ; b = 1, 3, 4\} =$

* The nilpotent element of $Z_3 \oplus Z_6$ is $(0,0)$.

Subrings

Definition: Let R be a ring. A non-empty subset $S \subseteq R$ is a subring if

(a) with respect to addition, S is a subgroup of R.

(b) S is closed under multiplication.

In the other words:

$(S,+)$ is a subgroup of $(R,+)$

- When $a \in S$ and $b \in S$ then $a+b \in S$.
- When $a \in S$ then $-a \in S$ $(0 \in S)$

When $a \in S$ and $b \in S$ then $a.b \in S$

Remarks: A subring of a ring is a ring in it's own right. However, a lot of things can occur.

(a)

It is possible for R to have a unity, but S does not

It is possible for S to have a unity, but R does n't

It is possible for both R and S to have the unity element but they are different

(b) Every ring has tow trivial subrings. The ring it self and the set $\{0\}$.

Definition: (subring test)

A nonempty subset S of a ring R is a subring if

(1) S is closed under subtraction i.e $(\forall a,b \in S \Rightarrow a-b \in S)$

(2) S is closed under Multipli cation (If $a,b \in S$, then $a.b \in S$)

Examples:

1- $\mathbb{Q}$ is a subring of $\mathbb{R}$.

Both $\mathbb{R}$ and $\mathbb{Q}$ have the same unity 1.

2- $S = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \in \mathbb{Z} \right\}$ is a subring of $M_2(R)$.

- Additive closur: $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a+b & 0 \\ 0 & 0 \end{pmatrix} \in S$
- Additive inverse closure

$$-\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} -a & 0 \\ 0 & 0 \end{pmatrix} \in S$$

- Multiplication closure:

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} \in S.$$

$\therefore$ S is a subring of R. Note that:

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the unity of R and $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ is the unity of S.
The unity of R is not the same as the unity of S.

3- $2\mathbb{Z}$ is a subring of $\mathbb{Z}$.

(1)

(2) Let $a, b \in 2\mathbb{Z}$. Then $a = 2x$ and $b = 2y$, where $x, y \in \mathbb{Z}$

$$a - b = 2x - 2y = 2(x-y) \in 2\mathbb{Z}$$

and

. $ab = (2x)(2y) = 2(2xy) \in 2\mathbb{Z}$

By the subring test, $2\mathbb{Z}$ is a subring of $\mathbb{Z}$.

4- The subset $S = \{0, 3, 6, 9\}$ is a subring of $\mathbb{Z}_{12}$.

+	0	3	6	9
0	0	3	6	9
3	3	6	9	0
6	6	9	0	3
9	9	0	3	6

×	0	3	6	9
0	0	0	0	0
3	0	9	6	3
6	0	6	0	6
9	0	3	6	9

acts like a unity since

$9 \times 0 = 0$

$9 \times 3 = 3$

$6 \times 9 = 6$

$9 \times 9 = 6$

- closed under addition
- $(0 \in S : a \in S \Rightarrow -a \in S)$

- closed under Multiplication

5- $Z[i] = \{a+ib \mid a\in Z\}$ is a subring of C

$Z[i] \subseteq C$ and $Z[i] \neq \phi$. Let $x = a+bi$ and $y = c+di$ for $a,b,c,d \in Z$

1) $x-y = (a+ib)-(c+id) = (a-c)+i(b-d)$

$\because a-c,\ b-c \in Z \quad \therefore x-y \in Z[i]$

2) $x.y = (a+ib)(c+id) = (ac-bd)+i(ad+bc)$

$\because ac-bd,\ ad+bc \in Z \quad \therefore xy \in Z[i]$

Therfore by subring test, $Z[i]$ is a subring of $\mathbb{C}$.

6- $Z[\sqrt{2}] = \{a+b\sqrt{2} \mid a,b \in Z\}$ is a subring of C

$Z[\sqrt{2}] \subseteq C$ and $Z[\sqrt{2}] \neq 0$. Let $x = a+b\sqrt{5}$, $y = c+d\sqrt{5}$ for $a,b,c,d \in Z$

1)- $x-y = (a+b\sqrt{5})-(c+d\sqrt{5}) = (a-c)+(b-d)\sqrt{5} = e+f\sqrt{5}$

Since e and $f \in Z \Rightarrow x-y \in Z[\sqrt{2}]$

2) $x.y = (a+b\sqrt{5}).(c+d\sqrt{5}) = (ac+5bd)+(bc+ad)\sqrt{5} = g+hi\sqrt{5}$

since h and $g \in Z \Rightarrow x.y \in Z[\sqrt{2}]$

Hence by subring test, $Z[\sqrt{2}]$ is a subring of C.

7- $Q(\sqrt{2}) = \{a+b\sqrt{2} \mid a,b \in Q\}$ is a subring of C. H.W.

General Results:

1- Subring of Z:

Theorem 1: All subring of Z are of the form mZ for some $m \in N \cup \{0\}$.

Example: let $E = 2Z$ be the set of even number and O, the set of odd numbers. Is either of these a subring of Z ?

2- Subring of Z_m.

$Z_m = \{0, 1, --- m-1\}$. For any positive divisors d of m, we let $dZ_m = \{da : a \in Z_m\} = \{0, d, 2d, \dots (\frac{m}{d} - 1)d\}$.

Ex: Find $2Z_{12}$ and 7_{21}.

$2Z_{12} = \{0, 2, 4, 6, 8, 10\}$ and $7Z_{21} = \{0, 7, 14\}$

Theorem 2: Every subring of Z_m is of the form dZ_m for some $d | m$

Ex: Find all subrings of Z_{12}.

The divisors of Z_{12} are 1, 2, 3, 4, 6, 12. Thus the subrings are

$Z_{12} = Z_{12}$

$2Z_{12} = \{0, 2, 4, 6, 8, 10\}$

$3Z_{12} = \{0, 3, 6, 9\}$ ✓ We prove this in Ex:4

$4Z_{12} = \{0, 4, 8\}$

$6Z_{12} = \{0, 6\}$

$12Z_{12} = \{0\}$

Ex: Is Z_6 ~~is~~ subring of Z_{12}.

No, because Z_6 is not even a subset of Z_{12}.

Integral domain

Definition:

An integral domain is a commutative ring with unity and no Jero divisors.

This is equivalent to say:

An integral domain is a commutative ring with unity in which the product of any two nonzero elements in not equal to Jero i.e $a.b=0 \Rightarrow a=0$ or $b=0$

Theorem:

Any subring of a field is an integral domain.

proof:

suppose R is a subring of a field F. Take $x, y \in R$ with $xy=0$. We need to show that one of x, y is Jero. Suppose $y \neq 0 \Rightarrow y$ is a unit. Thus

$$xyy^{-1}=0 \Rightarrow x=0$$

Examples:

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are integral domains.

2. $\mathbb{Z} \oplus \mathbb{Z}$ is not an integral domain since $(0,1).(1,0)=(0,0)$. So $(0,1)$ and $(1,0)$ are Jero divisors.

3. A subring of an integral domain is always an integral domain.

4. The ring $\mathbb{Z}[i]=\{a+bi \mid a,b \in \mathbb{Z}\}$ is an integral domain. [since it is a subring of $\mathbb{C}$]

5. $M_2(\mathbb{Z})$ of 2×2 matrices over integers is not an integral domain. since

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Remark: $M_2(R)$ is not integral domain even if R is. For example let $R = \mathbb{Z}_2$ is an integral domain. Then

$M_2(\mathbb{Z}_2)$ is not an integral domain. Since

$$\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\cdot\begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$$

i.e $M_2(\mathbb{Z}_2)$ has zero divisors.

* Cancellation Laws for multiplication:

Let a,b and c belong to an integral domain. If $a \neq 0$ and $ab = ac$, then $b = c$

proof:

From $ab = ac$, we have $a(b-c) = 0$. Since $a \neq 0$

$\Rightarrow b - c = 0$

Remark: In ring $\mathbb{Z}_6$, $3\cdot 2 = 3\cdot 4$ but $2 \neq 4$. So the Cancellation Law fail to hold in $\mathbb{Z}_6$. is not integral domain

Note: The cancellation law never fail to hold in rings with out zero divisors i.e (Integral domain).

Th(2): let p be a prime and $p|ab$ where $a,b \in \mathbb{Z}$, then $p|a$ or $p|b$.

Th: let $m \geq 2$. Then $\mathbb{Z}_m$ is an integral domain iff m is prime.

($\Leftarrow$) let $n = p$ be a prime. Suppose a and b are zero divisors in $\mathbb{Z}_p$ with $1 < a,b < p$. Then $ab \equiv 0 \pmod{p}$ so $p|ab$ but then $p|a$ or $p|b$ by Th(2). Contradiction. So there are no zero divisors.

($\Rightarrow$) if n is not prime then it has proper factors a,b with $1 < a,b < n$ and $m = ab$ so in $\mathbb{Z}_m$.

$a,b \neq 0$ but $a\cdot b = (a\cdot b] = m = 0$

" Field "

Definition: A ring F is a field if satisfying

1). $(F, +)$ is an abelian group.

2). $(F^*, \cdot)$ is an abelian group

3). The distributive Laws hold's

Note: The Key thing is the

1- Existence of multiplicative inverse

2- Also $ab = b \cdot a$ and

3- $1 \in F$.

Another definition of a field is given by:

A field is a Commutative ring in whic nonzero element has a multiplicative inverse.

Examples:

1- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields

2- $\mathbb{Z}, \mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{d}]$ are not fields since $\frac{1}{2}$ does n't belong to them.

3- $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ is a field. (why)

Being a subring of $\mathbb{C}$, it is an integral domain. Thus it remains to Show that every non-zero element has a multiplicative inverse. Suppose $x \in \mathbb{Q}(\sqrt{2}) \setminus \{0\}$. Then $x = a + b\sqrt{2}$ with $a, b \neq 0$. Then

$$x^{-1} = \frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{(a-b\sqrt{2})(a+b\sqrt{2})}$$

$$= \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$$

Note that $a^2 - 2b^2 \neq 0$ since if $a^2 - 2b^2 = 0$ then $\frac{a^2}{b^2} = 2$

$\Rightarrow \sqrt{2} = \pm \frac{a}{b} \in \mathbb{Q}$ (contradiction)

since $\sqrt{2}$ is irrational number belong to $\mathbb{R}$.

Theorem: Every field is an integral domain.

proof: Must check there are no Jero divisors

Suppose that $ab=0$, $a \neq 0$ and $b \neq 0$. Then

since it is a field

a^{-1} exsist , $a^{-1}ab = a^{-1}0 \Rightarrow b=0$ (contradiction)

Remark: The converse of the theorem is not true since $\mathbb{Z}$ is an integral domain but is not a field.

Theorem: Every finite integral domain is a field.

proof: Let D be a finit integral domain say

$D = \{a_1, a_2, \dots a_n\}$.

To show that D is a field, we need only to show that:

every nonJero element of D has a multiplicative inverse.

Take any $a \in F$. , $a \neq 0$. Consider $\{aa_1, aa_2, \dots aa_n\}$. If for some i and j we have $aa_i = aa_j$ then $a_i = a_j$ by the cancelation property. Therfore $\{aa_1 \dots aa_n\}$ is a set of n-distinct elements of D Since D. has n elements, $\{aa_1, \dots aa_n\} = D = \{a_1, a_2, \dots a_n\}$. Thus any a_i can be written as aa_j for somj. In particular, 1

$1 = aa_j$ for some j hence $a_j = a^{-1}$ and a has a multiplicative inverse.

The characteristic of Ring

Let R be any ring. If $a \in R$ we define

$$1a = a$$
$$2a = a+a$$
$$3a = a+a+a$$

and so on. In general, if n is any positive integer,

$$na = \underbrace{a+a+a+\cdots+a}_{n\text{-times}}$$

Definition: Let R be a ring. If there is a positive integer n s.t $na = 0$ for all $a \in R$ then the least such n is called the characteristic of R. If there is no such n then R is said to have characteristic 0

Example:

1- The characteristic of Z_n is n.

2- The rings C, R, Q and Z all have characteristic zero.

3- Let S be the subring of Z_8 given by $S = \{0, 2, 4, 6\}$, then

$$1 \cdot 2 = 2 \neq 0$$
$$2 \cdot 2 = 2+2 = 4 \neq 0$$
$$3 \cdot 2 = 2+2+2 = 6 \neq 0$$

So the char of S is not 1, 2 or 3 but

$$4 \cdot 2 = 2+2+2+2 = 8 = 0$$

and for all $a \in S$ we have

$$4+4+4+4 = 16 = 0$$
$$6+6+6+6 = 24 = 0$$
$$0+0+0+0 = 0$$

So S has characteristic 4.

Ideals and Factor ring

Definition: An ideal I of a commutative ring R is a subgroup of $(R, +)$ satisfying:

$$\forall a \in R \quad \forall x \in I \quad ax \in I \text{ and } xa \in I$$

If I is an ideal of R, we write $I \trianglelefteq R$.

Definition: The quotient ring or factor ring R/I is the ring of all cosets or residu classes $a + I$ with $a \in R$. $\Big\}$ $R/I = \{r+I : r$

Addition and multiplication in R/I are defined by

$$(a+I)+(b+I)=(a+b)+I$$

$$(a+I)(b+I)=ab+I$$

Ex: Show that $3\mathbb{Z} \trianglelefteq \mathbb{Z}$ and list all the distinct cosets of the ideal $3\mathbb{Z}$ in $\mathbb{Z}$.

To prove that $3\mathbb{Z}$ is an ideal in $\mathbb{Z}$, we need to show that:

① - $(3\mathbb{Z}, +)$ is a subgroup. Indeed, since

* $3\mathbb{Z}$ closed under addition.

* $0 \in 3\mathbb{Z}$

② $\forall a \in 3\mathbb{Z}$ and $b \in \mathbb{Z}$ then $ab = ba \in 3\mathbb{Z}$.

The factor ring is $\mathbb{Z}/3\mathbb{Z}$. This has 3 cosets:

$$\mathbb{Z}/3\mathbb{Z} = \{0+3\mathbb{Z},\ 1+3\mathbb{Z},\ 2+3\mathbb{Z}\}.$$

In general: $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ and the factor ring is $\mathbb{Z}/n\mathbb{Z}$.

Ideal test:

A nonempty subset I of a ring R is an ideal of R if

1- $a-b \in A$ whenever $a,b \in I$:

2- ra and ar in I whenever $a \in I$, and $r \in R$

Ex: Let I be the set of all polynomial in $\mathbb{Z}[x]$ with 0 constant term. Then $I \trianglelefteq \mathbb{Z}[x]$.

1)- $0 \in I$, and if $p(x)$, $q(x)$ have no constant term, neither does $p(x)-q(x)$. So I is a subgroup of $\mathbb{Z}[x]$.

2)- If $p(x) \in I$ and $r(x) \in \mathbb{Z}[x]$ then $p(x) = p_1x + p_2x^2 + \dots\dots + p_nx^n$ and $r(x) = r_0 + r_1x + \cdots + r_mx^n$ then $p(x)\,r(x) = p_1r_0x + \dots\dots$ has no constant term So $p(x)\,r(x) \in I$.

Theorem: Let R be a commutative ring. Let $a \in R$ and let $\langle a \rangle = \{ab \mid b \in R\}$. Then $\langle a \rangle$ is an ideal in R i.e $\langle a \rangle \trianglelefteq R$.

Proof:

① $\langle a \rangle$ is non-empty. If ra, $sa \in \langle a \rangle$ then $ra - sa = (r-s)a \in \langle a \rangle$ Sa $\langle a \rangle$ is a subgroup.

② Let $ra \in \langle a \rangle$ and b any element $\in R$. Then $(ra)b = b(ra) = (br)a \in \langle a$ so by the ideal test $\langle a \rangle$ is an ideal in R.

Definition: Let R be a commutative ring. The ideal $\langle a \rangle$ is called the principal ideal generated by a.

Ex: Find all principal ideal in $\mathbb{Z}_4$.

we compute (a) for every single $a \in \mathbb{Z}_4$

$\langle 0 \rangle = \{0\}$, $\langle 1 \rangle = \{0,1,2,3\}$, $\langle 2 \rangle = \{0,2\}$, $\langle 3 \rangle = \{0,1,2,3\}$

Since $\langle 1 \rangle = \langle 3 \rangle$, we have exactly 3 distinct principal ideals in $\mathbb{Z}_4$:

$\langle 0 \rangle$, $\langle 1 \rangle$ and $\langle 2 \rangle$.

Remarks:

1)- The ideals in Z_m are all principal.

2)- Every ideal of Z is principal

3)- Example above (the polynomial in $Z[x]$ with Jero constant term) is the principal ideal $\langle x \rangle$.

Further Example:

prove that $I = \{0, 3\}$ is an ideal in Z_6 and compute the cosets of Z_6/I.

We need to show that

1) $\{0, 3\}$ is an additive subgroup.

2)- if $a \in I$ and $b \in Z_6$ then $a \cdot b \in I$

+	0	3
0	0	3
3	3	0

x	0	1	2	3	4	5
0	0	0	0	0	0	0
3	0	3	0	3	0	3

Computing $a + I$ for every $a \in Z_6$ we have

$$0 + I = \{0, 3\} \quad ✓$$
$$1 + I = \{1, 4\} \quad ✓$$
$$2 + I = \{2, 5\} \quad ✓$$
$$3 + I = \{0, 3\}$$
$$4 + I = \{1, \textcircled{4}\}$$
$$5 + I = \{2, 5\}$$

There are 3 distinct cosets and therfore:

$Z_6/I = \{0 + I, 1 + I, 2 + I\}$

Remark:

Every ideal is a subring but the converse is not true. For example: we have proved that $S = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \in R \right\}$ is a subring of $M_2(R)$ but S is not an ideal in R. Take

$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in S$ and $B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in R$ then $AB = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \notin S$.

Definition: A ring homomorphism $\varphi : R \rightarrow S$ from a ring R to a ring S is a function from R to S that preserves both operations of R; so for all $a, b \in R$

- $\varphi(a+b) = \varphi(a) + \varphi(b)$.
- $\varphi(ab) = \varphi(a)\varphi(b)$.

- A ring homomorphism that is one-to-one and onto is called a ring isomorphism.

Definition: The image $\varphi(R)$ of a ring homomorphism $\varphi : R \rightarrow S$ is $\{s \in S \mid \varphi(r) = s \text{ for } r \in R\}$.

Definition: The Kernel $\ker(\varphi)$ of a ring homomorphism $\varphi : R \rightarrow S$ is $\{r \in R \mid \varphi(r) = 0\}$.

Example: Consider $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}_6$ defined by $\varphi(a) = a \bmod 6$ for all $a \in \mathbb{Z}$. Then for all $a, b \in \mathbb{Z}$

- $$\begin{aligned}\varphi(a+b) &= a+b \pmod 6 \\ &= (a \bmod 6) + (b \bmod 6) \\ &= \varphi(a) + \varphi(b)\end{aligned}$$

- $$\begin{aligned}\varphi(ab) &= ab \pmod 6 \\ &= (a \bmod 6)(b \bmod 6) \\ &= \varphi(a)\varphi(b)\end{aligned}$$

Here
$\varphi(0) = 0$
$\varphi(6) = 0$
different elements = Same image (onto)
not 1-1.

$\operatorname{Im}\varphi = \mathbb{Z}_6$ and $\ker\varphi = 6\mathbb{Z}$.

In general: For any $n \in \mathbb{Z}$, The mapping

$$\begin{aligned}\varphi : \mathbb{Z} &\rightarrow \mathbb{Z}_n \\ a &\rightarrow a \bmod n\end{aligned}$$

is a ring homomorphism with kernel equal to $n\mathbb{Z}$.

2- $\varphi: \mathbb{Z} \longrightarrow M_2(\mathbb{Z})$ defined by $\varphi(a) = \begin{bmatrix} 0 & 0 \\ a & a \end{bmatrix}$ for all $a \in \mathbb{Z}$.
Then for all $a, b \in \mathbb{Z}$

- $\varphi(a+b) = \begin{bmatrix} 0 & 0 \\ a+b & a+b \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ a & a \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ b & b \end{bmatrix} = \varphi(a) + \varphi(b)$

- $\varphi(ab) = \begin{bmatrix} 0 & 0 \\ ab & ab \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ a & a \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 \\ b & b \end{bmatrix} = \varphi(a) \cdot \varphi(b)$.

$\text{Im}\,\varphi = \left\{ \begin{bmatrix} 0 & 0 \\ a & a \end{bmatrix} \mid a \in \mathbb{Z} \right\}$. Also

$\text{Ker}\,\varphi = \{0\}$

. Note that φ is 1-1, but not onto.

3. $\varphi: \mathbb{Z}[i] \longrightarrow \mathbb{Z}[i]$ defined by $\varphi(a+bi) = a-bi$ for all $a \in \mathbb{Z}$.
Then for all $a, b \in \mathbb{Z}$

$$\begin{aligned} \varphi((a+bi)+(c+id)) = a-bi+c-id &= (a+c) + (b+d)i \\ &= (a-bi) + (c-d \\ &= \varphi(a+bi) + \varphi(c+di) \end{aligned}$$

$$\begin{aligned} \varphi(a+bi)\varphi(c+di) = (a-bi)(c-di) = (ac-bd) - (ad+bc)i \\ = \varphi((ac-bd)+(ad+bc)i) \\ = \varphi((a+bi)(c+di)). \end{aligned}$$

$\text{Im}\,\varphi = \mathbb{Z}[i]$. Also, $\text{Ker}\,\varphi = \{0\}$.

φ is 1-1 and onto, so φ is an isomorphism

2. $\varphi : \mathbb{Z} \longrightarrow M_2(\mathbb{Z})$ defined by $\varphi(a) = \begin{bmatrix} 0 & 0 \\ a & a \end{bmatrix}$ for all $a \in \mathbb{Z}$.
Then for all $a, b \in \mathbb{Z}$

- $\varphi(a+b) = \begin{bmatrix} 0 & 0 \\ a+b & a+b \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ a & a \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ b & b \end{bmatrix} = \varphi(a) + \varphi(b)$

- $\varphi(ab) = \begin{bmatrix} 0 & 0 \\ ab & ab \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ a & a \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 \\ b & b \end{bmatrix} = \varphi(a) \cdot \varphi(b)$.

$\operatorname{Im} \varphi = \left\{ \begin{bmatrix} 0 & 0 \\ a & a \end{bmatrix} \mid a \in \mathbb{Z} \right\}$. Also

$\operatorname{Ker} \varphi = \{0\}$

. Note that φ is 1-1, but not onto.

3. $\varphi : \mathbb{Z}[i] \longrightarrow \mathbb{Z}[i]$ defined by $\varphi(a+bi) = a-bi$ for all $a \in \mathbb{Z}$.
Then for all $a, b \in \mathbb{Z}$

$$\begin{aligned} \varphi((a+bi)+(c+id)) = a-bi+c-id &= (a+c) + (b+d)i \\ &= (a-bi) + (c-d \\ &= \varphi(a+bi) + \varphi(c+di) \end{aligned}$$

$$\begin{aligned} \varphi(a+bi)\varphi(c+di) = (a-bi)(c-di) &= (ac-bd) - (ad+bc)i \\ &= \varphi((ac-bd) + (ad+bc)i) \\ &= \varphi((a+bi)(c+di)). \end{aligned}$$

$\operatorname{Im} \varphi = \mathbb{Z}[i]$. Also, $\operatorname{Ker} \varphi = \{0\}$.

φ is 1-1 and onto, so φ is an isomorphism

Example : For any integer n we can define a ring homomorphisim

$$\varphi : \mathbb{Z} \rightarrow \mathbb{Z}_n \text{ by } a \rightarrow a \pmod n.$$

This is indeed a ring homomorphism since:

$$\varphi(a+b) = (a+b) \pmod n$$

$$= a \pmod n + b \pmod n$$

$$= \varphi(a) + \varphi(b).$$

and

$$\varphi(ab) = ab \pmod n$$
$$= a \pmod n . \; b \pmod n.$$
$$= \varphi(a)\, \varphi(b).$$

The kernel of the homomorphism φ is $n\mathbb{Z}$.

Show that the map $f : \mathbb{Z}_{12} \rightarrow \mathbb{Z}_4$ that sends ~~12~~ mod 12 to $a \pmod 4$ is well defined surjective homomorphism.

To show that f is well defined, we need to show that whenever:

$$a \pmod{12} = b \pmod{12} \text{ in } \mathbb{Z}_2 \Rightarrow f(a \bmod 12) = f(b \bmod 12)$$

$8 = 3 \bmod 5$

$\rightarrow 8-3 = 5k$ if $a \pmod{12} = b \bmod 12 \Rightarrow a - b = 12k$ for some $k \in \mathbb{Z}$. Thus

$5 = 5k$ $a - b = 4(3k)$ and hence

$\downarrow$

$k = 1$

$$f(a \bmod 12) = (a \bmod 4) = (b \bmod 4) = f(b \bmod 12)$$

$f(3 \bmod 12)$

$= f(3) = 3 \bmod 4$ as required.

$= 3$

To show that f is homomorphism, note that for any

$a \pmod{12}$, $b \pmod{12} \in \mathbb{Z}_{12}$, we have

$$f(a \bmod 12 + b \bmod 12) = f((a+b) \bmod 12)$$
$$= [(a+b) \bmod 4]$$
$$= a \bmod 4 + b \bmod 4$$
$$= f(a \bmod 12) + f(b \bmod 12).$$

and:

$$f([a]_{12}[b]_{12}) = f([ab]_{12}) = [ab]_4 = [a]_4[b]_4 = f([a]_{12})\, f(([b]_{12}$$

as required.

To show that f is surjective note that

$f[0]_{12} = [0]_4$, $f[1]_{12} = [1]_4$, $f[2]_{12} = [2]_4$ and $f[3]_{12} = [3]_4$.

Because we can hit everything in $\mathbb{Z}_4$, f is a surjective.

Find the kernel of f.

An element $[a]_{12} \in \mathbb{Z}_{12}$ is in the kernel of $f \Leftrightarrow [a]_4 = 0$, that is if $4 | a$. The integers between zero and eleven which are divisible by 4 are $\{0, 4, 8\}$. So the kernel of f is the ideal generated by $\{0, 4, 8\}$.

Polynomial Rings

Definitions:-

Let R be a commutative ring. Any expression of the form

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \mid a_i \in R$$

is called the ring of polynomials over R, in the indeterminate x.

- The elements $a_0, a_1, \dots a_n$ are called the coefficients of f.
- The coefficient a_n is called the leading coefficient.
- A polynomial is called monic if the leading coefficient is 1
- If n is the largest nonnegative number for which $a_n \neq 0$, we say that the degree of f is n and write $\deg f(x) = n$.
- If $f=0$ is the zero polynomial then $\deg(0) = -\infty$.
- The set of all polynomials with coefficients in R will be denoted by $R[x]$.
- Two functions f and g are equal on a set X iff $f(x) = g(x)$ for all $x \in X$. For example:

$f(x) = x^4 + 2x^3 + 1$ and $g(x) = (1+x)^2$ over $\mathbb{Z}_3$

There are only three elements in $\mathbb{Z}_3$ and for these

$$f(0) = 1 = g(0)$$
$$f(1) = 1 = g(1)$$
$$f(2) = 0 = g(2)$$

So as a functions over $\mathbb{Z}_3$ these are equal though as polynomials they are different.

* Addition and Multiplication in $R[x]$.

We define the sum of two polynomials as follows. Let

$$p(x) = a_0 + a_1 x + \dots + a_n x^n$$
$$q(x) = b_0 + b_1 x + \dots + b_m x^m$$

Then the sum of $p(x)$ and $q(x)$ is

$$p(x) + q(x) = c_0 + c_1 x + \cdots + c_k x^k$$

where $c_i = a_i + b_i$ for each i.

We define the product of $p(x)$ and $q(x)$ to be

$$p(x)\, q(x) = c_0 + c_1 x + \cdots + c_{m+n} x^{m+n}$$

where

$$c_i = \sum_{k=0}^{i} a_k b_{i-k} = a_0 b_i + a_1 b_{i-1} + \cdots + a_{i-1} b_1 + a_i b_0$$

for each i.

Examples:-

1- In $Z[x]$ the sum of $f(x) = 3x^2 + 5x - 1$ and

$$g(x) = 5x^3 - 3x^2 + 2x + 1$$

is $f(x) + g(x) = 5x^3 + 7x$

2- In $Z[x]$ the product of $p(x) = x^2 + 2x + 3$

$$q(x) = x^2 + 4$$

is $p(x)\, q(x) = x^4 + 2x^3 + 7x^2 + 8x + 12$

3- In $Z_3[x]$ the sum of $f(x) = 2x^3 + 2x^2 + x + 1$ and

$$g(x) = x^3 + 2x^2 + 2$$

is $f(x) + g(x) = 3x^3 + 4x^2 + x + 3$

$$= x^2 + x$$

using $3 \equiv 0 \mod 3$ and $4 \equiv 1 \mod 3$

4- In $Z_{12}[x]$ the sum of $p(x) = 3 + 3x^3$ and

$$q(x) = 4 + 4x^2 + 4x^4$$

is $p(x) + q(x) = 7 + 4x^2 + 3x^3 + 4x^4$ and

$p(x)\, g(x) = 0$

Remark:

The previous example tell us that we can not expect $R[x]$ to be integral domain if R is not an integral domain.

Theorem:- Let $p(x)$ and $q(x)$ are polynomials in $R[x]$, where R is an integral domain. Then

1. $\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$. Furthermore
2. $R[x]$ is an integral domain.

Example:

Let $q(x) = p(x) = 2x+1$ then:

In $\mathbb{Z}_4[x]$:

$p(x)q(x) = 4x^2+4x+1 = 1$ and $\deg[q(x)p(x)] = \deg 1 = 0$

whereas

$\deg(2x+1) + \deg(2x+1) = 1+1 = 2$

we see that $\therefore$ $\deg(p(x)q(x)) \neq \deg(p(x)) + \deg(q(x))$

and we conclude that:

The equality might not be hold if R is not an integral domain

In $\mathbb{Z}[x]$

$$\left.\begin{array}{l}\deg[p(x)q(x)] = \deg[4x^2+4x+1] = 2 \\ \deg(p(x)) + \deg(q(x)) = 1+1 = 2\end{array}\right\}$$ the equality is hold

$\mathbb{Z}[x]$ is an integral domain.

Remark:

In $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$ or $\mathbb{Z}_p[x]$ with p prime we have:

$$\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$$

This may not hold in $\mathbb{Z}_m[x]$ with m composite.

The Division Alogrithm

Theorem (Division Algorithm).
Let F be a field and let $f(x)$ and $g(x) \in F[x]$ with $g(x) \neq 0$. Then there exsit unique polynomials $q(x)$ and $r(x)$ in $F[x]$ s.t

$$f(x) = g(x)\, q(x) + r(x) \quad \text{and}$$

either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

Ex: Suppose we divide $x^3 - x^2 + 2x - 3$ by $x - 2$

$$x^2 + x \rightarrow q(x)$$

$$g(x) \leftarrow x - 2 \quad \big) \quad x^3 - x^2 + 2x - 3 \rightarrow f(x)$$

$$\underline{-x^3 \mp 2x^2}$$

$$x^2 + 2x - 3$$

$$\underline{-x^2 \pm 2x}$$

$$4x - 3$$

$$\underline{-4x \mp 8}$$

$$5 \rightarrow r(x)$$

Hence $x^3 - x^2 + 2x - 3 = (x-2)(x^2 + x + 4) + 5$

Definition: An element $a \in F$ is called a root (or zero) of the polynomial $f \in F[x]$ if $f(a) = 0$

Example:-

1- The elements $2, 3 \in \mathbb{Q}$ are roots of $x^2 - 5x + 6 \in \mathbb{Q}[x]$.

2- The Polynomial $x^2 + 1 \in \mathbb{Q}[x]$ has no roots in $\mathbb{Q}$, but two roots $\pm i \in \mathbb{C}$.

The Factor Theorem:

Let F be a field, $a \in F$, and $f(x) \in F[x]$. Then a is a zero of $f(x)$ iff $x-a$ is a factor of $f(x)$.

By other words:

a is a root of $f(x)$ in $F \Leftrightarrow x-a \mid f(x)$.

Ex: prove that $2x^{51} - 4x^{49} - 2^{51}$ is divisible by $x-2$ in $Q[x]$.

plugging in $x=2$ gives

$$\begin{aligned} &2 \cdot 2^{51} - 4 \cdot 2^{49} - 2^{51} \\ &= 2^{52} - 2^{51} - 2^{51} \\ &= 2^{52} - 2 \cdot 2^{51} \\ &= 2^{52} - 2^{52} = 0 \end{aligned}$$

Since $x=2$ is a root. $x-2$ is a factor by factor theorem.

Root Theorem:-

Let F be a field. A non-zero polynomial $p(x)$ of degree n in $F[x]$ can have at most n distinct zero in F.

Examples:

- The polynomial $x^2+1 \in C[x]$ has 2 roots in C.

- In $Z_8[x]$, The polynomial x^2-1 has 4 roots. There roots are 1, 3, 5 and 7. In fact, this does not contradict (Root Theorem) since Z_8 is not a field becaus $2 \times 4 = 0$.

In each case factor $f(x)$ into linear factor in $F[x]$.

1)- $f(x) = x^3+1$, $F = \mathbb{Z}_7[x]$.

In $\mathbb{Z}_7[x]$ we have $f(-1) = (-1)^3+1 = 0$. So that -1 is a root of $f(x)$. Hence $x+1 \mid f(x)$ in $\mathbb{Z}_7[x]$. By division $f(x)$ by $x+1$ we get

$(x^3+1) = (x+1)(x^2-x+1)$

Now we look for the roots of

$g(x) = x^2-x+1$ in $\mathbb{Z}_7$. $g(3) = 3^2-3+1 = 0$ (mod 7). So 3 is a root and by division x^2-x+1 with $x-3$ we get:

$x^2-x+1 = (x+3)(x+2)$ in $\mathbb{Z}_7[x]$.

Hence:

$x^3+1 = (x+1)(x-3)(x+2)$ in $\mathbb{Z}_7[x]$.

$$\begin{array}{r|l}
 & x^2-x+1 \\
\hline
x+1 & x^3+1 \\
 & \underline{x^3+x^2} \\
 & -x^2+1 \\
 & \underline{\mp x^2 \mp x} \\
 & x+1 \\
 & \underline{-x\mp 1} \\
 & 0
\end{array}$$

$$\begin{array}{r|l}
 & x+2 \\
\hline
x-3 & x^2-x+1 \\
 & \underline{x^2-3x} \\
 & 2x+1 \\
 & \underline{2x-6} \\
 & 7\equiv 0 \pmod 7
\end{array}$$

2)- $p(x) = x^4+x^3-2x^2-6x-4$ $F = \mathbb{Z}_5$

$p(0) = -4$, $p(1) = -8$, $p(-1) = 0$. Thus $x+1 \mid p(x)$

By division $p(x)$ by $x+1$ we get

$(x^4+x^3-2x^2-6x-4) = (x+1)(x^3-2x-4)$

Now we look for the roots of

$q(x) = x^3-2x-4$, $q(2) = 0$ so that $x-2 \mid q(x)$. by division $q(x)$ by $x-2$ we get

$x^3-2x-4 = (x-2)(x^2+2x+2)$

Now we look for the roots of x^2+2x+2 in $\mathbb{Z}_5$. Since $(1)^2+2(1)+2 = 0 \pmod 5$ and $(2)^2+2(2)+2 = 10 = 0 \pmod 5$. We have 1 and 2 are roots of x^2+2x+2

$$\begin{array}{r|l}
 & x^3-2x-4 \\
\hline
x+1 & x^4+x^3-2x^2-6x-4 \\
 & \underline{x^4+x^3} \\
 & -2x^2-6x-4 \\
 & \underline{-2x^2-2x} \\
 & -4x-4 \\
 & \underline{-4x-4} \\
 & 0
\end{array}$$

$$\begin{array}{r|l}
 & x^2+2x+2 \\
\hline
x-2 & x^3-2x-4 \\
 & \underline{x^3-2x^2} \\
 & 2x^2-2x-4 \\
 & \underline{2x^2-4x} \\
 & 2x-4 \\
 & \underline{2x-4} \\
 & 0
\end{array}$$

Thus in $\mathbb{Z}_5[x]$, $x^2+2x+2 = (x-1)(x-2) = (x+4)(x+3)$ (check)

Hence in $\mathbb{Z}_5[x]$,

$$\begin{aligned} x^4+x^3-2x^2-6x-4 &= (x+1)(x-2)(x+4)(x+3) \\ &= (x+1)(x+3)^2(x+4). \end{aligned}$$

GCD of F(x).

Definition: Let F be a field and suppose that $d(x)$ is the greatest common divisor of two polynomials $p(x)$ and $g(x)$ in $F[x]$. Then there exsist polynomials $r(x)$ and $s(x)$ s.t

$$d(x) = r(x)\,p(x) + s(x)\,g(x).$$

Furthermore, the GCD of two polynomials is unique.

Ex: Over $\mathbb{Q}[x]$ find a greatest common divisor of $f(x) = x^5 + 3x^4 + 5x^2 + 4x + 2$ and $g(x) = x^4 + 2x^3 + 4x^2 + 4x + 4$ and write the answer as a linear combination of f and g.

$$\begin{array}{r|l}
 & x+1 \\ \hline
x^4+2x^3+4x^2+4x+4 & x^5+3x^4+5x^3+5x^2+4x+2 \\
 & -x^5-2x^4-4x^3-4x^2-4x \\ \cline{2-2}
 & x^4+x^3+x^2+2 \\
 & -x^4-2x^3-4x^2-4x-4 \\ \cline{2-2}
 & -x^3-3x^2-4x-2
\end{array}$$

$$\begin{array}{r|l}
 & -\frac{1}{3}x-\frac{1}{3} \\ \hline
3x^2+6x+6 & -x^3-3x^2-4x-2 \\
 & x^3+2x^2+2x \\ \cline{2-2}
 & -x^2-2x-2 \\
 & x^2+2x+2 \\ \cline{2-2}
 & 0
\end{array}$$

$F(x) = g(x)(x+1) + (x^3+3x^2+4x+2)$

The GCD is: $3x^2+6x+6$

$$\begin{array}{r|l}
 & -x+1 \\ \hline
-x^3-3x^2-4x-2 & x^4+2x^3+4x^2+4x+4 \\
 & -x^4-3x^3-4x^2-2x \\ \cline{2-2}
 & -x^3+2x+4 \\
 & x^3+3x^2+4x+2 \\ \cline{2-2}
 & 3x^2+6x+6
\end{array}$$

$g(x) = (-x^3-3x^2-4x-2)(-x+1) + \underbrace{3x^2+6x+6}_{r_2(x)}$

$$\begin{aligned}
r_2(x) &= g(x) - (-x+1)(-x^3-3x^2-4x-2) \\
&= g(x) - (-x+1)\big(f(x) - (x+1)g(x)\big) \\
&= g(x) - (-x+1)f(x) + (-x+1)(x+1)g(x) \\
&= \big(1 + (-x+1)(x+1)\big)g(x) - (-x+1)f(x) \\
&= (1 - x^2 \cancel{-x} \cancel{+x} + 1)\,g(x) + (x-1)f(x) \\
&= (2 - x^2)\,g(x) + (x-1)f(x)
\end{aligned}$$

check!!

Factorization of polynomials.

Definition: Irreducible polynomial , Reducible polynomial

If $f \in F[x]$ can be factored $f(x) = g(x)\,h(x)$, with $g, h \in F[x]$ and

$$1 \leq \deg g \, , \, \deg h < \deg f$$

then we say f is reducible. If we can not factor f in this way we say it is irreducible.

1- Degree 2 and 3 Test :-

Theorem:- let $f \in F[x]$. Then

(i)- If $\deg(f) = 1$ then f is irreducible.

(ii)- If $\deg(f) = 2$ or 3, then f is irreducible $\Leftrightarrow$ has no roots:

Examples:

$x^2 - 7$ in $R[x]$

$= (x - \sqrt{7})(x + \sqrt{7})$ reducible ($\sqrt{7}$ is a root and $\sqrt{7} \in R[x]$).

$x^2 - 7$ in $\mathbb{Q}[x]$.

$= (x - \sqrt{7})(x - \sqrt{7})$ irreducible because $\sqrt{7}$ irrational number i.e $\sqrt{7} \notin \mathbb{Q}[x]$.

Remark:

The above theorem is easy to use when the field is $\mathbb{Z}_p$ because in this case, we can check for irreducibility of $f(x)$ by simply testing to see if $f(a) = 0$ for $a = 0, 1, \dots p-1$.

Examples:

1)- $f(x) = x^2 + 1$ over $\mathbb{Z}_5[x]$.

$f(0) = 1$, $f(1) = 2$, $f(2) = 0$

$f(x)$ is reducible over $\mathbb{Z}_5[x]$ since 2 is a root.

2)- $f(x) = x^2 + 1$ over $\mathbb{Z}_3[x]$

$f(0) = 1$, $f(1) = 2$, $f(2) = 2$

$f(x)$ is irreducible over $\mathbb{Z}_3[x]$ since it has no roots in $\mathbb{Z}_3[x]$.

Remark:

Note that polynomials of degree larger than 3 may be reducible over a field even though they do not have roots in the field

For example:

$x^4 + 2x^2 + 1 = (x^2+1)(x^2+1)$

It is reducible over $\mathbb{Q}$ but it has no rational roots.

Ex: List all polynomials of degree ≤ 3 in $\mathbb{Z}_2[x]$.

Degree 1: x, $x+1$.

Degree 2: x^2, x^2+x, x^2+1, x^2+x+1.

Degree 3: x^3, x^3+1, x^3+x, x^3+x^2, x^3+x^2+x, x^3+x^2+x+1
x^3+x^2+1, x^3+x+1.

H.W: List all polynomials of degree ≤ 3 in $\mathbb{Z}_3[x]$.

Ex: Find all monic irreducible polynomials of degree 2 in $\mathbb{Z}_3[x]$. Justify why each of these polynomials are irreducible and why these are the only irreducible.

Sol:

- A polynomial of degree 2 in $\mathbb{Z}_3[x]$ is irreducible $\Leftrightarrow$ it has no roots in $\mathbb{Z}_3[x]$.
- There are $3^2 = 9$ monic polynomials of degree 2 in $\mathbb{Z}_3[x]$
x^2, x^2+1, x^2+2, x^2+x, x^2+2x, x^2+x+1, x^2+x+2
x^2+2x+1, x^2+2x+2.
of which three have no constant, hence zero would be a root of these three. This leaves six possibilities. we test these six for roots

$f(x)$	x^2+1	x^2+2	x^2+x+1	x^2+x+2	x^2+2x+1	x^2+2x+2
$f(1)$	2	0	0	1	1	2
$f(2)$	2	0	1	2	0	1

There exactly 3 monic degree 2 polynomials without roots x^2+1, x^2+x+2, x^2+2x+2. Hence they are the only monic degree 2 irreducible polynomials in $\mathbb{Z}_2[x]$.

Ex: prove that the following polynomials are irreducible

1)_ $x^4+x^3+x^2+x+1$ is irreducible in $\mathbb{Z}_2[x]$.

We note that $f(x)$ has no roots in $\mathbb{Z}_2[x]$ since $f(0)=1=f(1)$ so by: Factor. Th, $f(x)$ has no linear factor and also has no degree 3 factor. Hence we check the irreducible polynomial of degree 2 factors. The only irreducible polynomial of degree 2 in $\mathbb{Z}_2[x]$ is x^2+x+1 hence we divid $f(x)$ by x^2+x+1 and we get a remainder of $x+1$. Therfore x^2+x+1 is not a factor of $f(x)$. Hence $f(x)$ is irreducible.

$$\begin{array}{r|l} & x^2 \\ \hline x^2+x+1 & x^4+x^3+x^2+x+1 \\ & \underline{x^4+x^3+x^2} \\ & x+1 \end{array}$$

2)_ x^2+1 is irreducible over $\mathbb{Z}_7[x]$.

A polynomial of degree 2 or 3 is irreducible iff has no zeros. Since x^2+1 does n't have any zero in $\mathbb{Z}_7[x]$ so it is irreducible.

2- Mod p irreducibility tests_

Let p be a prime and suppose that $f(x) \in \mathbb{Z}[x]$ with degree $f(x) \geq 1$. Let $\bar{f}(x)$ be the polynomial in $\mathbb{Z}_p[x]$ obtained from $f(x)$ by reduction all the coefficients of $f(x)$ mod p. If $\bar{f}(x)$ is irreducible over $\mathbb{Z}_p$ and $\deg \bar{f}(x) = \deg f(x)$, then $f(x)$ is irreducible over $\mathbb{Q}$.

Ex: show that the following polynomials are irreducible, over $\mathbb{Q}[x]$.

1)- $x^4 - 7x^3 + 5x^2 - 3x - 9$

The mod p reduction of $x^4 - 7x^3 + 5x^2 - 3x - 9 \in \mathbb{Z}[x]$ is $\bar{f}(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Z}_2[x]$ and by above example #1, $\bar{f}(x)$ is irreducible in $\mathbb{Z}_2[x]$ so $f(x)$ is irreducible in $\mathbb{Q}[x]$

2)- $x^5 + 5x^2 + 1$

The mod 2 reduction of $f(x) = x^5 + 5x^2 + 1 \in \mathbb{Z}[x]$ is $\bar{f}(x) = x^5 + x^2 + 1 \in \mathbb{Z}_2[x]$. $\bar{f}(x)$ has no roots in $\mathbb{Z}_2[x]$ which means $f(x)$ has no linear factors. Suppose $\bar{f}(x)$ is reducible. Then it is divisible by an irreducible quadratic which must be x^2+x+1 (the only one has no roots in $\mathbb{Z}_2[x]$). Since $x^2 + x + 1 = (x^3+x^2)(x^2+x+1) + 1$. Thus $f(x) \in \mathbb{Z}_2[x]$ is irreducible and therefore, $x^5 + 5x^2 + 1 \in \mathbb{Q}[x]$ is irreducible.

$$
\begin{array}{r|l}
 & x^3 + x^2 \\
\hline
x^2+x+1 & x^5 + x^2 + 1 \\
 & \underline{x^5 + x^4 + x^3} \\
 & x^4 + x^3 + x^2 + 1 \\
 & \underline{x^4 + x^3 + x^2} \\
 & 1
\end{array}
$$

3)- $x^4 + x + 1$

The mod 2 reduction of $f(x) = x^4 + x + 1 \in \mathbb{Z}[x]$ is $\bar{f}(x) = x^4 + x + 1 \in \mathbb{Z}_2[x]$. Since $f(0) = 1 = f(1)$. it follows that $f(x)$ has no linear factors. Suppose that $f(x)$ is reducible polynomial in $\mathbb{Z}_2[x]$. Then it must be the product of irreducible quadratic factors. Since the only irreducible quadratic polynomial in $\mathbb{Z}_2[x]$ is x^2+x+1. Thus we have $\bar{f}(x) = (x^2+x+1)^2 = x^4 + x^2 + 1$ which is not the case. Thus $\bar{f}(x) \in \mathbb{Z}_2[x]$ is irreducible and hence $x^4 + x + 1 \in \mathbb{Q}[x]$ is irreducible.

3- Eisenstein Criterion:-

Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. If there is a prim such that $p \mid a_{n-1}, \ldots p \mid a_0$ but $p \nmid a_n$ and $p^2 \nmid a_0$ then $f(x)$ is irreducible over $\mathbb{Q}$.

Ex: Use Eisenstein's Criterion to show that each of the following polynomials is irreducible in $\mathbb{Q}[x]$.

1)- $f(x) = 3x^2 + 15x^4 - 20x^3 + 10x + 20$

$f(x)$ is irreducible over $\mathbb{Q}$ because $5 \nmid 3$ and $25 \nmid 20$ but 5 does divide $15, -20, 10$ and 20.

2- $g(x) = x^4 - 12x^2 + 18x - 24$

$f(x)$ is irreducible over $\mathbb{Q}[x]$ because $3 \nmid 1$ and $9 \nmid 24$ but 3 does divide -12, 18 and -24.

3- $h(x) = x^4 + 1$

$$h(x+1) = (x+1)^4 + 1$$
$$= x^4 + 4x^3 + 6x^2 + 4x + 2.$$

This polynomial is irreducible over $\mathbb{Q}[x]$ because $2 \nmid 1$ and $4 \nmid 2$ but 2 does divide $4, 6,$ and 2. Hence $h(x)$ is irreducible.

Remarks:-

Theorem: Let F be a field and $p(x)$ an irreducible polynomial over F. Then $F[x]/p(x)$ is a field.

1. The elements of $F[x]/p(x)$:

Ex: The elements of $\mathbb{Z}_2[x]/x^2+1$ are given by

$$\mathbb{Z}_2[x]/(x^2+1) = \{ax+b+\langle x^2+1\rangle \mid a,b \in \mathbb{Z}_2\}$$
$$= \{0+\langle x^2+1\rangle, 1+\langle x^2+1\rangle, x+\langle x^2+1\rangle, x+1+\langle x^2+1\rangle\}$$
$$= \{0, 1, x, x+1\}$$

The calculation is done by this way:

For example: $1+\langle x^2+1\rangle = x^2+2 = x^2 \pmod 2$. Since we have $p(x) = x^2+1 \Rightarrow x^2 = -1 \Rightarrow x^2 = 1 \pmod 2$

Thus $1+\langle x^2+1\rangle = 1$

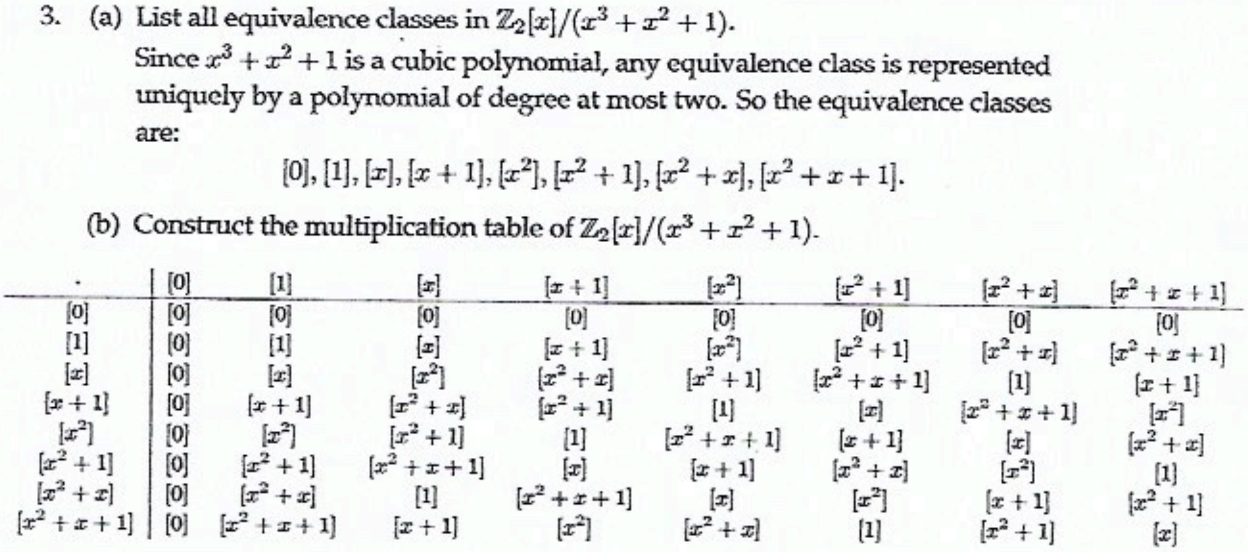
2. Provide the addition and multiplication table for $\mathbb{Z}_2[x]/x^2+1$

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$1+x$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\times$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	1	$x+1$
$x+1$	0	$x+1$	$x+1$	0

$\Rightarrow x(x+1) = x^2+x = 1+x$

we note that $\mathbb{Z}_2[x]/(x^2+1)$ is not a field since $(x+1)(x+1) = x^2+1 = 0$. In the otherwords, there is a zero divisors since x^2+1 is reducible and thus $\mathbb{Z}_2[x]/(x^2+1)$ is not a field.



3. (a) List all equivalence classes in $\mathbb{Z}_2[x]/(x^3+x^2+1)$.

Since x^3+x^2+1 is a cubic polynomial, any equivalence class is represented uniquely by a polynomial of degree at most two. So the equivalence classes are:

$$[0], [1], [x], [x+1], [x^2], [x^2+1], [x^2+x], [x^2+x+1].$$

(b) Construct the multiplication table of $\mathbb{Z}_2[x]/(x^3+x^2+1)$.

$\cdot$	$[0]$	$[1]$	$[x]$	$[x+1]$	$[x^2]$	$[x^2+1]$	$[x^2+x]$	$[x^2+x+1]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[x]$	$[x+1]$	$[x^2]$	$[x^2+1]$	$[x^2+x]$	$[x^2+x+1]$
$[x]$	$[0]$	$[x]$	$[x^2]$	$[x^2+x]$	$[x^2+1]$	$[x^2+x+1]$	$[1]$	$[x+1]$
$[x+1]$	$[0]$	$[x+1]$	$[x^2+x]$	$[x^2+1]$	$[1]$	$[x]$	$[x^2+x+1]$	$[x^2]$
$[x^2]$	$[0]$	$[x^2]$	$[x^2+1]$	$[1]$	$[x^2+x+1]$	$[x+1]$	$[x]$	$[x^2+x]$
$[x^2+1]$	$[0]$	$[x^2+1]$	$[x^2+x+1]$	$[x]$	$[x+1]$	$[x^2+x]$	$[x^2]$	$[1]$
$[x^2+x]$	$[0]$	$[x^2+x]$	$[1]$	$[x^2+x+1]$	$[x]$	$[x^2]$	$[x+1]$	$[x^2+1]$
$[x^2+x+1]$	$[0]$	$[x^2+x+1]$	$[x+1]$	$[x^2]$	$[x^2+x]$	$[1]$	$[x^2+1]$	$[x]$

4. Let $E = \mathbb{Q}[x]/(x^2 - 3)$.

(a) Find the multiplicative inverse of $[3x+4] \in E$.

Let $[ax+b] \in E$ be the multiplicative inverse of $[3x+4]$. Then

$$\begin{aligned}[1] &= [3x+4][ax+b] = [3ax^2 + (3b+4a)x + 4b] \\ &= [3a \cdot 3 + (3b+4a)x + 4b] = [(4a+3b)x + (9a+4b)].\end{aligned}$$

So we have $4a + 3b = 0$, $9a + 4b = 1$. By solving this system of linear equations, we obtain $a = \frac{3}{11}$, $b = -\frac{4}{11}$. So the multiplicative inverse of $[3x+4]$ is $[\frac{3}{11}x - \frac{4}{11}]$.

(b) IS E a field ? Explain your answer

The polynomial $x^2 - 3$ has no roots in $\mathbb{Q}$. So $x^2 - 3$ is irreducible Therefor, $\mathbb{Q}[x]/(x^2 - 3)$ is a field.

5. Let $R = \mathbb{Z}_3[x]/(x^2 + 2x + 2)$. Determine how many congruence classes there are in R and list a representatine of each congruence class.

There are 3 classes. one classe is for Polynomial of degree zero. The other classe is for polynomial of degree 1 and the last one is for zero Polynomial. Hence there are $3^2 = 9$ elements. They are:

$[0]$, $[1]$, $[2]$, $[x]$, $[x+1]$, $[x+2]$, $[2x]$, $[2x+1]$, $[2x+2]$.

b)- Show that $\mathbb{Z}_3[x] / x^2 + 2x + 2$ is a field.

By Theorem [$F/p(x)$ is a field when $p(x)$ is irreducible], it is enough to show that $x^2 + 2x + 2$ is irreducible in $\mathbb{Z}_3[x]$.

In deed $x^2 + 2x + 2$ is irreducible in $\mathbb{Z}_3[x]$ since it has no roots in $\mathbb{Z}_3$ and therefore $\mathbb{Z}_3[x]/x^2 + 2x + 2$ is a field.

6. Construct a field of order 4. What are the elements of this field? Show that the sum of the elements of this field is equal to zero (that is, the additive identity of this field).

Answer: Since $4 = 2^2$, we start with a field $\mathbb{Z}_2$ of characteristic 2 and look for an irreducible polynomial of degree 2 in $\mathbb{Z}_2[x]$. It is easy to note that $p(x) = x^2 + x + 1$ has no zeros in $\mathbb{Z}_2$ since $p(0) = 1 = p(1)$. Hence, the polynomial $p(x) = x^2 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$. Thus $\mathbb{Z}_2[x]/ < x^2 + x + 1 >$ is a field with 4 elements. The elements of this field are given by

$$\begin{aligned}\mathbb{Z}_2[x]/ < x^2 + x + 1 > &= \{ax + b + < x^2 + x + 1 > \mid a, b \in \mathbb{Z}_2\}\\ &= \{0 + < x^2 + x + 1 >,\ 1 + < x^2 + x + 1 >,\\ &\qquad x + < x^2 + x + 1 >,\ x + 1 + < x^2 + x + 1 >\}\\ &= \{0, 1, \alpha, \alpha + 1\},\end{aligned}$$

7. Construct a field of order 4. Provide the addition and multiplication tables for this field.

Answer: Note that α is a zero of the polynomial $p(x) = x^2 + x + 1$ since

$$\begin{aligned}p(\alpha) &= \alpha^2 + \alpha + 1\\ &= (x + < x^2 + x + 1 >)^2 + (x + < x^2 + x + 1 >) + (1 + < x^2 + x + 1 >)\\ &= (x^2 + x + 1 + < x^2 + x + 1 >)\\ &= 0 + < x^2 + x + 1 >\\ &= 0.\end{aligned}$$

Hence $\alpha^2 + \alpha + 1 = 0$ or $\alpha^2 = -\alpha + 1$ which is $\alpha^2 = \alpha + 1$.

The addition table for $\mathbb{Z}_2[x]/ < p(x) >$ is the following:

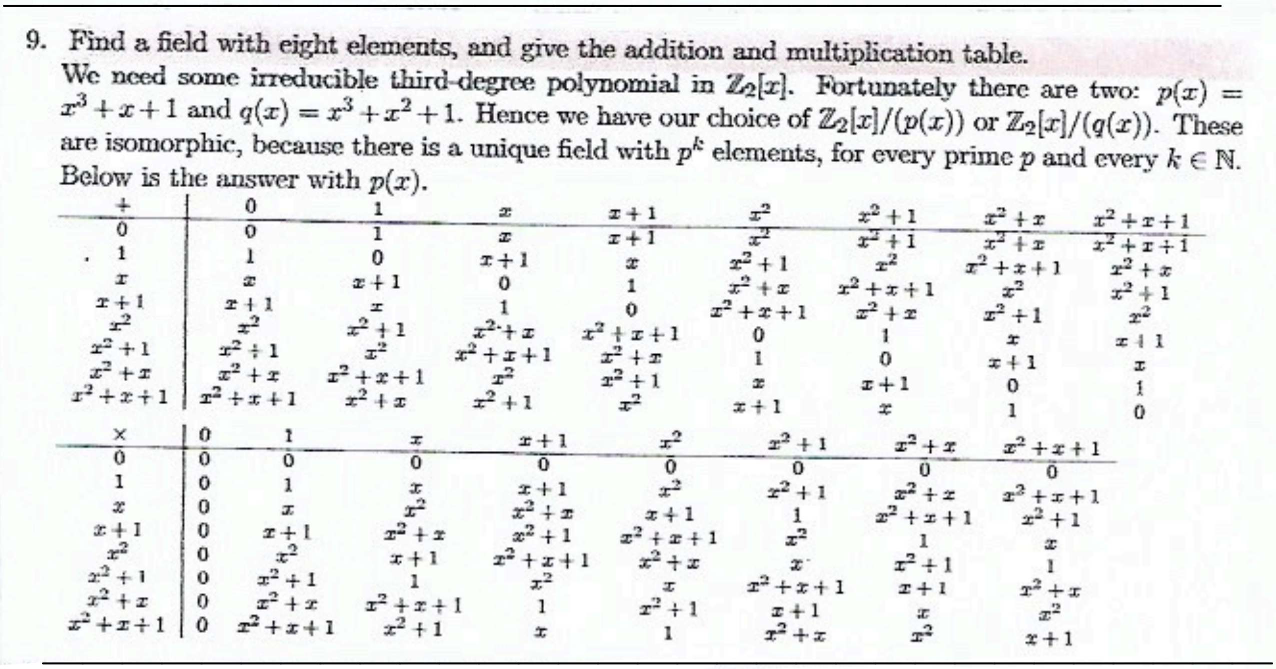
$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

The multiplication table for $\mathbb{Z}_2[x]/ < p(x) >$ is the following:

$\cdot$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

8. Construct a field of order 25. What are the elements of this field?

Answer: Since $25 = 5^2$, we start with a field $\mathbb{Z}_5$ of characteristic 5 and look for an irreducible polynomial of degree 2 in $\mathbb{Z}_5[x]$. Such a polynomial is $p(x) = x^2 + x + 1$.



9. Find a field with eight elements, and give the addition and multiplication table.

We need some irreducible third-degree polynomial in $\mathbb{Z}_2[x]$. Fortunately there are two: $p(x) = x^3 + x + 1$ and $q(x) = x^3 + x^2 + 1$. Hence we have our choice of $\mathbb{Z}_2[x]/(p(x))$ or $\mathbb{Z}_2[x]/(q(x))$. These are isomorphic, because there is a unique field with p^k elements, for every prime p and every $k \in \mathbb{N}$. Below is the answer with $p(x)$.

$+$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

$\times$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$